AGUSTÍ CERRILLO I MARTÍNEZ

Doctor en Derecho
Profesor de Derecho administrativo
Universitat Oberta de Catalunya

Este trabajo ha sido seleccionado y ha obtenido el ***Accésit Premio Estudios Financieros 2005*** en la Modalidad de ***DERECHO ADMINISTRATIVO.***

El Jurado ha estado compuesto por: don Joaquín BORRELL MESTRES, don Joaquín FERRER JACAS, don Tomás FONT LLOVET, don Alfredo GALÁN GALÁN, doña María Jesús MONTORO CHINER y don Joaquín TORNOS MAS.

Los trabajos se presentan con seudónimo y la selección se efectúa garantizando el anonimato de los autores.

Extracto:

E*L* uso de las tecnologías de la información y la comunicación por las Administraciones públicas reporta importantes beneficios, aunque también son algunos los riesgos que puede generar. En particular, el artículo se centra en la exposición de los riesgos que pueden ocasionar para la seguridad de las transacciones y en el análisis de los instrumentos técnicos y jurídicos que existen en la actualidad para hacerles frente.

La utilización de la firma electrónica permite garantizar la autenticidad, la integridad y la conservación de los documentos y, por tanto, es un

.../...

.../...

mecanismo idóneo para garantizar las relaciones telemáticas entre las Administraciones públicas y los ciudadanos.

En el artículo se detallan diversos aspectos relativos al régimen jurídico de la firma electrónica, así como las peculiaridades de su uso por las Administraciones públicas.

Sumario:

1. INTRODUCCIÓN

Hoy en día está ampliamente aceptado que las tecnologías de la información y de la comunicación están provocando importantes cambios en las estructuras económicas, sociales y, también, políticas y administrativas. El estudio de la Administración pública y del Derecho administrativo no puede pasar por alto las transformaciones que, en general, se están produciendo en nuestra sociedad, también llamada sociedad de la información.

En este artículo nos proponemos exponer cuáles son los principales riesgos de las nuevas tecnologías de la información y de la comunicación en la Administración pública y cómo el Derecho administrativo, en la medida en que ya se han ido aprobando diversas normas, les está haciendo frente.

Para ello, a continuación, destacaremos cómo las tecnologías de la información y de la comunicación están ya transformando profundamente la manera como se desarrolla la actividad de la Administración pública. Uno de los ámbitos en que se están experimentando mayores repercusiones es el relativo a las relaciones entre los ciudadanos y las Administraciones públicas. Son nuevos los retos y los problemas que se plantean y a los que la técnica y el derecho, de una manera combinada, tienen que hacer frente.

Ahora bien, hay que dejar claro ya, desde este momento, que la lógica que incorpora la Administración electrónica no tiene que ser únicamente la de automatizar los procesos que se están siguiendo en la actualidad. Es decir, no consiste en hacer lo mismo que se venía haciendo hasta ahora utilizando las TIC. Como afirma la OCDE, «la tecnología es un facilitador pero no una solución» [1]. Por eso, es importante innovar, adaptar y repensar lo que se ha estado haciendo hasta ahora a la nueva realidad [2].

[1] OECD: «Engaging citizens online for better policy-making», *Policy Brief*, núm. marzo, 2003, pág. 1.

[2] Luis FELIPE PARADELA en el prólogo al libro *Firma digital y Administraciones públicas* afirma que «[l]a firma electrónica no se puede introducir en la Administración sin cambiar la forma de actuar tradicional de la Administración pública y de los ciudadanos. Y, sobre todo, exige nuevas formas de entender las organizaciones» (pág. 10).

2. LAS RELACIONES TELEMÁTICAS ENTRE LOS CIUDADANOS Y LA ADMINISTRACIÓN PÚBLICA. UNA APROXIMACIÓN A SU RÉGIMEN JURÍDICO

En la actualidad todavía hay muchas dudas y miedos sobre la incorporación de la informática con efectos externos a las Administraciones públicas. Si la introducción de la informática en la gestión interna de la Administración no ha supuesto especiales problemas y ha sido vista como un símbolo de su modernización, la utilización de la informática como medio relacional con los ciudadanos, tanto para recibir información como para enviarla, no ha sido aceptada, en general, hasta hace relativamente poco tiempo.

«El uso que de Internet viene haciendo la Administración pública es todavía muy limitado: a) como fuente de información (a modo de tarjeta de visita digital o de tablón de anuncios electrónico) la Administración pone anuncios y publica información sobre sí misma o alguno de sus órganos o agencias, requisitos, resultados de determinadas actuaciones, etc.; b) la comunicación directa con el ciudadano es, sin embargo, menor, y de ordinario se limita al correo electrónico; c) las transacciones integrales, ininterrumpidas y sin necesidad de una firma a mano o de presencia física, resultan aún más infrecuentes. No son pocas, desde luego, las reformas internas y organizativas que la Administración ha de emprender para explotar Internet en sus relaciones con el ciudadano. A todo ello no es tampoco ajeno el hecho de que la seguridad y certidumbre jurídicas, la confianza, en suma, en la comunicación electrónica, se encuentren en un estadio inicial.» [3]

Si bien son muchos los beneficios que puede reportar la utilización de las tecnologías de la información y de la comunicación por la Administración pública (eficacia, eficiencia, inmediatez o rapidez), también son importantes los riesgos que puede generar si no se adoptan medidas suficientes para hacerles frente. Entre estos riesgos, podemos destacar [4]:

- El riesgo relativo al incremento de la fractura digital (*digital divide*) y, por lo tanto, de la agravación de las desigualdades.
- El riesgo relativo a la desconfianza, por parte, tanto de los usuarios como de los propios administradores (degradación de la calidad del servicio, despersonalización de la prestación de los servicios públicos, etc.).
- El riesgo de reducir las garantías de los ciudadanos frente la Administración pública.
- El riesgo contra la privacidad de las personas.
- El riesgo contra la seguridad de las transacciones.

[3] BARNES VÁZQUEZ, J. (2000): «Una reflexión introductoria sobre el derecho administrativo y la Administración pública en la sociedad de la información», *Revista Andaluza de Administración Pública*, núm. 40.

[4] Sobre estos aspectos, véase CHEVALIER, J. (2002): «La mise en ouvre de l'Administration electronique», en: *Colloque International «L'Administration électronique au service des citoyens»*, París.

El Derecho administrativo puede ofrecer medios para hacer frente a estos riesgos. En particular, nuestra atención se centrará en exponer los mecanismos que ha ido adoptando el Derecho administrativo con el fin de mantener las garantías de los ciudadanos frente a la Administración pública y, en particular, para garantizar la seguridad de las transacciones electrónicas.

Precisamente, desde un punto de vista jurídico, la incorporación de las nuevas tecnologías por parte de las Administraciones públicas no es sino una manifestación del principio constitucional de eficacia (art. 103.1) y una concreción de esta exigencia constitucional en los procedimientos administrativos es que éstos se tramiten con celeridad [5].

La Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJPAC) recoge algunas previsiones, de carácter general, sobre la utilización de las nuevas tecnologías de la información y de la comunicación en las relaciones de las Administraciones públicas con los ciudadanos. La aprobación de la LRJPAC en 1992 supuso un paso adelante en el proceso de reconocimiento del papel que las nuevas tecnologías podían tener en las relaciones entre las Administraciones públicas y los ciudadanos. Según su exposición de motivos, la LRJPAC:

«aborda de manera frontal y decidida –en contraposición a la timidez de las previsiones de la Ley de Procedimiento Administrativo de 1958– la instalación en soporte informático de los registros generales, así como la integración informática de aquéllos con los restantes registros administrativos.»

Hay diversos preceptos de la LRJPAC que, de manera más o menos directa, regulan el uso de las nuevas tecnologías por parte de las Administraciones públicas. Así, por ejemplo, los artículos 38, 45 y 59 hacen referencia a la informatización de los registros, a la incorporación de los medios electrónicos en el procedimiento administrativo y en la práctica de las notificaciones, respectivamente [6].

Desde un punto de vista genérico y programático, el artículo 45 de la LRJPAC prevé que las Administraciones públicas impulsarán el uso 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 respecto a la utilización de estos medios establecen la Constitución y las leyes. Es especialmente interesante destacar en este punto la necesaria protección de la intimidad de las personas [7].

---

5 Véase AGIRREAZKUENAGA, I; CHINCHILLA, C. (2001): «El uso de medios electrónicos, informáticos y telemáticos en el ámbito de las Administraciones Públicas», *Revista Española de Derecho Administrativo*, número 109. Véase, asimismo, VALERO TORRIJOS, J. (2004): *El régimen jurídico de la e-Administración. El uso de medios informáticos y telemáticos en el procedimiento administrativo*, Granada: Comares.

6 Hay que recordar que estos preceptos fueron modificados por la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, con el fin de prever las consecuencias de la incorporación de las nuevas tecnologías en la tramitación de los procedimientos administrativos haciendo especial incidencia en los registros (art. 38 LRJPAC) y la notificación de los actos administrativos (art. 59 LRJPAC).

7 Véase al respeto, FERNÁNDEZ SALMERÓN, M. (2003): *La protección de los datos personales en las Administraciones públicas*, Madrid: Thomson-Civitas.

Como tendremos oportunidad de ir exponiendo a continuación, uno de los objetivos que la legislación básica persigue es garantizar que, desde el punto de vista jurídico, la incorporación de las nuevas tecnologías en las relaciones de los ciudadanos con las Administraciones públicas no conlleve variaciones de los principios garantizados tradicionalmente en las relaciones plasmadas en el papel. Por eso, se prevé que en la utilización de soportes, medios y aplicaciones electrónicas, informáticas y telemáticas hace falta que se asegure la autenticidad, la confidencialidad, la integridad, la disponibilidad y la conservación de la información [8]. Es decir, las relaciones entre las Administraciones públicas y los ciudadanos mediante las nuevas tecnologías tienen que poseer las mismas garantías que, por otra parte, ya están reconocidas en las relaciones *presenciales* [9].

Hay dos aspectos de carácter general sobre los que conviene prestar atención en este punto. En primer lugar, el reconocimiento de los procedimientos y actuaciones de las Administraciones públicas que pueden ser objeto de tramitación telemática y, en segundo lugar, la validación del *software* o programario necesario para poderlo hacer.

Con respecto a los procedimientos que se tramiten en soporte informático, la LRJPAC sólo establece que tienen que garantizar la identificación y el ejercicio de la competencia por el órgano que lo ejerza [10].

Aplicando este precepto en la Administración General del Estado, el Real Decreto 772/1999, de 7 de mayo, regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado. En este real decreto se prevé que mediante una orden ministerial se crearán los registros administrativos. Estas órdenes ministeriales tendrán que especificar los trámites y procedimientos a los que se pueda aplicar la presentación de escritos telemática [11]. Así, por ejemplo, diferentes órganos de la Administración General del Estado han ido aprobando los listados que contemplan los procedimientos de tramitación telemática que se llevan a cabo bajo su competencia [12].

---

8 Artículo 45.5 de la LRJPAC y el artículo 4 del Real Decreto 263/1996, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado. Véanse en particular las modificaciones introducidas por el 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 por los ciudadanos.

9 Este principio está claramente recogido, por ejemplo, en el Decreto 324/2001, de 4 de diciembre, relativo a las relaciones entre los ciudadanos y la Administración de la Generalitat de Cataluña a través de Internet, cuyo artículo 3 prevé que «[e]n la prestación de los servicios públicos y en las relaciones de los ciudadanos con la Administración de la Generalitat mediante el uso de las técnicas telemáticas a través de Internet se tiene que garantizar el respeto a los derechos y a las libertades reconocidos en la Constitución y regulados por los tratados y las leyes, sin ninguna discriminación en razón del medio utilizado».

10 Artículo 45.3 de la LRJPAC. Véase al respecto BAUZÁ MARTORELL, F.J. (2002): *Procedimiento administrativo electrónico*, Granada: Comares.

11 Artículo 14 del Real Decreto 772/1999, de 7 de mayo, modificado por el Real Decreto 209/2003, de 21 de febrero.

12 Por ejemplo, el Ministerio de Economía. En particular, la Orden de 26 de diciembre de 2001 recoge un listado de los procedimientos susceptibles de aplicación a través del Registro Telemático con respecto a actos administrativos dictados por órganos del Ministerio: recursos administrativos; reclamaciones previas al ejercicio de las acciones civiles y laborales; reclamaciones de responsabilidad patrimonial; revisión de actos nulos de pleno derecho; declaración de lesividad de actos administrativos; revocación de actos administrativos. Véase http://www.mineco.es/admonelectronica/.

A nivel autonómico, podemos traer a colación la regulación adoptada por la Generalitat de Cataluña que prevé, por ejemplo, que los procedimientos administrativos que se tramiten telemáticamente tienen que cumplir los mismos requisitos que en el resto de procedimientos. Ahora bien, en particular, hará falta que se adopten las medidas técnicas que aseguren la identidad, la integridad, la disponibilidad, el no rechazo por razones técnicas, la conservación de la información, la confidencialidad y la accesibilidad de todas las personas [13]. Para garantizar estos principios, el Decreto 324/2001, prevé que la aprobación de procedimientos telemáticos corresponde a los consejeros de los Departamentos de la Generalitat. Éstos también aprobarán los sistemas telemáticos, los programas y las aplicaciones que se usarán. Hará falta que, previamente, la asesoría jurídica del departamento haga un informe previo sobre diversos aspectos (efectos de la presentación de los documentos, sistema de cómputo de los plazos, posibilidad que los ciudadanos puedan conocer el estado de la tramitación de los expedientes administrativos). Los procedimientos serán publicados en el DOGC [14]. Hasta el momento se han aprobado trece [15].

Con respecto al *software* o programario que se utilice en el desarrollo de la Administración electrónica, la LRJPAC prevé que las aplicaciones y los programas que efectúen tratamientos de información cuyo resultado sea utilizado en el ejercicio de potestades administrativas, tendrán que aprobarse mediante una resolución del órgano administrativo que tenga atribuida la competencia para resolver el procedimiento y tendrá que difundir públicamente sus características [16].

Desde un punto de vista general todos estos aspectos se detallan en los *Criterios de seguridad, conservación y normalización de las aplicaciones para el ejercicio de potestades* aprobados por el Consejo Superior de Informática en su sesión de 18 de diciembre de 2001 [17] para delimitar las características que deben tener las aplicaciones y programas informáticos a fin de garantizar los diferentes criterios establecidos por la LRJPAC [18]:

– Los criterios de seguridad exponen los requisitos, criterios y recomendaciones relativos a la implantación de medidas de seguridad organizativas y técnicas en el diseño, desarrollo, implantación y explotación de estas aplicaciones para el ejercicio de potestades [19].

13 Artículo 12.2 del Decreto 324/2001.

14 Artículos 11 y ss. del Decreto 324/2001.

15 Las Órdenes aprobadas lo son para la tramitación telemática de los procedimientos relativos a las entidades jurídicas, apertura de centro de trabajo, obras de construcción, corrección ortográfica de nombres y apellidos, prueba de acceso a ciclos de formación, inscripción a pruebas para obtener certificados de conocimiento de catalán, acceso a determinados cuerpos de la Administración de la Generalitat de Cataluña, autorización de máquinas recreativas y de azar, licencias de pesca recreativa, actividades de educación en el ocio, control y seguimiento de residuos industriales y cédula de habitabilidad.

16 Con respecto a los programas y las aplicaciones, véanse los artículos 5 y ss. del Real Decreto 263/1996 y los artículos 18 y 19 del Decreto catalán 324/2001, 4 de diciembre.

17 Véase la versión actualizada de 24 de junio de 2004 en la dirección Internet: http://www.csi.map.es/csi/pg5c10.htm.

18 En relación a la aprobación de programas y aplicaciones a nivel de la Administración de la Generalitat de Cataluña, véase el artículo 18 del Decreto 324/2001.

19 Véase http://www.map.es/csi/criterios/index.html.

– Los criterios de normalización exponen pautas para la normalización de estas aplicaciones con el objetivo de facilitar la compatibilidad técnica, la disponibilidad, la interoperatividad y la conformidad con las normas nacionales e internacionales.

– Los criterios de conservación exponen los requisitos, criterios y recomendaciones para la conservación de la información en soporte electrónico de estas aplicaciones [20].

2.1. La seguridad en las relaciones telemáticas entre la Administración y los ciudadanos. El uso de la firma electrónica.

Como es bien conocido, Internet es un canal de comunicación configurado por múltiples redes interconectadas de acceso libre y con un carácter global. Internet ha sido diseñado como un sistema abierto para facilitar el intercambio de información, lo que ha ido en detrimento de la seguridad de las transacciones y la garantía de aspectos como la confidencialidad, la autenticidad o la integralidad de las comunicaciones.

Ante esta situación, son vigentes las palabras de MARTÍNEZ NADAL al afirmar que «[e]l impulso por parte de las Administraciones públicas de la utilización de las técnicas electrónicas, informáticas y telemáticas es un deseo del legislador que se traduce en un imperativo a la hora de garantizar la seguridad en el empleo de las mismas» [21].

Todo ello porque la extensión del uso de las tecnologías de la información y la comunicación en la Administración pública puede suponer riesgos para la seguridad de las transacciones. En particular, la utilización de las tecnologías de la información y la comunicación en la tramitación de los procedimientos administrativos puede provocar [22]:

– Que se suplanten el autor y la fuente del mensaje. Es el problema de la autoría de los mensajes electrónicos.

– Que se altere el mensaje, de forma accidental o maliciosa. Es el problema de la integridad de los mensajes electrónicos.

– Que niegue el emisor del mensaje haberlo transmitido o el destinatario haberlo recibido. Es el problema del rechazo en origen o en destino de los mensajes electrónicos.

---

20 Véase la Comunicación de la Comisión sobre la seguridad de las redes y de la información COM(2001)298 final y la Resolución del Consejo de 28 de enero de 2002, relativa a un enfoque común y a acciones específicas en materia de seguridad de las redes y de la información.

21 LAFUENTE, M. (2002): «El soporte electrónico en el procedimiento administrativo», en: BAÑO LEÓN, J.M.; CLIMENT BARBERÀ, J.: *Nuevas perspectivas del régimen local. Estudios en homenaje al profesor José María Boquera Oliver*. Valencia: Tirant lo Blanch.

22 MARTÍNEZ NADAL, A. (2001): *La firma electrónica* (2.ª edición), Madrid: Civitas, pág. 34.

– Que se haya leído el contenido del mensaje por una persona no autorizada. Es el problema de la confidencialidad de los mensajes electrónicos.

Estos extremos están garantizados en la *presencialidad* mediante la identificación del ciudadano interesado a través de, por ejemplo, la exhibición del documento nacional de identidad o el pasaporte [23], la constancia en papel de la información, así como su firma manuscrita [24]. Respecto al uso de la firma manuscrita es ilustrativa la STS de 3 de noviembre de 1997:

«La firma es el trazado gráfico, conteniendo habitualmente el nombre, los apellidos y la rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y virtualidad y obligarse con lo que en ellos se dice. Aunque la firma puede quedar reducida, sólo, a la rúbrica o consistir, exclusivamente, incluso, en otro trazado gráfico, o en iniciales, o en grafismos ilegibles, lo que la distingue es su habitualidad, como elemento vinculante de esa grafía o signo de su autor. Y, en general, su autografía u ologrfía, como vehículo que une a la persona firmante con lo consignado en el documento, debe ser manuscrita o de puño y letra del suscribiente, como muestra de la inmediatez y de la voluntariedad de la acción y del otorgamiento.»

Ahora bien, la firma manuscrita no es la única manera de acreditar estos extremos. Asimismo, lo ha reconocido la STS anteriormente citada:

«Pero la firma autógrafa no es la única manera de signar, pues hay otros mecanismos que, sin ser firma autógrafa, constituyen trazados gráficos, que asimismo conceden autoría y obligan. Así, las claves, los códigos, los signos y, en casos, los sellos con firmas en el sentido indicado. Y, por otra parte, la firma es un elemento muy importante del documento, pero, a veces, no esencial, en cuanto existen documentos sin forma que tienen valor probatorio (como son los asientos, registros, papeles domésticos y libros de los comerciantes).

En consecuencia, aunque, al igual que en el caso de los documentos comunes, puede haber documentos electrónicos sin firma, el documento electrónico (…) es firmable, en el sentido de que el requisito de la firma autógrafa o equivalente puede ser sustituido, por el lado de la criptografía, por medio de cifras, signos, códigos, barras, claves u otros atributos alfanuméricos que permitan asegurar la procedencia y veracidad de su autoría y autenticidad de su contenido.»

Por tanto, no hay inconveniente en poder utilizar los medios informáticos para conseguir esta misma finalidad siempre y cuando se disponga de sistemas de seguridad que permitan garantizar la fiabilidad de la comunicación transmitida, la constancia de la recepción de los documentos y la identidad de los interlocutores. De hecho, así lo ha confirmado el ordenamiento jurídico. Desde un punto

23 Artículos 9 y 10 de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana.

24 Respecto al valor probatorio de la firma manuscrita, véase, por ejemplo, ORMAZÁBAL, G. (2005): «El valor probatorio de la firma electrónica», en: PEGUERA, M. (coord.): *Derecho y nuevas tecnologías*, Barcelona: editorial UOC, págs. 52 y ss.

de vista genérico es interesante recordar como el artículo 45 de la LRJPAC, que es el artículo que con carácter básico establece los principios del uso de los medios informáticos y telemáticos por parte de las Administraciones públicas, establece la necesidad de garantizar la identificación y el ejercicio de la competencia por el órgano que lo ejerce y la autenticidad, integridad, conservación y, en su caso, recepción por el interesado, de los documentos electrónicos.

Pero, en particular, nos interesa destacar la regulación contenida en la Ley 59/2003, de 19 de diciembre, de firma electrónica (en adelante, LFE) [25]. Esta ley tiene por objeto transponer al ordenamiento jurídico español 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. No obstante, hay que observar que, de hecho, esta Directiva ya se había incorporado al ordenamiento jurídico español mediante el Real Decreto-Ley 4/1999, de 17 de septiembre [26].

La LFE se dicta, entre otros títulos, en ejercicio de la competencia estatal prevista en el artículo 149.1.18.ª de la CE relativa a las bases del régimen jurídico de las Administraciones públicas [27]. Esto ha permitido que hasta cuatro comunidades autónomas ya hayan aprobado normas que regulan la utilización de la firma electrónica por parte de la Administración autonómica [28].

En primer lugar, se puede destacar la ley de La Rioja, dado que se dirige a todas las Administraciones públicas de la comunidad autónoma y no únicamente a la autonómica [29].

En segundo lugar, en Cataluña también se ha regulado esta materia a través del Decreto 324/2001, de 4 de diciembre, relativo a las relaciones entre los ciudadanos y la Administración de la Generalitat de Cataluña a través de Internet. El Decreto 324/2001 establece un régimen jurídico aplicable diferente en función de que el procedimiento administrativo tramitado telemáticamente cuente con la utilización de certificados digitales o no. En particular se prevé en aquellos procedimientos en los que se requiera garantizar la autenticidad, la confidencialidad y la integridad [30].

---

25 BOE de 20 de diciembre de 2003.

26 Véase un análisis exhaustivo de esta normativa en MARTÍNEZ NADAL, A. (2001): *La firma electrónica* (2.ª edición), Madrid: Civitas.

27 Disposición derogatoria única de la LFE.

28 Decreto 205/2001, de 3 de diciembre, por el que se regula el uso de la firma electrónica en los procedimientos administrativos de la Administración Pública de la Comunidad Autónoma de Canarias y Decreto 87/2002, de 30 de mayo, del Gobierno Valenciano, por el que se regula la utilización de la firma electrónica avanzada en la Generalitat Valenciana.

29 Esta ley regula el uso de la firma electrónica a nivel de las Administraciones públicas de La Rioja incluyendo, por lo tanto, también las Administraciones locales.
Es interesante poner de relieve como esta ley prevé que los ciudadanos tienen derecho a: solicitar de las Administraciones públicas el uso del sistema de firma electrónica avanzada en los procedimiento en que actúen como interesados; utilizar el sistema de firma electrónica avanzada en aquellos procedimientos que hayan sido habilitados por la autoridad competente para ser tramitados con este sistema.
También se prevé que la Administración de la comunidad autónoma colaborará con las Administraciones locales, con todo aquello que requieran, en la implantación del sistema de firma electrónica avanzada (art. 2.3).
Finalmente, se establece que las Administraciones locales de La Rioja podrán establecer el procedimiento para el establecimiento de la firma electrónica mediante ordenanza.

30 Artículos 15 y 16 del Decreto 324/2001.

La firma electrónica es un mecanismo idóneo para garantizar las relaciones telemáticas entre las Administraciones públicas y los ciudadanos, ya que garantizan la identidad, la fiabilidad del contenido transmitido e, incluso, también las fechas y hora de envío y recepción. De hecho, tal y como establece la propia normativa sobre firma electrónica, ésta, siempre que disfrute de determinadas características, tendrá el mismo valor jurídico que la firma manuscrita. La firma electrónica es un conjunto de datos en forma electrónica que, consignados juntamente a otros datos o asociados a ellos, puede ser utilizada como medio de identificación del firmante.

Este concepto es el punto de partida recogido en la ley antes de introducir otros mecanismos que permiten dar mayor seguridad al sistema para garantizar no sólo la identidad del firmante sino también el contenido del mensaje. Por eso, la propia ley define a continuación la firma electrónica avanzada que es la firma que utiliza la técnica de la criptografía asimétrica, es decir, con un par de claves [31].

La LFE establece que la firma electrónica avanzada se caracteriza por permitir identificar al firmante y detectar cualquier modificación de los datos firmados, por estar vinculada al firmante de manera única y a los datos a que se refiere y por haber sido creada por medios que el firmante puede mantener bajo su exclusivo control. Posteriormente, la LFE prevé que la firma electrónica puede ser reconocida, lo que requiere que se base en un certificado reconocido y sea generada por un dispositivo seguro de creación de firma [32].

Con las tres primeras exigencias (identificación del firmante, creación por medios bajo su exclusivo control y vinculación única a él) lo que se pretende es garantizar la autenticación del autor y evitar el rechazo en origen de los mensajes electrónicos (es decir, que sea posible determinar su autoría y que el autor no pueda rechazarlo); y con el último requisito (vinculación a los datos que permite detectar cualquier alteración posterior) se pretende salvaguardar la integridad de los documentos electrónicos.

Una firma electrónica avanzada es, por lo tanto, un conjunto de caracteres que acompañan a un documento o un fichero, acreditando quién es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad).

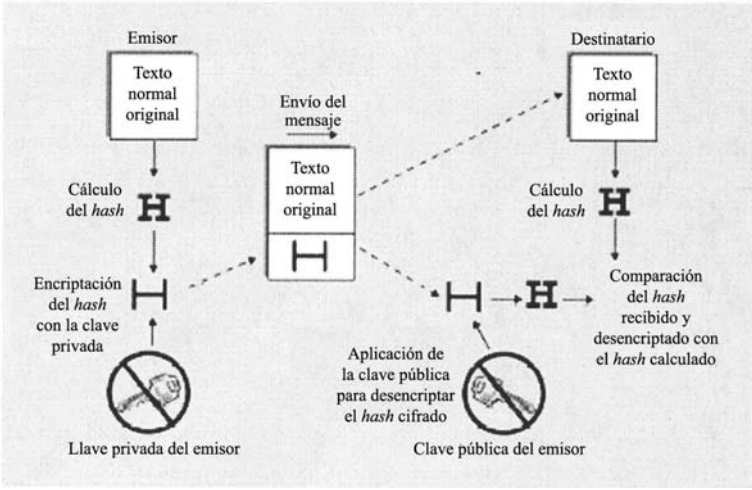
El proceso de firma electrónica parte del mensaje en claro que se encripta o cifra mediante la clave privada, que sólo es conocida por su titular y que tiene que mantenerla en secreto [33]. De hecho, se puede dar el caso de que no tenga conocimiento ya que puede estar incorporada a una tarjeta inteligente y únicamente se pueda acceder a ella mediante un código secreto o por un dispositivo de identificación biométrica. Mediante esta clave se produce un documento ininteligible que sólo se

31 Hay dos sistemas de firma electrónica: la firma simétrica o de llave única y la firma asimétrica o de par de llaves.

32 Artículo 3 de la LFE.

33 La LFE define que los datos de creación de firma son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica. Se considera como causa de extinción de la vigencia de un certificado electrónico la puesta en peligro del secreto de los datos de creación de firma del firmante (art. 8.1 LFE).

puede descifrar para obtener el texto en claro mediante otra clave, la clave pública, que es de conocimiento general y es puesta en conocimiento público mediante su inclusión en listados o directorios de acceso público en Internet [34]. La clave privada y la clave pública están relacionadas matemáticamente pero de manera que es virtualmente imposible que quien conoce la clave pública pueda derivar de ella la clave privada.



Fuente: Ormazábal (2005)

Ilustración : Proceso de firma electrónica asimétrica

Desde el punto de vista técnico se tiene que decir que no se cifra todo el mensaje, dado el alto coste en recursos que eso supondría. Por eso lo que se firma es un resumen del original (que no tendrá más de dos líneas, independientemente de la longitud del texto) creado de forma automática (*digest*). Es importante tener en cuenta que la modificación de cualquier parte del texto, aunque sólo sea un acento, genera un resumen diferente. Eso es lo que se conoce como algoritmo *hash* (mecanismo criptográfico irreversible que a partir de una entrada cualquiera genera una salida única de longitud constante) que es lo que finalmente se firma y que acompañará al documento original.

El receptor recibe el documento y la firma del *hash* y tiene que verificar la firma. Esta operación consiste en descifrar el *hash* firmado con la clave privada aplicando la clave pública y, por otra parte, aplicando la clave pública sobre todo el documento recibido. Cuando el *hash* recibido y descifrado y este segundo *hash* coincidan, el destinatario tendrá la seguridad de que el mensaje recibido ha sido firmado por su emisor y que tenía aquel contenido. En el caso de que no haya coincidencia tendrá que poner en duda estos extremos.

34 Según la LFE, los datos de verificación de firma son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma.

Con este sistema, el titular de la clave privada puede enviar mensajes y quien los recibe tiene la seguridad de que provienen de aquella persona. Al mismo tiempo, el receptor puede enviar al titular de la clave privada un mensaje cifrado con la clave pública que sólo podrá ser descifrado mediante la clave privada.

El proceso de creación de firma como la aplicación de los datos de verificación se realiza a través de los dispositivos de creación y verificación de firma [35]. Como se puede pensar, buena parte del sistema se basa en la seguridad que ofrezcan estos dispositivos que se utilizan en la firma electrónica. Por eso, los dispositivos de creación de firma tienen que ofrecer las siguientes garantías:

– Los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.

– Existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.

– Los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.

– El dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.

Con respecto a los dispositivos de verificación de firma, hará falta que:

– Los datos utilizados para verificar la firma correspondan a los datos mostrados a la persona que verifica la firma.

– La firma se verifique de forma fiable y el resultado de esa verificación se presente correctamente.

– La persona que verifica la firma electrónica pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.

– Se muestren correctamente tanto la identidad del firmante, o, en su caso, conste claramente la utilización de un seudónimo, como el resultado de la verificación.

– Se verifiquen de forma fiable la autenticidad y la validez del certificado electrónico correspondiente.

– Pueda detectarse cualquier cambio relativo a su seguridad.

35 Artículos 24 y 25 de la LFE.

La LFE establece que la firma electrónica reconocida tiene una eficacia jurídica consistente en la equiparación con la firma manuscrita tradicional. Es decir, si la firma cumple los requisitos necesarios para ser considerada como firma electrónica reconocida, tendrá con respecto a los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel [36]. Eso tiene más consecuencias ya que la firma electrónica puede incorporarse en un documento electrónico que tiene valor y eficacia jurídica y que será admitido como prueba en juicio [37].

No hay que decir, a estas alturas, que las Administraciones públicas pueden utilizar la firma electrónica. Ya el Real Decreto-Ley 14/1999 admitía la posibilidad de que las Administraciones públicas utilizasen la firma electrónica en sus relaciones con los ciudadanos. Además, se preveía que el Estado o las comunidades autónomas podían establecer las condiciones adicionales que se considerasen necesarias para salvaguardar las garantías de cada procedimiento.

La LFE confirma estos extremos al afirmar 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 ellas y en las relaciones que mantengan las Administraciones públicas entre ellas o con los ciudadanos [38]. Desde el punto de vista del procedimiento administrativo, es interesante poder observar cómo la firma electrónica puede utilizarse en las diferentes fases del procedimiento administrativo tramitado telemáticamente: en la presentación de solicitudes (art. 70 LRJPAC), para practicar las actuaciones de la instrucción de la manera más cómoda posible para los interesados (art. 85.1 LRJPAC), para la formulación de alegaciones y para la notificación de las resoluciones (art. 59 LRJPAC).

De acuerdo con la LFE, cuando las Administraciones públicas utilicen la firma electrónica pueden añadir más condiciones que las previstas para el resto de transacciones electrónicas. Entre estas condiciones se pueden incluir, por ejemplo, la imposición de datos electrónicos en los documentos electrónicos integrados en un expediente administrativo, es decir, un conjunto de datos en forma electrónica utilizados como medio para constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados.

Estas condiciones adicionales también tienen que garantizar lo que prevé el artículo 45 de la LRJPAC pero a su vez deben ser objetivas, proporcionadas, transparentes y no discriminatorias y no obstaculizar la prestación de servicios a los ciudadanos [39].

La utilización de firmas basadas en la criptografía asimétrica plantea el problema de una distribución fiable de las claves públicas. Para hacer frente a esta situación, la LFE da un paso más allá en

36 Artículo 3.4 de la LFE.

37 La LFE prevé que el documento electrónico puede ser soporte de documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas (art. 3.6 LFE).

38 Artículo 4.1 de la LFE.

39 Artículo 5.3 de la LFE.

la seguridad de la firma electrónica y establece el concepto de firma electrónica reconocida que es aquélla basada en un certificado reconocido y generado mediante un dispositivo seguro de creación de firma.

De acuerdo con el proceso de firma electrónica que se ha descrito anteriormente, cuando el receptor de un documento firmado electrónicamente quiere verificar su origen y contenido necesita tener la clave pública vinculada a la clave privada del firmante. En este proceso falta una fase que permite precisamente acreditar que la clave privada pertenece a quien dice que es su titular. Eso se podría hacer mediante el intercambio manual de las claves entre los interesados en un procedimiento o los firmantes de un contrato. Pero en tanto es obvio que estas opciones presentan desventajas ya que son poco prácticas y seguras. Por ello, se hace mediante la intervención de un tercero de confianza llamado también prestador de servicios de certificación o entidad de certificación que asegura la certeza sobre la relación entre la persona y su firma digital mediante la emisión de certificados electrónicos que son documentos firmados electrónicamente por los prestadores de servicios de certificación que vinculan unos datos de verificación de firma a un firmante y confirman su identidad [40].

La LFE regula detalladamente los certificados electrónicos [41]. En particular, la LFE contiene una serie de obligaciones mínimas para la emisión de certificados electrónicos (por ejemplo, obligaciones relativas a la protección de datos personales, seguridad o fiabilidad técnica). Estas condiciones pueden verse reforzadas con el fin de dotar el certificado de especiales garantías de seguridad, lo que da lugar al surgimiento de un certificado reconocido.

La LFE se refiere a los certificados reconocidos como aquellos certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en la ley con respecto a la comprobación de la identidad de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten. Entre otros datos, los certificados reconocidos incluirán la identificación del firmante y del prestador del servicio de certificación, los datos de verificación de firma que correspondan a los datos de creación de firma que estén bajo el control del firmante, el período de validez del certificado así como los límites que se puedan haber establecido.

Es importante recordar que para que la firma electrónica tenga los mismos efectos jurídicos que la firma manuscrita hace falta que ésta se base en un certificado reconocido.

Llaman especialmente la atención las obligaciones relativas a la comprobación de la identidad y circunstancias personales de los solicitantes del certificado reconocido, teniendo que personarse delante de los encargados, de verificarla y acreditarse con el DNI u otro medio admitido en derecho. Para el caso de personación en la solicitud de certificados que se expidan, previa identificación del solicitante ante las Administraciones públicas, se regirán por lo que establece la normativa administrativa [42].

40 Artículo 6.1 de la LFE.

41 Véase el Título II de la LFE relativo a los certificados electrónicos.

42 Artículo 13.1 de la LFE.

La expedición de los certificados la realizan los prestadores de los servicios de certificación. La prestación de los servicios de certificación no está sujeto a ninguna autorización previa y se realizará en régimen de libre competencia [43]. No obstante, se prevé toda una serie de intervenciones públicas en esta actividad. En primer lugar, se establece un conjunto de obligaciones a los prestadores de los servicios (por ejemplo, con respecto a la protección de los datos personales que precisen o a la información a los solicitantes sobre todo el proceso de certificación y las obligaciones del firmante) que se recogerán en una declaración de prácticas de certificación y que se verán incrementadas para los prestadores de servicios de certificación que expidan certificados reconocidos. En segundo lugar, se prevé un sistema de acreditación voluntaria de los prestadores que permitirá garantizar a los usuarios de los servicios unos determinados niveles de calidad y, por lo tanto, de seguridad [44]. En tercer lugar, se establece un sistema de supervisión de la actividad de los prestadores. Con eso se pretende controlar el cumplimiento de los requisitos relativos a esta actividad por parte de los prestadores del servicio. Para el caso de incumplimiento la LFE prevé, finalmente, un régimen sancionador.

El hecho de que el servicio de certificación se preste en régimen de libre competencia no es obstáculo para que las Administraciones públicas también puedan desarrollar esta importante tarea [45]. Las Administraciones públicas, o los organismos públicos o entidades dependientes o vinculadas a ellas, también pueden prestar el servicio de certificación y lo tienen que hacer bajo los principios de objetividad, transparencia y no discriminación [46].

Con respecto a las entidades públicas de prestación de servicios de certificación se pueden referenciar dos ejemplos: la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda [47] y la Agencia

43 Artículo 5.1 de la LFE.

44 En particular, el artículo 26 de la LFE prevé que la certificación de un prestador de servicios de certificación es el procedimiento voluntario por el que una entidad cualificada, pública o privada, emite una declaración a favor de un prestador de servicios de certificación, que implica un reconocimiento del cumplimiento de requisitos específicos en la prestación de los servicios que se ofrecen al público.

45 Véase, al respecto, el Real Decreto 1317/2001, de 30 de noviembre, por el que se desarrolla el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, en materia de prestación de servicios de seguridad por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, en las comunicaciones a través de medios electrónicos, informáticos y telemáticos con las Administraciones públicas.

46 Artículo 5.3 de la LFE.

47 El artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, en materia de prestación de servicios de seguridad preveía que la Fábrica Nacional de Moneda y Timbre (FNMT) podía prestar los servicios de certificación para garantizar la seguridad, validez y eficacia de las comunicaciones telemáticas que se produjesen entre los órganos de la Administración General del Estado y entre ellos y los ciudadanos. También se preveía la posibilidad de que la FNMT pudiera prestar estos servicios a las Comunidades Autónomas, los entes locales y entidades de derecho público dependientes de ellas. Este artículo destacaba que estos servicios se podían prestar también por otros prestadores de servicios de certificación. Esto se reitera en el Real Decreto 1317/2001, de 30 de noviembre, relativo a la prestación de servicios de seguridad en las comunicaciones de las Administraciones públicas a través de técnicas y medios electrónicos, informáticos y telemáticos. La FNMT puede convenir en régimen de libre concurrencia la prestación de los servicios de certificación con cualquier Administración pública. Éste ha sido el caso, por ejemplo, de la Diputación de Barcelona.

Catalana de Certificación [48]. El primero de ellos ha sido el que ha liderado la prestación de servicios de certificación para las Administraciones públicas en España durante bastante tiempo, y el segundo, a pesar de ser una iniciativa más reciente, está llamado a tener una importante relevancia en Cataluña dado que se crea en el marco del *Consorci per a l'Administració Oberta i Electrònica de Catalunya,* que es una entidad asociativa formada por la Generalitat de Cataluña y el Consorcio local Localret.

Finalmente, en el ámbito de las Administraciones públicas, hay que preguntarse si cuando se utiliza la firma electrónica en un procedimiento administrativo hace falta que se obtenga un certificado emitido por un prestador de servicios de certificación pública. En otras palabras, hay que preguntarse si, en las relaciones con la Administración pública, los ciudadanos pueden usar certificados obtenidos de prestadores de servicios de certificación privados. Desde un punto de vista general, ¿puede la Administración pública limitar los certificados que pueden usar a los ciudadanos al relacionarse con ella? [49]

La LFE establece que las Administraciones públicas podrán establecer las condiciones adicionales que se consideren necesarias. Ahora bien, como se ha observado anteriormente estas prescripciones adicionales hacen referencia a la salvaguardia de las garantías de cada procedimiento. Además, la propia norma establece que la prestación de los servicios de certificación por parte de las Administraciones públicas se tendrá que prestar de acuerdo con el principio de no discriminación y, por lo tanto, no parece que mientras los prestadores privados puedan garantizar las mismas condiciones que las entidades públicas sea razonable y justificado establecer de manera justificada esta posibilidad.

En particular, teniendo en cuenta que la obligación principal de los prestadores de servicios de certificación es la comprobación de la identidad del solicitante del certificado, una vez se haya

48 La Agencia Catalana de Certificación es un organismo autónomo de carácter comercial, con personalidad jurídica propia y pública, del Consorci per a l'Administració Oberta i Electrònica de Catalunya, con patrimonio independiente y plena capacidad jurídica, que tiene por objeto gestionar certificados digitales y prestar servicios relacionados con la firma electrónica y con los procesos de identificación necesarios a nivel de actuación de las administraciones públicas catalanas [Resolución PRE/2649/2002, de 16 de septiembre, por la cual se da publicidad a los Estatutos de la Agencia Catalana de Certificación (DOGC de 22 de septiembre de 2002)].
El conjunto de servicios ofrecidos por CATCert conforma el sistema público catalán de certificación, incluyendo los siguientes: servicios de certificación digital de certificados de clase 1 y clase 2, para certificados personales y de dispositivos; servicios de clasificación de proveedores de servicios de certificación y servicios complementarios; servicios de validación de firma electrónica y certificados digitales; servicios de sello de tiempo y servicios de archivo de documentos firmados. CATCert creó, el 8 de enero del 2003, una jerarquía de entidades de certificación, cuya raíz es la propia Agencia, de la que dependen una entidad de certificación para el mundo local y uno otra para la Generalitat. Asimismo, de esta última entidad depende la entidad de certificación de la Secretaría de Administración y Función Pública, que tiene que proveer de certificados digitales a los empleados públicos de la Generalitat de Cataluña que lo requieran.
A nivel local, la Agencia Catalana de Certificación ha llevado a cabo diferentes proyectos piloto para establecer el certificado del ciudadano (IdCAT) en municipios como Girona, Pont de Suert, Guissona, Sant Cugat, Manresa, Barcelona, Sabadell, Sant Feliu de Llobregat, Terrassa, Cornellà de Llobregat, Móra d'Ebre, Reus, Mataró, Sant Boi de Llobregat, Lleida y Santa Coloma de Gramenet. También se ha avanzado en la Diputación de Tarragona, la de Lleida y la de Barcelona, con las que se han suscrito convenios de reconocimiento.

49 Por ejemplo, la regulación de la presentación telemática de la declaración del IRPF prevé que el certificado requerido es exclusivamente el emitido por la FNMT.

personado ante los encargados de verificarla y que se haya acreditado mediante el documento nacional de identidad, el pasaporte o cualquier otro medio admitido en derecho y que, además, se establece como una infracción muy grave el incumplimiento de esta obligación con una sanción consistente en una multa comprendida entre los 150.001 y los 600.000 euros, parece oportuno concluir que no es necesario que esta tarea la pueda realizar, a los efectos que estamos comentando, únicamente un funcionario o empleado público.

BIBLIOGRAFÍA

AA.VV. (2003): *Firma digital y Administraciones Públicas*. Madrid: MAP.

Agència Catalana de Certificació. *Resum d'activitats de l'Agència Catalana de Certificació durant l'any 2003* (2003).

AGIRREAZKUENAGA, I; CHINCHILLA, C. (2001): «El uso de medios electrónicos, informáticos y telemáticos en el ámbito de las Administraciones Públicas», *Revista Española de Derecho Administrativo,* núm. 109.

BARNES VÁZQUEZ, J. (2000): «Una reflexión introductoria sobre el derecho administrativo y la Administración pública en la sociedad de la información», *Revista Andaluza de Administración Pública*, núm. 40.

BAUZÁ MARTORELL, F.J. (2002): *Procedimiento administrativo electrónico*. Granada: Comares.

CHEVALIER, J. (2002): «La mise en ouvre de l'Administration electronique», en: *Colloque International «L'Administration électronique au service des citoyens»*. París.

FERNÁNDEZ SALMERÓN, M. (2003): *La protección de los datos personales en las Administraciones públicas*. Madrid: Thomson-Civitas.

LAFUENTE, M. (2002): «El soporte electrónico en el procedimiento administrativo», en: BAÑO LEÓN, J.M.; CLIMENT BARBERÀ, J.: *Nuevas perspectivas del régimen local. Estudios en homenaje al profesor José María Boquera Oliver*. Valencia: Tirant lo Blanch.

MAJÓ, J. (1997): *Xips, cables i poder*. Barcelona: Ediuoc-Enciclopèdia Catalana.

MARTÍNEZ NADAL, A. (2001): *La firma electrónica* (2.ª edición). Madrid: Civitas.

OECD: «Engaging citizens online for better policy-making», *Policy Brief*, núm. marzo, 2003.

ORMAZÁBAL, G. (2005): «El valor probatorio de la firma electrónica», en: PEGUERA, M. (coord.): *Derecho y nuevas tecnologías*. Barcelona: Editorial UOC.

VALERO TORRIJOS, J. (2004): *El régimen jurídico de la e-Administración. El uso de medios informáticos y telemáticos en el procedimiento administrativo*, Granada: Comares.