tecnimap 2002
www.tecnimap.com
VII JORNADAS SOBRE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA MODERNIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS
A CORUÑA
15, 16, 17 y 18 de octubre de 2002
Palacio de Congresos y de la Ópera
Ponencias

El interesado en el Procedimiento Administrativo Electrónico. La escindibilidad de la firma electrónica.

Felio J. Bauzá Martorell.

1.- Identificación del interesado.

Mientras los art. 70 y 110 LRJPAC hacen referencia a la identificación del interesado o de la persona que lo represente, así como la firma del solicitante o acreditación de la autenticidad de su voluntad expresada por cualquier medio, por el contrario en sede electrónica el art. 7.2.b del RD 263/1996 se limita a exigir que "se identifique fidedignamente al remitente y al destinatario de la comunicación". Habrá que colegir, por consiguiente, que junto a la identificación del remitente en los supuestos de representación, habrá que dejar constancia en la comunicación electrónica de la identidad del representado. A mayor abundamiento, habrá que acreditar la voluntad del solicitante mediante un sistema de firma electrónica que, junto a la autenticidad del emisor de la comunicación, pueda acreditar la autenticidad del mensaje en los términos del art. 4.2 del RD 263/1996.

Los mecanismos de autenticación simple –aquella basada en mecanismos tradicionales de usuario y contraseña- resultan insuficientes para acreditar fidedignamente (art. 7.2) al interesado que se dirige a un órgano administrativo, en la medida que un tercero puede hacer uso de ellos con relativa facilidad. Por ello habrá que recurrir a la autenticación fuerte basada en la utilización de técnicas de criptografía asimétrica y en el uso de certificados electrónicos.

Ayuntamiento de A Coruña
XUNTA DE GALICIA

El dato de la autenticidad se garantiza con la firma electrónica, regulada en nuestro país en el Real Decreto Ley 14/1999, de 17 de septiembre[1], y definida en el apartado a del art. 2 de ese cuerpo legal como "el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge".

Tradicionalmente la forma de firmar electrónicamente un documento consiste en el cifrado de ese mensaje mediante una clave por parte del emisor, de manera que el sujeto receptor descifra el documento aplicando esa misma clave.

Este mecanismo de cifrado en el que los dos agentes de una comunicación utilizan la misma clave para cifrar y descifrar el mensaje se denomina simétrico. Gráficamente el cifrado mediante clave simétrica consiste en que el particular (A) que dirige una solicitud a un órgano administrativo (B), cifra ese mensaje aplicando la clave de común acuerdo con el órgano administrativo, que a su vez para hacer el escrito o solicitud inteligibles aplicará la misma clave.

Este mecanismo simétrico de firma electrónica no cumple los requisitos de las comunicaciones que dirigen los particulares a la Administración por cuanto el art. 70 LRJPAC exige no sólo la identificación del interesado en su apartado a, sino también la "firma del solicitante o acreditación de la autenticidad de su voluntad expresada por cualquier medio" en su apartado d.

El modo en que la telemática ha verificado la garantía de la integridad del mensaje, que –desde la vertiente que aquí nos interesa- se conecta con la acreditación de la autenticidad de la voluntad del interesado sin que haya sido manipulada, desde el punto de vista subjetivo y objetivo de la comunicación, consiste en la criptología asimétrica. Este sistema de firma electrónica se fundamenta en la utilización de dos claves asociadas matemáticamente, si bien del conocimiento de una no puede derivarse la otra. Una de estas dos claves es privada, conocida únicamente por su titular[2] , y la otra

1 *No vamos a referirnos in extenso sobre esta norma más que de forma instrumental, al objeto de aplicar la firma electrónica a las comunicaciones en la Administración. Para ello nos remitimos a los rigurosos estudios de la profesora A. MARTÍNEZ NADAL –La ley de firma electrónica, Civitas, Madrid, 2000; Comercio electrónico, firma digital y autoridades de certificación, Civitas, Madrid, 1998- de obligada lectura. Sí debemos traer a colación en este momento una característica de esta norma que consiste en su aprobación con carácter previo a la directiva europea que regula la firma electrónica –la Directiva 1999/93/CE del Parlamento Europeo y del Consejo sobre un marco comunitario para la firma electrónica, aprobada el 13 de diciembre de 1999 y publicada en el DOCE, serie L, número 13, de 19 de enero de 2000.*
Siendo así que en Derecho comunitario las directivas se conciben como normas de objetivos que los Estados miembros deben alcanzar utilizando los medios –en lo referente a la competencia central o territorial y a los instrumentos de transposición (ley o reglamento)- y que carecen de eficacia directa salvo la no transposición en plazo de la directiva al ordenamiento estatal o la transposición incorrecta de la misma, la aprobación de una norma estatal sobre una materia de competencia comunitaria –la necesidad, en este caso, de estimular el desarrollo del comercio electrónico al objeto de evitar la fragmentación del mercado único- es una decisión que puede originar contradicciones entre el ordenamiento estatal y el comunitario que se substanciarán de acuerdo con el principio comunitario de primacía.
2 *Puede que ese conocimiento sea meramente relativo. Con frecuencia la clave privada se almacenará en una tarjeta inteligente, o se accederá a ella mediante un número de identificación personal, o incluso mediante un dispositivo de identificación biométrica como el reconocimiento del iris o de la huella digital.*

pública, accesible por cualquier persona[3]. A mayor abundamiento, estas claves se combinan computacionalmente sobre un resumen de la comunicación –conocido como hash[4]- de manera que la autenticidad va asociada no sólo a la identificación del interesado (autenticidad), sino también a su voluntad (integridad): si el particular interesado cifra la comunicación –transformada en la secuencia de bits que es el hash- que dirige a la Administración con su clave privada, y el órgano administrativo descifra la comunicación aplicando la clave pública del interesado, se tiene la garantía de la autenticación y la integridad del mensaje.

Por consiguiente, si un particular desea dirigir una solicitud o escrito a un órgano administrativo, sólo necesita tener una pareja de claves que pueda utilizar para comunicarse de forma segura con cualquier órgano administrativo cuyo titular disponga a su vez de otra pareja de claves, sin que haga falta que el remitente y el destinatario intercambien previamente clave alguna[5]. El particular sólo necesita conocer la clave pública del titular del órgano administrativo al que dirige un escrito o solicitud para cifrar con la misma este último. Otra cosa es que, a los efectos de intentar asegurar que la clave pública de un titular le corresponde efectivamente a ese titular y no a otro, sea necesario asimismo contar con una tercera parte de confianza que acredite de forma fehaciente cuál es la clave pública de cada persona, que será el prestador de servicios de certificación[6].

Un documento se firma digitalmente si el extracto o resumen de la comunicación –hash- se cifra mediante la clave secreta del emisor, de suerte que el receptor del mensaje podrá acceder a él si sobre ese elemento cifrado se aplica la clave

__3__ Otra cosa es que la distribución de claves públicas deba incorporar un elemento de seguridad. En efecto, si nada impide que la distribución de claves públicas pueda hacerse manualmente, mediante el intercambio entre los dos sujetos de la comunicación, este sistema puede resultar poco operativo en comunidades amplias. Aún así, la seguridad en la distribución y en la custodia de la clave pública no es total, como tampoco existe una acreditación de que se ha hecho entrega de la clave pública ni de que la clave entregada es la que se dice que se ha entregado. Con el fin de evitar tener que cifrar la distribución de las claves mediante unas claves distintas y así sucesivamente, se arbitra un sistema de autoridad certificadora que interviene en el tráfico electrónico en calidad de tercera parte de confianza que proporciona un sistema de seguridad: emite un certificado que liga una clave pública con el sujeto del certificado y confirma que el eventual firmante identificado en el certificado tiene la correspondiente clave privada.

__4__ La Recomendación de la Unión Internacional de Telecomunicaciones UIT-T.X.810 (1995 S), relativa a Tecnología de la Información -Interconexión de sistemas abiertos- marcos de seguridad para sistemas abiertos: visión general, define en su página 3 al hash o resumen cifrado como la característica de un ítem de datos, por ejemplo un valor de comprobación criptográfico o el resultado de la ejecución de una función de cálculo unidireccional sobre lo datos, que es suficientemente peculiar del ítem de datos y que no es factible, mediante cálculo, hallar otro ítem de datos que posea las mismas características.

__5__ J.L. MATEO HERNÁNDEZ, La firma digital y las autoridades de certificación, en M.A. DAVARA RODRÍGUEZ (Coord.), Encuentros sobre Informática y Derecho 1999-2000. Aranzadi. Pamplona, 2000. Pág. 187 y ss.

__6__ El interesado que dirija una comunicación a la Administración, si tiene que cifrar esa comunicación con la clave pública del titular del órgano al que se dirige, necesita contar con un certificado que emite un prestador de servicios de certificación de que efectivamente esa clave pública corresponde a un determinado titular.
Como en la práctica no es viable que todos los usuarios estén certificados por la misma autoridad, surge la necesidad de que unas autoridades de certificación certifiquen a su vez a otras, bien de forma jerárquica o mediante certificaciones cruzadas entre autoridades del mismo nivel. La infraestructura necesaria para el uso de los sistemas de clave pública, incluyendo los prestadores de servicios de certificación, se llama Infraestructura de Clave Pública (Public Key Infraestructure (PKI)).

pública del emisor. Con esta fórmula sí existe una garantía total y absoluta de que el mensaje proviene de quien dice provenir y que su voluntad que transmite es esa y no otra.

Esta firma digital mediante un criptosistema asimétrico se recoge en el Real Decreto Ley 14/1999 bajo el concepto de firma electrónica avanzada y se define en su art. 2.b como "la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos".

Por consiguiente las peculiaridades propias de la firma electrónica, siempre que sea avanzada, serán conciliables con los requisitos que la LRJPAC exige para las comunicaciones ordinarias que los interesados dirigen a la Administración. La firma electrónica ordinaria –por el hecho de no encontrarse vinculada al autor ni al contenido del mensaje- es un concepto tan amplio que no permite garantizar material ni jurídicamente la autenticidad ni la integridad de una comunicación, requisitos de todo punto insoslayables en las comunicaciones dirigidas a la Administración por un elemental principio de seguridad jurídica[7].

2- El interesado en el procedimiento administrativo electrónico.

El concepto de interesado que recoge el art. 31 LRJPAC hace referencia a personas físicas y jurídicas. Por el contrario, el Real Decreto Ley sobre firma electrónica se refiere en su art. 2.c al signatario como "la persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa". Esta determinación desplaza en favor de la representación la intervención en el tráfico jurídico electrónico de las personas jurídicas. Si bien en ningún momento una persona jurídica abandonará la veste de interesado en un procedimiento administrativo en Derecho español, las comunicaciones electrónicas a un órgano administrativo

7 Prueba de la cualificación de la firma electrónica avanzada en materia de integridad y seguridad, es que el Real Decreto de 17 de diciembre de 1999, que aprueba las normas que regulan la contratación telefónica o electrónica en España, prevé la posibilidad de firmar el contrato de forma electrónica, si bien para que ésta tenga el mismo valor que la firma manuscrita, exige que esta firma electrónica sea avanzada. Sin utilizar este término, la Ley venezolana sobre Mensajes de Datos y Firmas Electrónicas en su art. 16 hace referencia a la firma electrónica avanzada cuando señala que "la firma electrónica que permita vincular al signatario con el mensaje de datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa".

deberá dirigirlas mediante un representante persona física que podrá actuar como consignatario. El Decreto Ley sobre firma electrónica vincula los datos de creación de firma –"códigos o claves criptográficas privadas que el signatario utiliza para crear la firma electrónica" (art. 2.d)- exclusivamente a las personas físicas.

Ahora bien, que el Derecho español reserve expresamente la condición de signatario a una persona física no significa que el ordenamiento jurídico prohiba a una persona jurídica la posibilidad de dirigir a la Administración comunicaciones electrónicas. Ciertamente el Real Decreto Ley 14/1999 en su art. 2.c se refiere al signatario como una persona física. De hecho en su art. 8, relativo a los requisitos que debe reunir un certificado reconocido, alude en su aptdo. e a la identificación del signatario "por su nombre y apellidos", sin que mencione la forma de identificar a las personas jurídicas como es la denominación social. Sólo permite de forma excepcional, bajo el sometimiento a un régimen específico, que una persona jurídica pueda ser signataria en las obligaciones tributarias siempre que así se desarrolle por el Ministerio de Hacienda (art. 5.3). Por el contrario, la Directiva no acota la cualidad de signatario a la persona física. Su art. 2.3 define como firmante a "la persona que está en posesión de un dispositivo de creación de firma y que actúa en su propio nombre o en el de la entidad o persona física o jurídica a la que representa". En este sentido, la Directiva no prohibe a la persona jurídica ser titular de un par de claves para operar en el tráfico jurídico electrónico, en su propio nombre o en representación de una persona física o incluso también jurídica.

Si bien la contradicción entre ambos subsectores del ordenamiento jurídico –estatal y comunitario- no es total, no hay que descartar la hipótesis de que una autoridad certificadora se niegue, con base en el art. 2.c del Real Decreto Ley 14/1999, a otorgar a una persona jurídica unos datos de creación de firma, y éste alegue ante la jurisdicción española la eficacia directa de la Directiva. Posiblemente los órganos jurisdiccionales españoles se vean obligados a formular ante el Tribunal de Justicia de las Comunidades Europeas una cuestión prejudicial de interpretación del art. 2.3 de la Directiva de acuerdo con lo previsto en el art. 177.b TUE. Es probable que hasta entonces esta polémica no se zanje[8].

8 *El Consejo Superior de Informática del Ministerio de Administraciones Públicas hace público un Proyecto de Criterios de seguridad, conservación y normalización de las aplicaciones para ejercicio de potestades (<<http://www.map.es/csi/pg5c10.htm>>) con una serie de recomendaciones relativas a la autenticidad. Si bien carecen de efectos jurídicos, interesa entrar a conocer la sensibilidad del CSI por los requisitos de orden subjetivo de las comunicaciones con medios electrónicos, informáticos y telemáticos en la Administración.*

3.- Escindibilidad de la firma electrónica.

Un problema de especial relevancia que se plantea en la firma electrónica –no así, como veremos, en la firma manuscrita- y que resulta vital en la relación jurídico-administrativa, consiste en la utilización de una clave privada ajena para firmar electrónicamente un documento en un proceso en el que no se reviste la condición de interesado. Ya sea como consecuencia de una autorización o de un uso indebido (descifre, sustracción de clave) existe una posibilidad cierta de utilizar la firma de una persona mediante criptosistemas por un tercero ajeno, fenómeno que se conoce como la escindibilidad de la firma electrónica.

Como advierte CAVANILLAS MÚGICA, el hecho informático añade nuevas patologías a la teoría del consentimiento: el error tecnológico es una de ellas (lo que se quiso emitir no coincide con lo que recibió el destinatario de la declaración de voluntad) y la suplantación informática es otra (el dispositivo técnico a través del cual una persona emite sus declaraciones de voluntad es empleado o es suplantado por una tercera persona, que se hace pasar por la primera)[9], y ello a pesar de las técnicas de control de identidad existentes que enumera GUERRA BALIC (tarjetas magnéticas, códigos secretos…)[10].

Siendo así que la firma electrónica participa de la naturaleza del sello, la utilización del mismo por cualquier persona permite firmar en nombre de su titular, de forma equivalente a la utilización de claves de acceso a un sistema informático, donde la garantía de que el sujeto que utiliza un clave es su titular no siempre es cierta. SÁNCHEZ BLANCO se refiere a este fenómeno cuando señala que "el correo electrónico genera la problemática de violación de correspondencia mediante el uso del password de otra persona que, a su vez, implica la suplantación de identidad"[11].

El acceso a los equipos informáticos y lógicos es una de las cuestiones más debatidas en las comunicaciones con medios técnicos y despiertan la sensibilidad del legislador. Las Directrices de la Comisión Europea sobre Mejores prácticas para la utilización de datos legibles por máquina (DLM) –establecidas por iniciativa de la Comisión en el marco del

9 *S. CAVANILLAS MÚGICA, Informática y teoría del contrato, en M.A. DAVARA RODRÍGUEZ (Coord.), Encuentros sobre Informática y Derecho 1996-1997. Aranzadi. Pamplona, 1997. Pág. 270.*

10 *J.T. GUERRA BALIC, La conclusión de los contratos por medios informáticos. Revista Informática y Derecho núm. 8. UNED (Centro Regional de Extremadura). Mérida, 1995.*

11 *A. SÁNCHEZ BLANCO, Internet. Sociedad, empresa y poderes públicos. Comares. Granada, 2000. Pág. 37.*

seguimiento de las conclusiones del Consejo Europeo de 17 de junio de 1994, en colaboración con expertos nacionales de los Estados miembros- prestan especial atención a los derechos de acceso como piedra angular de la autenticidad, la integridad y la confidencialidad de las comunicaciones con medios electrónicos, informáticos y telemáticos y sistematizan los diferentes niveles de acceso a la información electrónica que pueden tener los usuarios: acceso a la página de cubierta, acceso a parte o a la totalidad del documento y acceso para visualizar y/o para imprimir.

La Norma ISO 7498-2 define el control de acceso como un servicio de seguridad que previene el uso de un recurso sin la autorización respectiva, mientras que en España el Real Decreto 994/1999 se refiere al control de acceso como un mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos .

En nuestro país el Ministerio de Trabajo y Seguridad Social establece, mediante Orden de 17 de enero de 1996, el control de accesos al sistema informático de la Seguridad Social. Si bien esta norma vertebra el sistema de información de la Seguridad Social en torno a tres principios de configuración de la seguridad –confidencialidad, integridad y disponibilidad- no es menos cierto que en el control de acceso al sistema subyace un elemento de identificación, pues difícilmente se puede acreditar alguno de estos tres principios si no existe una garantía en la identidad del sujeto que accede al sistema. Prueba de ello es que en su art. 3.a la Orden Ministerial obliga a asignar a cada usuario un perfil de las posibilidades de acciones que puede realizar, restringido al ámbito exclusivo y concreto de sus funciones como gestor del sistema. Como igualmente esta afirmación se corresponde con la previsión establecida en el aptdo. b de este mismo precepto cuando exige que todos los usuarios autorizados a acceder al sistema deban quedar identificados y autentificados, de forma que en todo momento pueda conocerse el usuario y los motivos por los que se accedió a la correspondiente información contenida en el sistema.

Esta identificación se intenta conseguir hoy por hoy con una habilitación en forma de autorización que asigna a cada usuario una contraseña personal y un código de acceso, de manera que la Seguridad Social no puede sino presumir que la persona que accede al sistema con una contraseña y un código es el titular de los mismos sin que ello deba ser forzosamente cierto. La Orden se limita en su art. 6 a hacer responsable a cada usuario de todos los accesos que se realicen mediante el uso de su contraseña personal y del código de acceso que se le haya facilitado como medio de autorización, obligándole a mantener la custodia y secreto de la contraseña y a vigilar posibles usos ajenos.

Como se aprecia, este sistema no resuelve la posibilidad de que un tercero ajeno a la relación social puede acceder al sistema informático de la Seguridad Social. La Orden se limita a arbitrar en ese caso los mecanismos de responsabilidad administrativa y disciplinaria, pero no se cubre la laguna de seguridad de que el sistema adolece.

Lo mismo cabe decir de la firma electrónica y de la utilización de claves como forma de acceso. Siendo así que con frecuencia las claves del signatario se encuentran almacenadas en una tarjeta de banda magnética, el elemento de seguridad que incorpora la firma electrónica a las comunicaciones se puede burlar operando en el tráfico jurídico con la tarjeta correspondiente a otro titular. En este caso el certificado de la autoridad certificadora acreditará que la clave que se utiliza para cifrar una comunicación electrónica corresponde a un titular que en la práctica no será el signatario de esa comunicación y, sin embargo, se le atribuirán los efectos de la firma electrónica. Lo mismo se puede decir de la seguridad de las claves mediante un control de acceso a través de un número de identificación personal (PIN), más fácil de burlar si cabe que la utilización de tarjetas inteligentes.

Otra forma de acceso a los datos de creación de firma consiste en el uso de certificados que se alojan en el terminal informático (como el de la FNMT-RCM para las declaraciones tributarias telemáticas) y no en tarjetas, lo cual hace posible que un tercero opere en el correo electrónico de un titular del certificado de usuario y se identifique en el tráfico jurídico como este último.

Sólo la seguridad del par de claves a través de un dispositivo de identificación biométrica[12] puede resultar idóneo para asegurar que el signatario de un documento mediante una clave es el titular de la misma, sin perjuicio de que la huella biométrica exclusivamente garantice el acceso al sistema informático, de manera que en modo alguno acreditará que el uso posterior al acceso es el que se dice ser[13].

La escindibilidad de la firma electrónica cuestiona dos de las cualidades que tradicionalmente se han predicado de la criptología: la autenticación de origen y la irrefutabilidad de origen. Con la utilización de claves ajenas, ya no será posible afirmar que el emisor del mensaje es quien dice ser, como tampoco resultará imposible negar que se ha remitido una comunicación a un destinatario.

12 *Los denominados sistemas inteligentes de identificación y control de las personas hacen acopio de mecanismos biométricos de identificación personal: las huellas dactilares, que se utilizan como llave de acceso a sistemas informáticos; el reconocimiento del iris, en el sentido de que cada persona posee una distribución única de los músculos que cierran la pupila y una pigmentación exclusiva que da color a los ojos, de manera que el iris permitiría identificar a una persona aun tapándole los ojos con un antifaz o un velo; y el reconocimiento automático del rostro, según el cual un programa informático analiza puntos clave de una cara y mide las distancias y curvas entre ellos. Sobre biometría, vid. A. K. JAIN, R. BOLLE, S. PANKANTI, Biometrics: personal identification in networked society. Kluwer Academic. Boston, 1999. S. LIU y M. SILVERMAN, A practical guide to Biometric Security Technology. IEEE Computer Society, IT Pro-Security. 2001. S. PANKATI, S. PRABHAKAR y A. JAIN. On the individually of Fingerprints. 2001. Para más información, vid. <<www.biometrics.org>> del Biometric Consrtium y <<www.biometricgroup.comunicación>> del International Biometric Group.*

13 *Daniel Ricardo Altmark sistematiza en tres categorías las técnicas de autenticación del documento electrónico: el código secreto o código de impresión (PIN), la criptografía y la biometría. D.R. ALTMARK, Valor jurídico del documento electrónico en el Derecho Argentino, cit. por V. CARRASCOSA LÓPEZ, Informática y Derecho núm. 8. 1995. Pág. 166-167.*

CASTAÑO SUÁREZ interpreta el art. 6 del Real Decreto 263/1996 en el sentido de exigir la autenticidad exclusivamente en los documentos electrónicos emitidos por la Administración General del Estado y no así en comunicaciones de los particulares[14], extremo que no compartimos. Bien es cierto que este precepto in fine exige que los códigos u otros sistemas de identificación en los documentos emitidos por los órganos de la Administración General del Estado o por sus entidades vinculadas o dependientes estén protegidos de forma que únicamente puedan ser utilizados por las personas autorizadas por razón de sus competencias o funciones, mientras que nada dice respecto de los códigos que vayan a utilizar los particulares en sus comunicaciones con la Administración con medios electrónicos, informáticos y telemáticos.

Sin embargo, no parece que de ello haya que extraer un tratamiento más liviano de la autenticidad en función del sujeto que emite un documento. Por el contrario, este precepto trata de garantizar que la persona que firma un documento en nombre de un órgano administrativo es la que está habilitada para representar a ese órgano y no otra, particularidad que no se materializa en las comunicaciones de los particulares. Que los códigos identificativos de los particulares no estén protegidos "de forma que únicamente puedan ser utilizados por las personas autorizadas por razón de sus competencias o funciones" no es óbice para entender que estos códigos deban ser computacionalmente aptos para garantizar la autenticidad del particular que se relaciona con la Administración en sede electrónica. Es más, el párrafo primero del art. 6.1 condiciona la validez de los documentos –no sólo de los órganos y entidades de la Administración General del Estado- sino también de los particulares a que quede acreditada, entre otras cuestiones, la identidad del autor y la autenticidad de su voluntad.

El legislador ejerce especial énfasis en la equiparación de la firma electrónica avanzada y la firma manuscrita (art. 3 del Real Decreto Ley 14/1999 y art. 5 de la Directiva 1999/93) cuando esa equiparación no es absoluta por las limitaciones que afectan a la firma electrónica. Ciertamente la firma manuscrita es inseparable de la persona y cumple una función no sólo identificadora del autor de la comunicación sino acreditativa de su voluntad. Por el contrario la firma electrónica es un mecanismo separado de la persona y por consiguiente puede ser utilizado por otra distinta del titular. El dato de la escindibilidad contradice la definición que ILLESCAS ORTIZ otorga a la firma electrónica como "instrumento cierto de atribución de paternidad de una declaración de voluntad o ciencia"[15]. En puridad, al decir de BOLÁS

14 R. CASTAÑO SUÁREZ, El Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, en M. A. DAVARA RODRÍGUEZ (Coord.), X Encuentros sobre Informática y Derecho 1996-1997. Aranzadi, 1997. pág. 417.
15 R. ILLESCAS ORTIZ, La firma electrónica y el Real Decreto Ley 14/1999, de 17 de septiembre. Derecho de los Negocios, 2. Octubre, 1999.

ALFONSO, la firma electrónica no garantiza que una persona concreta haya firmado un documento sino que la firma utilizada se encuentra registrada a su nombre[16]. Por este mismo motivo habrá que admitir que, si la firma manuscrita implica forzosamente que el firmante vive al tiempo de estamparla, nada impide que una persona fallecida pueda firmar electrónicamente un documento.

Todo lo más, la insuficiencia de la firma electrónica para garantizar la autenticidad de las comunicaciones deberá completarse con otros medios para acreditar la autoría del mensaje: el testimonio para demostrar el origen del mensaje o la prueba de exhibición de documentos. Si la identificación del interesado que se relaciona telemáticamente con la Administración descansa sobre una tercera parte de confianza, la colaboración de la autoridad certificadora se muestra insuficiente y exige su extensión al origen del mensaje para asegurar la completa identificación del particular que dirige una solicitud o escrito a un órgano administrativo en soporte magnético.

Esta dificultad en la equiparación entre la firma manuscrita y la firma electrónica se traslada a la eficacia probatoria de los documentos en soporte papel y en soporte magnético. El art. 23 del Proyecto de Ley de Servicios de Sociedad de la Información y de Comercio Electrónico de 8 de febrero de 2002 somete la prueba de la celebración de un contrato por vía electrónica a las reglas generales del Ordenamiento jurídico y a lo dispuesto en la legislación sobre firma electrónica, si bien el régimen jurídico de la firma electrónica no garantiza los requisitos generales del Ordenamiento jurídico en materia de identidad y autenticidad.

Como decimos, la utilización de la firma ajena, con o sin consentimiento del que formalmente firma, por parte del que materialmente rubrica no tiene sentido en la firma manuscrita. El ordenamiento arbitra soluciones para intervenir en el tráfico jurídico a través de otro –la representación (art. 32 LRJPAC)- o para declarar nulos los actos que sean constitutivos de delito (art. 62.1.d LRJPAC)- en este caso, la falsificación de la firma de una persona tipificada en el Capítulo II del Título XVIII del Código Penal, relativo a las falsedades documentales.

Por el contrario, el mecanismo de la firma electrónica hace posible que, en las comunicaciones dirigidas a la Administración, se pueda suplantar la personalidad del titular de una clave privada, convirtiendo en innecesaria la institución de la representación.

Un sector de la doctrina administrativista encabezado por LLISET BORRELL entiende que, dada la dificultad de acreditar la autenticidad en las comunicaciones electrónicas, nada obsta a que los nuevos medios técnicos puedan iniciar con

16 *J. BOLÁS ALFONSO, Firma electrónica, comercio electrónico y firma electrónica pública notarial. Revista Jurídica del Notariado. Octubre-diciembre 2000. Pág. 42.*

plena eficacia un procedimiento, bajo la condición resolutoria de que después se complete el sistema sustituyéndolo por el tradicional medio escrito[17], solución que nos parece poco ambiciosa. Hacer depender la eficacia de un documento telemático del mismo escrito en soporte papel equivale a negar que las comunicaciones en soporte magnético surtan efectos.

La escindibilidad de la firma electrónica arranca de la naturaleza de la firma digital basada en la criptología, que no es otra –al decir de TENA ARREGUI y DE LA NUEZ SÁNCHEZ-CASADO- que la recuperación del concepto de sello[18]: siendo así que el sello es el resultado de una combinación entre la firma manuscrita y el poder al portador, "la firma electrónica vendría a equipararse a una especie de sello que, llevando implícito el consentimiento de su titular, puede ser utilizado por cualquiera".

Esta habilitación de poder que puede plantear la firma electrónica genera inseguridad jurídica y puede desembocar en una conflictividad sin precedentes cuando el ordenamiento establece una presunción –prácticamente iuris et de iure- de que el signatario de un documento es el titular de la clave privada con que el mismo se cifra. Al decir de RODRÍGUEZ ADRADOS, "para que la firma digital valiese como firma habría que demostrar que fue el titular mismo quien utilizó la clave privada; y como esta prueba es imposible, la firma digital no puede considerarse declaración de su voluntad"[19].

Sea como fuere, la autenticidad de la voluntad del interesado que el art. 70 LRJPAC exige que se acredite en los documentos que éste dirige a un órgano administrativo no queda garantizada mediante la criptología, en la medida en que la autenticidad que garantiza la firma electrónica no se corresponde necesariamente con la identidad del autor de la firma ni del documento que se firma, de manera que el Real Decreto Ley 14/1999 se limita a presumir que el contenido de la comunicación se corresponde con la voluntad del interesado.

Sin perjuicio de lo que más adelante concluimos en materia de validez y eficacia de estas comunicaciones en soporte electrónico, informático o telemático, esta presunción puede desencadenar unas consecuencias jurídicas en clave de inseguridad toda vez las comunicaciones públicas en soporte electrónico serán revocables, de suerte que la inseguridad no será sólo jurídica sino también técnica y material. Piénsese por ejemplo en la utilización de la clave privada por

17 *F. LLISET BORELL y otros, Régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común: comentarios a la Ley 30/1992 y su conexión con el Régimen Local. Abella. El Consultor de los Ayuntamientos y Juzgados. Madrid, 1994. Pág. 233.*
18 *R. TENA ARREGUI y E. DE LA NUEZ SÁNCHEZ-CASADO, La firma electrónica, ¿un poder al portador? Diario LA LEY núm. 5.340. Jueves, 28 de junio de 2001.*
19 *A. RODRÍGUEZ ADRADOS, La firma electrónica. Revista Jurídica del Notariado. Julio-septiembre 2000. Pág. 174.*

un tercero que ejerce de signatario de la comunicación sin consentimiento de su titular: el órgano administrativo destinatario incurrirá en un acto administrativo inválido de admisión de esa comunicación, nulidad que se contaminará a los subsiguientes actos de trámite encadenados al anterior. Para declarar la nulidad del acto administrativo, que no habrá tenido efectos, al titular y supuesto signatario le corresponderá la carga de la prueba de que él no ha firmado electrónicamente esa comunicación, prueba que parece igualmente imposible.

Al mismo tiempo huelga decir que con la utilización de una clave sin consentimiento de titular se incurre en responsabilidad patrimonial, al margen de la penal, frente a terceros que habrá que residenciar en el titular de la clave por su negligencia en la custodia de la misma, o en el prestador de servicios por negligencia en no impedir el descifre de la clave[20], y quién sabe, posiblemente en la propia Administración dada la naturaleza objetiva sin necesidad de culpa de la responsabilidad que diseña la Ley 30/1992.

Por otra parte, si la firma se utilizara con consentimiento de su titular, la comunicación que un tercero dirigiera a la Administración tendría validez y eficacia, siendo posible que el tercero que hace uso de la firma de otro pueda ceder a su vez la clave a otro signatario y así sucesivamente, extremo equivalente al otorgamiento de una escritura de poder general a favor del que en cada momento resulte tenedor del documento. En todos estos casos, al existir consentimiento del titular de la clave privada, habrá que aceptar la validez y eficacia de la comunicación que un tercero –en calidad de signatario real del titular/signatario formal- dirija a un órgano administrativo.

Si tanto la Directiva 1999/93 como el Real Decreto Ley 14/1999 pretenden residenciar los efectos de la firma electrónica en el régimen general de los contratos y obligaciones, no podemos concluir de otra forma sino asumiendo la presunción de que el signatario se corresponde con el titular del par de claves, que en caso de que exista consentimiento habrá que admitir la validez de las comunicaciones, y, en caso contrario, habrá que declarar nulos los actos encadenados a esa comunicación y depurar responsabilidades frente a terceros. Como afirman TENA ARREGUI y DE LA NUEZ SÁNCHEZ-CASADO, "la aplicación de las reglas generales del mandato a un título al portador crea este efecto de rueda loca, al crear un título de legitimación incontrolable tanto en su ámbito como en el número y caracterización de los apoderados".

20 *A. GARCÍA CAMPO, La contratación electrónica. Aspectos jurídicos, en M.A. DAVARA RODRÍGUEZ (Coord.), Encuentros sobre Informática y Derecho 1994-1995. Aranzadi. Pamplona, 1995. Pág. 65.*

En materia de medios electrónicos de pago en el contexto del mercado interior europeo, la CEE en su Recomendación de 17 de noviembre de 1988 puso de relieve la necesidad de que los pagos ordenados mediante la tecnología de las comunicaciones fueran irrevocables, consecuencia lógica del carácter objetivo del pago electrónico. Esa irrevocabilidad, como garantía de seguridad jurídica, habrá que extrapolarla al conjunto de las comunicaciones con medios electrónicos, informáticos y telemáticos, que sólo admitirán excepción por motivos de legalidad (revisión de oficio y declaración de lesividad) o de oportunidad (revocación). Pues bien, si la técnica no encuentra solución a la escindibilidad de la firma electrónica, la revocabilidad de los actos administrativos se convertirá en moneda corriente en el tráfico electrónico administrativo hasta el punto de que siempre planeará sobre un acto o resolución el fantasma de su invalidez y de la declaración de no haber surtido efectos (nulidad) o de paralizar los efectos del acto o resolución (anulabilidad).

En definitiva, si –como venimos diciendo- la eficacia probatoria del documento generado con medios electrónicos, informáticos y telemáticos se reconduce al reconocimiento judicial, de la misma manera será un órgano jurisdiccional el que deberá confirmar o no la presunción de que el firmante electrónico de un documento es el titular de la clave con que ese documento aparece firmado. Posiblemente en esta sede haya que traer a colación lo previsto para los documentos privados en el art. 1.226 del Código Civil cuando señala que "aquel a quien se oponga en juicio una obligación por escrito que aparezca firmada por él, está obligado a declarar si la firma es o no suya".

Con ello se traslada la eficacia –y, en parte, la validez de las comunicaciones dirigidas a la Administración con medios electrónicos, informáticos y telemáticos al fallo judicial que un juzgado o tribunal puede elaborar al cabo de meses o años de haberse practicado la comunicación, de manera que la relación jurídico-administrativa con medios técnicos se convierte en inviable.