C-350

Panamá, 19 de noviembre de 2002.

Ingeniero
Laurencio Guardia
Director General del Instituto de Acueductos y
Alcantarillados Nacionales (IDAAN)
E. S. D.

Señor Director General:

Con agrado le brindo mi parecer jurídico a su c*onsulta administrativa* del 23 de septiembre del 2002, identificada nota No.2523. Esta *"consulta"* dice relación con la interpretación específica de la Ley 6 de 2002, mejor conocida como Ley de Transparencia, y la Ley 11 de 1998, sobre almacenamiento tecnológico de documentos oficiales.

Los hechos

En su consulta se hace una descripción de algunos hechos relacionados con la interrogante jurídica de su despacho. De la misma resaltan los siguientes elementos:

1. En su gestión cotidiana, la Administración del Instituto de Acueductos y Alcantarillados Nacionales (en lo sucesivo el IDAAN), ha tenido como política institucional conservar las discusiones de las reuniones de la Junta Directiva en soporte de cintas magnéticas, mejor conocidas como casetes.
2. Esta información parece haber sido declarada por la propia institución como de acceso restringido, por guardar relación con la discusión de las estrategias comerciales, financieras y operativas de esa Institución.
3. Hoy en día se tiene la duda de si en el IDAAN esa información, guardada en soporte magnético debería ser conservada y custodiada porque ellas tienen relación con los antecedentes de las decisiones de la entidad.
4. El instrumento legal que obligaría a guardar esa información lo es la Ley 11 de 1998, por la cual se regula el almacenamiento tecnológico de documentos".

La consulta.

Estamos frente a una solicitud de opinión jurídica, sobre un caso específico. No obstante, no se nos permite conocer cuál es la interpretación de los abogados del IDAAN, respecto del posible derecho aplicable, y no se menciona de manera específica a las normas concretas que regulan la materia.

En todo caso el IDAAN explica, aunque de manera general y sin referirse a una norma concreta[1], que se encuentran ante la duda al no saber si la información contenida en casetes (la cual presumen es información de carácter reservado), debe ser conservada o no.

Consideración Previa

Al no contar con una especificación conceptual de parte del consultante, nos limitaremos a confrontar la validez de las normas especiales que regulan la información pública.

Opinión de la Procuraduría de la Administración.

Para dar respuesta a su duda, tocaremos el tema de la interpretación de la ley general sobre información pública y los fines o cometidos perseguidos por la ordenación del procedimiento administrativo general al exigir la conservación de los antecedentes de la decisión administrativa. Para ello reproduciremos la norma directamente aplicable.

Derecho aplicable.

<u>En la Ley 6 de 2002.</u>

> "**Artículo 14**. La información definida por esta Ley como de acceso restringido no se podrá divulgar, por un periodo de diez años, contado a partir de su clasificación como tal, salvo que antes del cumplimiento del periodo de restricción dejen de existir las razones que justificaban su acceso restringido.
>
> Se considerará de acceso restringido, cuando así sea declarado por el funcionario competente, de acuerdo con la presente Ley:
>
> 1. La información relativa a la seguridad nacional, manejada por los estamentos de seguridad.
>
> 2. Los secretos comerciales o la información comercial de carácter confidencial, obtenidos por el Estado, producto de la regulación de actividades económicas.
>
> 3. Los asuntos relacionados con procesos o jurisdiccionales adelantados por el Ministerio Público y el Órgano Judicial, los cuales sólo son accesibles para las partes del proceso, hasta que queden ejecutoriados.

[1] Explicación esta que a la luz del artículo 6 de la Ley 38 de 2000 es importante, para que el dictamen de la Procuraduría de la Administración, incida en una solución concreta.

4. La información que versa sobre procesos investigativos realizados por el Ministerio Público, la Fuerza Pública, la Policía Técnica Judicial, la Dirección General de Aduanas, el Consejo Nacional de Seguridad y Defensa, la Dirección de Responsabilidad Patrimonial de la Contraloría General de la República, la Dirección de Análisis Financiero para la Prevención de Blanqueo de Capitales, la Comisión de Libre Competencia y Asuntos del Consumidor y el Ente Regulador de los Servicios Públicos.

5. La información sobre existencia de yacimientos minerales y petrolíferos.

6. Las memorias, notas, correspondencia y los documentos relacionados con negociaciones diplomáticas, comerciales o internacionales de cualquier índole.

7. Los documentos, archivos y transcripciones que naciones amigas proporcionen al país en investigaciones penales, policivas o de otra naturaleza.

8. Las actas, notas, archivos y otros registros o constancias de las discusiones o actividades del Consejo de Gabinete, del Presidente o Vicepresidentes de la República, con excepción de aquellas correspondientes a discusiones o actividades relacionadas con las aprobaciones de los contratos.

9. La transcripción de las reuniones e información obtenida por las Comisiones de la Asamblea Legislativa, cuando se reúnan en el ejercicio de sus funciones fiscalizadoras para recabar información que podría estar incluida en los numerales anteriores.

En caso de que las autoridades correspondientes consideren que deba continuarse el carácter de restringido de la información detallada en este artículo, corresponderá a los Órganos Ejecutivo, Legislativo o Judicial, según sea el caso, emitir resoluciones por las cuales se prorrogará hasta por un máximo de diez años adicionales, la restricción sobre la información mencionada en este artículo. En ningún caso el carácter de restringido podrá superar los veinte años, contados a partir de la primera clasificación, procediendo la divulgación de la información si antes del cumplimiento del periodo de restricción adicional dejaren de existir las razones que justificaban tal acceso restringido.

El proceso de terminación de la restricción al acceso de la información opera de pleno derecho por el solo transcurso del tiempo, sin necesidad de resolución o acto administrativo alguno.

En caso de que exista un documento que contenga en forma parcial información cuyo acceso se encuentre restringido en los términos de este artículo, deberá proporcionarse el resto de la información que no esté exceptuada".

"Artículo 16. Las instituciones del Estado que nieguen el otorgamiento de una información por considerarla de carácter confidencial o de acceso restringido, deberán hacerlo a través de resolución motivada, estableciendo las razones en que fundamentan la negación y que se sustenten en esta Ley".

<u>En la Ley 38 de 2000.</u>

"**Artículo 70:** Al expediente sólo tienen acceso, además de los funcionarios encargados de su tramitación, las partes interesadas, sus apoderados, los pasantes de éstos, debidamente acreditados por escrito ante el despacho, y los abogados, sin perjuicio del derecho de terceros interesados en examinar el expediente u obtener copias autenticadas o certificaciones de la autoridad respectiva, siempre que no se trate de información confidencial o de reserva que obedezca a razones de interés público, o que pueda afectar la honra o el prestigio de las partes interesadas, conforme a las disposiciones legales vigentes.

Cuando se trate de obtener copias de documentos o certificaciones que versan sobre información confidencial, aquéllas se emitirán únicamente a solicitud de autoridad, del Ministerio Público, de los tribunales o de cualquier dependencia estatal que haga constar que la requiere para tramitar o resolver asunto de su competencia, en cuyo caso dicha autoridad debe cuidar que la información se maneje con igual carácter.

La calificación de confidencialidad de una información deberá ser objetiva y ceñirse a las condiciones establecidas en leyes vigentes. El funcionario no podrá negarse a dar una información, so pretexto de que es confidencial o de acceso restringido, si ésta no se encuentra previamente clasificada como información confidencial o de acceso restringido, en normas legales vigentes".

(Modificado por la Ley No. 45 de 27 de noviembre de 2000, publicado en la Gaceta Oficial No. 24,191.)

El glosario de la Ley 38 de 2000.

Al momento de interpretar una norma es muy importante que se tenga referentes o definiciones que más o menos nos indiquen el sentido y alcance de los términos empleado. Esta cuestión es por lo regular olvidada por el legislador o los funcionarios, al momento de dictar o desarrollar las leyes. La forma de ayudar al intérprete a saber cuál es el significado específico de una determinada terminología técnica, es a través de los llamados glosarios.

Los glosarios tienen la finalidad de orientar, educar, despejar dudas, facilitar la interpretación y mejorar la aplicación del derecho escrito.

En el glosario de la Ley 38 de 2000, se pueden inferir ideas para interpretar en debida forma el alcance y sentido del artículo 70. Veamos:

"Artículo 201. Los siguientes términos utilizados en esta Ley y sus reglamentos, deben ser entendidos conforme a este glosario:

1. Acto administrativo. Declaración emitida o acuerdo de voluntad celebrado, conforme a derecho, por una autoridad u organismo público en ejercicio de una función administrativa del Estado, para crear, modificar, transmitir o extinguir una relación jurídica que en algún aspecto queda regida por el Derecho Administrativo.

Todo acto administrativo deberá formarse respetando sus elementos esenciales: competencia, salvo que ésta sea delegable o proceda la sustitución; objeto, el cual debe ser * lícito y físicamente posible; finalidad, que debe estar acorde con el ordenamiento jurídico y no encubrir otros propósitos públicos y privados distintos,

de la relación jurídica de que se trate; causa, relacionada con los hechos, antecedentes y el derecho aplicable; motivación, comprensiva del conjunto de factores de hecho y de derecho que fundamentan la decisión; procedimiento, que consiste en el cumplimiento de los trámites previstos por el ordenamiento jurídico y los que surjan implícitos para su emisión; y forma, debe plasmarse por escrito, salvo las excepciones de la ley, indicándose expresamente el lugar de expedición, fecha y autoridad que lo emite.

2. Actuaciones. Conjunto de actos, diligencias y trámites que integran un expediente, pleito o proceso en la esfera gubernativa. También se conoce como actuaciones a todas las tramitaciones que constituyen las piezas del expediente, redactadas durante el desarrollo del proceso.

44. Expediente. Conjunto de papeles, documentos y otras pruebas que pertenecen a un asunto o negocio, acopiado a consecuencia de una petición de parte u oficiosamente por la administración por razones de interés público.

57. Información confidencial o de reserva. Aquélla de acceso restringido que, por razones de interés público o particular, no puede ser difundida, porque podría ocasionar graves perjuicios a la sociedad, al Estado o a la persona respectiva, como es el caso concerniente a las negociaciones de tratados y convenios internacionales, seguridad nacional, situación de salud, ideas políticas, estado civil, inclinación sexual, antecedentes penales y policivos, cuentas bancarias y otras de naturaleza similar, que tengan ese carácter de acuerdo con una disposición legal.

102. Secretario o Secretaria del Despacho. Funcionario adscrito al despacho público o autoridad encargada de resolver un proceso administrativo, entre cuyas funciones principales están: custodiar y velar por la protección adecuada de los documentos, papeles y pruebas del proceso e instrumentos en general utilizados en la oficina, relacionados con la tramitación de los asuntos; autorizar con su firma entera, debajo de la cual expresará su cargo, todas las declaraciones, notificaciones, copias, diligencias y comisiones; llevar o encargar a quien corresponda la foliación correcta de los expedientes; mantener un archivo ordenado y confiable de éstos; informar a las personas interesadas, abogados o pasantes, el estado de los expedientes de su incumbencia que cursen en el despacho; hacer las notificaciones personales o por medio de un funcionario del despacho y las demás establecidas en esta Ley. Quien haga las veces de Secretario o Secretaria, asume estos deberes.

En la Ley 11 de 1998.

"**Artículo 5.** Las películas, reproducciones, microfichas, discos o certificaciones públicas, que han resultado de la utilización de algún sistema de almacenamiento tecnológico permitido por esta Ley, serán autenticados por el jefe del respectivo archivo u oficina pública o privada que ostenta la custodia".

"**Artículo 6.** Los originales de los documentos sujetos al sistema de almacenamiento tecnológico, deber reposar en los archivos de las respectivas oficinas públicas o privada en un lugar seguro, hasta que puedan ser depurados de acuerdo con las reglas técnicas, que para tal efecto reglamente el Órgano Ejecutivo".

"**Artículo 7.** Los documentos almacenados tecnológicamente conforme a esta Ley, constituyen un principio de prueba por escrito y podrán ser complementarios por medio de testigos".

Interpretación del derecho aplicable.

El derecho a la información.

En la presente *"consulta administrativa"* hay que partir de la distinción que hay entre el derecho del IDAAN de conservar la información de las deliberaciones y reflexiones de su Junta Directiva y el derecho que tienen las personas de tener acceso a esa información y el derecho de protección de esos datos, entre los cuales se podría incluir la información relativa a las estrategias institucionales.

Este derecho involucra: el acceso a los documentos administrativos como los archivos públicos, como las obligaciones informativas del Estado, el régimen de las empresas y actividades relacionadas con la información, el estatuto de los profesionales de la información, el régimen de responsabilidad civil y penal en materia de información. Importa igualmente, prevenir o minimizar riesgos, especialmente la protección de grupos sensibles o la prohibición de prácticas monopolísticas; compatibilizar el ejercicio de este derecho con el derecho y respeto a la intimidad personal; asegurar el cumplimiento de las obligaciones informativas del Estado; respetar el principio general de transparencia en la operación de la información.

El derecho a la información como garantía exigible al Estado.

La primera pregunta que hay que responderse para saber si existe tal derecho es si existe una norma en la Constitución panameña que lo establezca. En los artículos 37 y 41 constitucionales se señala que el derecho a la información será garantizado por el Estado, asegurando igualmente la protección de la forma de emisión del pensamiento. Veamos:

"**Artículo 41.-**Toda persona tiene derecho a presentar peticiones y quejas respetuosas a los servidores públicos por motivos de interés social o particular, y él de obtener pronta resolución.

El servidor público ante quien se presente una petición consulta o queja deberá resolver dentro del término de treinta días.

La ley señalará las sanciones que corresponden a la violación de está norma."

Sin embargo, este enunciado es muy general. En primer lugar, no dice qué es eso que se llama derecho a presentar peticiones y si estas incluyen el derecho de pedir información, aunque sí afirma que ese algo, va a ser garantizado por el Estado. Ahora bien, a no dudar las peticiones pueden en su sentido natural, involucrar una solicitud de información.

En la ley formal se encuentra regulada en el artículo 837 del Código Administrativo en donde se establece lo siguiente:

> "Todo individuo tiene derecho a que se **le den copias de los documentos** que existan en las secretarías y en los archivos de las oficinas del orden administrativo, siempre que no tenga carácter de reserva..." (Destaca la Procuraduría de la Administración)

A través de los artículos 13.1 de la Convención Americana de Derechos Humanos y el 19.2 del Pacto Internacional Sobre Derechos Civiles y Políticos, podemos darnos cuenta de la formulación moderna de la libertad de expresión, que es lo que algunos autores han denominado el derecho a la información en sentido amplio. Esta incluye tres libertades diferentes:

1. La libertad de buscar o de investigar;
2. La libertad de recibir; y,
3. La libertad de difundir informaciones, opiniones, ideas, por cualquier medio.

Dicho de otra manera, se encuentra aquí este haz de derechos que subsumen los derechos tradicionales de expresión y le añaden la libertad de recibir y la libertad de buscar o investigar informaciones.

La libertad que existe en relación con el Estado está protegida directa y subjetivamente por lo menos por un derecho de igual contenido, a que el Estado no impida al titular del derecho, para su ejercicio. Es decir, tengo la libertad de solicitar información **que individualmente o colectivamente le atañe a los ciudadanos** y junto con ella tengo un derecho subjetivo para exigir que el Estado no le impida obtenerla.

Entonces una libertad es la vinculación de una libertad protegida y un derecho a no impedir las acciones protegidas por esa libertad. Esto se traduce básicamente en que el Estado no impida esas acciones.

Esta regla tiene sus excepciones en el artículo 14 de la ley 6 de 2002, en donde se listan aquellas actuaciones administrativas que generan una información de carácter reservado. Y esta lista, por tener como contenido excepciones, es muy limitado y no se puede ampliar por medio de la interpretación ampliada. O sea, que en esta materia, la interpretación es restrictiva, y no se pueden inferir o deducir informaciones de carácter reservado o restringido, que no se encuentren expresamente indicadas en la lista legal.

En el caso bajo estudio, la Ley 6 de 2002, en materia de excepciones sólo incluye las deliberaciones del Consejo de Gabinete por lo que las discusiones de la Junta Directiva del IDAAN, de hacer parte de una decisión concreta, deberá estar a disposición de los solicitantes; pues ella podría ser antecedente de la actuación denunciada.

Es decir, que en tanto la información contendida de las deliberaciones de la Junta Directiva, hagan parte o sean el antecedente de actos administrativos específicos, por medio de los cuales se hayan afectado derechos de personas y éstos sean denunciados de ilegales; dichas deliberaciones deben ser puesta a disposición del denunciante, pues esa información (las deliberaciones relativas a un asunto específico) son los antecedentes que explican la decisión administrativa.

En otro orden de ideas, si esa información (las deliberaciones relativas a un asunto específico) dice relación con la discusión de las políticas y estrategias empresariales del IDAAN, en su calidad de empresa o las personas que compiten en el mercado abierto de producción, traslado (trasporte) o distribución de aguas; ellas si pudiese tener carácter reservado, pues sería un secreto comercial o industrial.

En el caso bajo estudio, al ser el IDAAN el suministrador exclusivo de agua, es decir al no haberse abierto el mercado hídrico; sus deliberaciones no podrían ser tomadas como información de carácter reservado, pues no constituyen un secreto comercial o industria. Ahora bien, en materia de producción de aguas, sí parece haber un mercado más o menos abierto, pues existen varios productores que le venden al IDAAN agua. En este caso de la producción, las demás empresas no han de tener derecho a que se les brinde la información económica o empresarial o de cualquier tipo, que reposen en los archivos del IDAAN, pues de brindárselas, se estaría compartiendo la estrategia empresarial y comercial a la competencia.

Conclusión particular

La información contendida en expedientes administrativos gozan de una garantía más específica que la información general sobre la cual rige en primera instancia la Ley de transparencia. La primera: la información que detenta la Administración en razón de un expediente administrativo, se requiere para asuntos particulares, y está regida por el artículo 70 de la Ley 38 de 2000.

Este derecho, debe referirse a documentos en los cuales se contiene información de la Administración, y no de otras personas que podrían ser afectadas por la debelación de dicha documentación. Es más bien, un derecho relativo a la publicidad y trasparencia. Según se ha dicho, en la ley aparecen algunas normas específicas que pretenden explicitar los derechos que demuestran muy tangiblemente la voluntad de dar a la actividad administrativa interna la máxima publicidad y trasparencia posible, lo que evidentemente facilita que los ciudadanos puedan disponer de la debida información para hacer mejor uso de sus derechos.

En cuanto a la información contenida en las grabaciones de las reuniones de la Junta Directiva del IDAAN, no parece haber una norma legal que expresamente indique que ella (la información) sea de carácter reservado, por lo tanto, en principio debería ser pública. Esto es así, ya que no basta con que la entidad declare que la información tiene carácter reservado, sino que primero debe haber una norma legal que así lo declare.

Ahora bien, si una persona: solicitante de la información, se refiere a una información concreta debatida en la Junta Directiva, y esa información hace parte de una potencial postura respecto de un caso (procedimiento administrativo) ya entablado en el IDAAN; el particular solicitante debe esperar a que la información sea asumida en un acto administrativo resolutivo concreto, para luego pedir acceso a ella. Es decir, que si la información no se refiere a una política general, sino a un asunto concreto, el particular deberá esperar a que se adopte una medida específica respecto de ese caso, para poder tener acceso a dichas deliberaciones.

La conservación de los antecedentes de la decisión administrativa.

De la atenta lectura del artículo 14 de la Ley 6 de 2002, se desprende que las autoridades correspondientes aunque consideren, amparados en una norma legal expresa, que deban no pueden suministrar una información, por tener ésta el carácter de restringida; le corresponderá emitir una resolución por las cuales se mantiene hasta por un período de diez años, la restricción sobre la información concreta. Es más de ser necesario dicho periodo se puede prorrogar por diez años más. Lo cual indica que:

1. En ningún caso el carácter de restringido podrá superar los veinte años, contados a partir de la primera clasificación,

2. Se debe proceder a la divulgación de la información si antes del cumplimiento del periodo de restricción adicional dejaren de existir las razones que justificaban tal acceso restringido.

3. Todo indica que el proceso de terminación de la restricción al acceso de la información opera de pleno derecho por el solo transcurso del tiempo, sin necesidad de resolución o acto administrativo alguno.

4. Para poder poner la información a disposición de las personas, luego del periodo de reserva o restricción, ha debido ser conservada.

Esta última reflexión es de suyo importante, pues de ella se infiere el deber de conservar la información emanada de las instituciones públicas, aún en el caso de que dicha información sea de carácter reservado o restringido.

Así pues con mayor razón, si la información no tiene dicho carácter, por lo tanto, no importa tanto en qué soporte se encuentra la información, lo cierto es que debe tenerse en soportes confiables, seguros y fidedignos.

Ahora bien, si la información es pasada en soporte informática, según lo señala la Ley 11 de 1998, se debe presumir que ese medio guarda las características del original, y por tanto, podría prescindirse de las cintas de casete. Pero en todo caso, se debe tener disponible esa información porque hace parte de la historia institucional del IDAAN, y por tanto, la misma prueba la buena gestión pública. Esta afirmación nos

lleva a que, si no se cuenta con la manera de guardar en soporte informático, las actas de reuniones de la Junta Directiva, se deben conservar las cintas de casete.

Todo lo antedicho tiene su explicación en el nuevo sistema de regulación del procedimiento administrativo, incorporado en la Ley 38 de 2000, pues se parte de la idea de posibilitar la debida defensa de los derechos y garantías de los ciudadanos frente a la administración. En este sentido, se le brinda al ciudadano el derecho al acceso a la información pública para que, la persona pueda conocer los antecedentes o causas originarias, de los actos administrativos, y con ello, pueda defenderse frente a la Administración.

Otra razón la da la Ley 6 de 2002, por la cual se establece la obligación de la trasparencia de toda actuación pública. Esto ya que se intenta hacer que las oficinas públicas permitan la evaluación de los servicios públicos, de parte de los ciudadanos. En este sentido la Ley 6 de 2002, permite que las personas accedan a documentos públicos y con esa información puedan saber de qué manera se gestiona y usan los bienes públicos; a fin de hacer una evaluación real de las verdaderas políticas públicas y del compromiso de los agentes oficiales, sobre todo de los altos funcionarios del Estado.

Hay un doble sentido, por un lado la debida defensa de las personas, cuando estas se enfrentan a la Administración; y por otro el ideal de democratización y verdadera representación pública.

Finalmente, la Junta Directiva del Instituto de Acueductos y Alcantarillados Nacionales debería conservar las grabaciones de las reuniones de la Junta Directiva, hasta tanto sean pasados a soportes informáticos o más confiables, aunque sean transcritos en actas aprobadas y firmadas.

Con la pretensión de haber colaborado con su despacho, quedo de usted,
Atentamente,

Alma Montenegro de Fletcher
Procuradora de la Administración.

AMdeF/15/hf.

Comentarios respecto del proyecto de ley por medio del cual se adopta la normativa aplicable a la Firma Electrónica o Digital

La actual doctrina de los Tribunal Constitucionales y Cortes Supremas de los países del llamado Derecho Románico, sostienen que 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 firma 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 (y, en especial, el documento electrónico con función de giro mercantil) 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 alfa-numéricos que permitan asegurar la procedencia y veracidad de su autoría y la autenticidad de su contenido.

Por lo tanto, si se dan todas las circunstancias necesarias para acreditar la autenticidad de los ficheros electrónicos o del contenido de los discos de los ordenadores o procesadores y se garantiza, con las pruebas periciales en su caso necesarias, la veracidad de lo documentado y la autoría de la firma electrónica utilizada, el documento mercantil en soporte informático, con función de giro, debe gozar de plena virtualidad jurídica operativa.

El pasado mes de octubre el Pleno del Congreso convalidó el Real Decreto-Ley sobre Firma Electrónica, una norma que va a impulsar de forma decisiva la Sociedad de la Información en España y que

garantiza la seguridad de las comunicaciones que realicen las empresas y los ciudadanos a través de la red y, en especial, el comercio electrónico.

España se convierte así, junto a Alemania, en el primer país que introduce una regulación completa sobre esta materia, que abre las puertas a un intercambio de bienes y servicios.

La firma electrónica es un código de autenticación que identifica formalmente al autor o los autores de un documento. Tendrá el mismo valor jurídico que la firma manuscrita y será admisible como prueba en juicio.

El Ministro de Fomento, en su intervención en el pleno del Congreso, señaló que "La Ley comporta un compromiso claro para que las nuevas tecnologías en las comunicaciones sean accesibles a todos. Se facilita con ello, la modernización tecnológica, no sólo en los ámbitos empresariales sino, también y especialmente, en los domicilios de los ciudadanos".

COMERCIO ELECTRÓNICO

Hay que destacar la importancia que la norma tiene para el sector de las pequeñas y medianas empresas españolas y el desarrollo y uso del comercio electrónico en España con la máxima seguridad jurídica de tal manera que se protejan los derechos de consumidores y usuarios.

Las empresas españolas podrán constituir una red virtual para la distribución de sus productos, incluso más allá de nuestras fronteras, sin necesidad de contar con una red física, con el ahorro que representa.

SEGURIDAD JURÍDICA

Para proteger la seguridad y la integridad de las comunicaciones, la firma electrónica tendrá que estar avalada por un certificado

reconocido que permita verificar la identidad del usuario y que será expedido por el prestador de servicios de certificación.

Estas empresas o entidades de certificación, que actuarán como notarios de la red, deberán inscribirse en un registro público.

Puntos principales del Real Decreto:

1.- Ambito de aplicación.

- Regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación. Las normas sobre esta actividad son de aplicación a los prestadores de servicios establecidos en España.

2.- Definición de firma electrónica y firma electrónica avanzada.

El Real Decreto define a la firma electrónica 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 los autores del documento que la recoge".

"Firma electrónica avanzada" es 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.

3.- Efectos jurídicos de la firma electrónica.

La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio.

4.- Creación de un Registro Público de prestadores de servicios de certificación en el Ministerio de Justicia, en el que deberán solicitar su inscripción con carácter previo al inicio de su actividad. Con el fin de garantizar su máxima eficacia jurídica, pública o privada, la firma electrónica tendrá que estar avalada por un certificado reconocido que permita verificar la identidad del usuario y que será expedido por el prestador de servicios de certificación.

Asimismo, el texto legislativo establece las obligaciones, garantías y condiciones exigibles a los prestadores de servicios de certificación.

régimen de acreditación de los notarios de la Red o de las entidades que certificarán a los usuarios que su firma electrónica es segura.

La acreditación de estas entidades es voluntaria pero se configura como un sello de calidad respecto de su adecuación a la normativa vigente, y otorgará garantías a los usuarios de que la empresa con la que trabaja tiene las suficientes garantías de seguridad y confidencialidad de sus datos y de sus comunicaciones.

El reglamento también regula el régimen aplicable a los dispositivos seguros de creación de la firma electrónica y a los de verificación, que también podrán obtener del Ministerio de Fomento un sello de calidad que demuestre que son especialmente seguros para la prestación de servicios de firma electrónica.

Todos los certificados otorgados del mismo modo en los distintos estados de la Unión Europea serán reconocidos automáticamente en España, mientras que para los expedidos en terceros países será necesaria la firma de un convenio de reconocimiento mutuo.

LA FIRMA ELECTRONICA. VALOR JURIDICO Y SEGURIDAD

Apollònia Martínez Nadal. Profesora Titular de Derecho Mercantil. Departamento de Derecho Privado. E-mail:

Universitat de les Illes Balears. Carretera de Valldemossa, km 7'5. CP 07003 Palma (Baleares)

I.- Introducción; firma electrónica, certificados y entidades de certificación como solución técnica para la seguridad de las comunicaciones electrónicas. II.- Valor jurídico de la firma electrónica: finalidad del Real Decreto-ley 14/1999. Nociones básicas previas. 1.- Firma electrónica. a) Concepto y clases. b) Nociones relacionadas: datos y dispositivos de firma electrónica. 2.- Certificados. 3.- Prestadores de servicios de certificación. a) Noción y funciones. b) Principios generales para la prestación de servicios de certificación. c) Condiciones exigibles a los prestadores de servicios de certificación. III.- Efectos legales de la firma electrónica. IV.- Conclusiones.

I.- INTRODUCCION: FIRMA ELECTRONICA, CERTIFICADOS Y ENTIDADES DE CERTIFICACIÓN COMO SOLUCIÓN TÉCNICA PARA LA SEGURIDAD DE LAS COMUNICACIONES ELECTRONICAS.

En el comercio electrónico, el clásico documento de papel es sustituido por el novedoso documento electrónico. Correlativamente, desaparecen las tradicionales firmas manuscritas y las funciones que ellas desempeñan. Desde el punto de vista técnico, se ofrece la firma digital, basada en la criptografía asimétrica, como técnica sustitutiva que puede desempeñar iguales o incluso superiores funciones.

Los criptosistemas de clave asimétrica o pública están basados en el uso de un par de claves asociadas: una clave privada, conocida sólo por su titular, que debe mantenerla en secreto (e incluso puede ocurrir que ni siquiera el titular conozca la clave privada, que probablemente se mantendrá en una tarjeta inteligente, o se podrá acceder a ella mediante un número de identificación personal, o, en la situación ideal, mediante un dispositivo de identificación biométrica, p.ej., a través del reconocimiento de una huella digital), y una clave pública, relacionada matemáticamente con ella, y que puede ser accesible para cualquiera (e incluso debe serlo, a través, p.ej., de directorios públicos de fácil

acceso). Si bien las dos claves están matemáticamente relacionadas entre sí, el diseño y la ejecución en forma segura de un criptosistema asimétrico hace virtualmente imposible que las personas que conocen la clave pública puedan derivar de ella la clave privada (inderivabilidad).

Este sistema de criptografía asimétrica permite realizar firmas digitales, que proporcionan autenticidad, integridad y no rechazo de origen, y que pueden resultar tanto o más útiles, válidas y eficaces en el comercio y en los procedimientos legales como la firma escrita sobre papel. El procedimiento básico para ello es el siguiente:

a') El emisor de un mensaje (cifrado o no a efectos de confidencialidad) lo cifra digitalmente utilizando su clave privada, y su receptor podrá descifrarlo utilizando la clave pública del suscriptor, de forma tal que si el mensaje, conteniendo información textual, es legible, tiene la seguridad de que el mensaje ha sido enviado por el titular de la clave privada correspondiente a la clave pública que él utiliza (autenticación); que, además, el mensaje no ha sido modificado (integridad), y que, finalmente, el emisor del mensaje no puede negar ser el autor de ese mensaje con un determinado contenido (no repudiación de origen). Cualquiera que tenga la clave pública del usuario puede verificar la integridad del mensaje: si el mensaje ha sido modificado, el criptograma no se descifrará de forma adecuada, mostrando que ha sido alterado o sustituido.

b') No obstante, el procedimiento es algo más complicado porque debe añadirse un nuevo elemento: la función de hash, algoritmo que transforma una secuencia de bits en otra menor, y que se aplica tanto para la creación como para la verificación de la firma digital. Debido a que la aplicación de criptografía asimétrica sobre la totalidad del mensaje puede resultar costosa, especialmente si este es muy extenso, se aplica sobre el mensaje inicial el algoritmo con función de hash, y se obtiene un resumen del mismo (denominado compendio del mensaje o huella digital), caracterizado por su irreversibilidad (esto es, a partir del resumen no puede obtenerse el mensaje completo inicial), y por ser único del mensaje (es decir, es computacionalmente imposible obtener

un segundo mensaje que produzca el mismo resumen o hash), de forma que cualquier cambio en el mensaje produciría un resumen o hash diferente.

A continuación, el resumen o hash, de menor extensión, es cifrado con la clave privada de criptografía asimétrica del firmante (que proporciona, como veremos, integridad, autenticidad y no rechazo de origen). Y, finalmente, ambos mensajes, el mensaje inicial, total, y en claro, y la firma digital (el hash o resumen cifrado), son remitidos conjuntamente al destinatario.

c') Finalmente, el receptor, que cuenta con dos elementos (el mensaje inicial y la firma del hash) debe proceder a la verificación de la firma. La verificación de la firma digital es el proceso de comprobación de esa firma por referencia al mensaje original y a una clave pública dada, determinando de esta forma si la firma digital fue creada para este mismo mensaje utilizando la clave privada que corresponde a la clave pública referida. Para ello, el verificador realizará dos operaciones: descifrará el hash firmado con la clave privada del emisor aplicando la clave pública del mismo; y aplicará la función de hash sobre el mensaje completo que ha obtenido (pues no es posible realizar lo contrario: 'desresumir' el hash que ha recibido, dada la irreversibilidad ya mencionada de esta función). Si el hash recibido y descifrado y el segundo hash obtenido coinciden, el destinatario tiene la seguridad de que el mensaje recibido ha sido firmado por el emisor con ese contenido. Por contra, si uno u otro de los dos elementos ha sido alterado en algún momento, no habrá coincidencia de los dos resúmenes, con lo que el receptor no podrá ni deberá llegar a la misma conclusión. Y todo ello, que aparenta ser un complicado proceso matemático, se produce en cuestión de segundos con la ayuda de ordenadores.

De esta forma, la firma digital puede definirse, pues, como la transformación de un mensaje utilizando una función de hash y un criptosistema asimétrico, de forma que una persona que tenga el mensaje inicial y la clave pública del firmante puede determinar de forma segura:

1) si la transformación fue realizada usando la clave privada que corresponde a la clave pública del firmante; y se satisface así la necesidad de autenticación, porque si un mensaje fue firmado con la clave privada de un sujeto, sólo puede ser verificado por el receptor utilizando la clave pública de ese mismo sujeto.

2) si el mensaje inicial ha sido alterado desde la transformación; y se satisface así la exigencia de integridad, pues, si el mensaje ha sido alterado en lo más mínimo, su resumen no coincidirá con el resumen firmado del mismo descifrado aplicando la clave pública de su emisor; y si el mensaje firmado ha sido alterado no coincidirá con el resumen del mensaje en claro.

La firma digital consigue, así, iguales, si no superiores efectos, que la firma manuscrita pues da integridad, autenticidad, y, en definitiva, no rechazo de origen. En este sentido, las diversas iniciativas legislativas existentes sobre firma digital realizan un reconocimiento de los efectos de la misma equiparándola, con más o menos exigencias, a la firma manuscrita, y estableciendo, incluso, determinadas presunciones o reglas de atribución a su favor.

En cualquier caso, ha de tenerse en cuenta que estas presunciones legales y reglas de atribución serán ciertas siempre y cuando tengan un fundamento técnico adecuado. Es decir, para que se atribuya un mensaje firmado con una clave privada determinada al titular de esa clave es necesario que el par de claves en cuestión cumpla una serie de características y requisitos, que implican una mínima calidad de las claves y unas mínimas garantías del procedimiento de generación de las mismas:

1) en primer lugar, ha de tratarse de un par de claves seguro, de forma que no ha de ser posible obtener la clave privada, que ha de mantenerse en secreto, a partir de la clave pública, lo cual dependerá, en gran medida, de la longitud de la clave, así como también de los avances de la técnica.

La seguridad del par de claves puede depender de restricciones que establezcan un tamaño mínimo para la clave y otras restricciones. En teoría, algunas claves podrían hallarse a través de intentos sistemáticos (brute-force attacks); no obstante, la longitud de la clave puede establecerse de tal forma que el código no pueda romperse en un periodo de tiempo viable o realizable.

Esta irreversibilidad del proceso consistente en la esperanza de que será imposible de derivar la clave privada secreta de un usuario a partir de su clave pública se denomina "no viabilidad computacional", concepto relativo basado en el valor de los datos protegidos, la capacidad computacional general requerida para protegerlos, el tiempo necesario para protegerlos y el costo y el tiempo necesario para atacar esos datos, evaluando esos factores en función de la tecnología actual y de los adelantos tecnológicos previstos para el futuro. En función de estos factores, se distingue, por una parte, entre seguridad incondicional o teórica (el sistema es seguro frente a un atacante con tiempo y recursos computacionales ilimitados) y seguridad computacional o práctica (el sistema es seguro frente a un atacante con tiempo y recursos limitados).

2) en segundo lugar, el par de claves ha de ser único, es decir, no deben existir dos o más personas con la misma clave (no es posible que la clave x sea, al mismo tiempo, la clave de firma de A, de B y de C; en tal caso, mensajes firmados por B serían atribuibles a A). Por ello, los procedimientos de generación de claves han de introducir los elementos de aleatoriedad necesarios para evitar que dos personas utilizando el mismo programa de generación obtengan las mismas claves.

3) en tercer lugar, el procedimiento de generación ha de ser adecuado, de forma que no ha de ser posible obtener la clave privada reproduciendo del procedimiento de generación de claves.

Todo ello sin perjuicio de que, asimismo, para el buen funcionamiento del sistema de certificados sea esencial que la clave privada esté bajo

el control única y exclusivamente del suscriptor, así como que este suscriptor esté correctamente identificado.

La criptografía contribuye, pues, en gran medida a la seguridad de las transacciones comerciales en una red abierta e insegura como Internet; pero la criptografía puede ser sólo una parte de esta historia de la seguridad. Obsérvese que efectivamente, los sistemas de criptografía asimétrica garantizan que la clave privada del emisor se corresponde con la clave pública utilizada para descifrar el mensaje, y que, en última instancia, el mensaje se ha firmado con la correspondiente clave privada (atribuida, p.ej., a A). Y esto, sin embargo, no asegura la autenticación (que el mensaje ha sido firmado por A), porque incluso si las claves se corresponden matemáticamente, no hay asociación intrínseca con una persona determinada: no existe garantía de que ese par de claves, que se corresponden matemáticamente, correspondan efectivamente a la persona a la que se atribuyen (esto es, A, que puede no existir o haber sido suplantado por una tercera persona). Y para la solución de estos problemas de la firma digital, la criptografía necesita de una tercera parte de confianza, la cual actuará para asegurar el vínculo entre la clave pública y el titular de la clave privada.

II.- VALOR JURÍDICO DE LA FIRMA ELECTRÓNICA: FINALIDAD DEL REAL DECRETO-LEY 14/1999. NOCIONES BÁSICAS PREVIAS.

Como hemos señalado, la firma digital consigue iguales, si no superiores efectos, que la firma manuscrita pues da integridad, autenticidad, y, en definitiva, no rechazo de origen. En este sentido, las diversas iniciativas legislativas existentes sobre firma digital realizan un reconocimiento de los efectos de la misma equiparándola, con más o menos exigencias, a la firma manuscrita, y estableciendo, incluso, determinadas presunciones o reglas de atribución a su favor.

En el derecho español, el Real Decreto-Ley 14/1999, sobre firma electrónica, primera regulación general de la firma electrónica en el ordenamiento español tiene como finalidad, conforme a su art. 1.1, coincidente básicamente con el art. 1 de la directiva por la que se

establece un marco común para la firma electrónica, la regulación del "uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación". Y, en particular, dedica el Real Decreto su art. 3 al reconocimiento jurídico de efectos a la firma electrónica. En tanto que este reconocimiento depende de conceptos previos (básicamente firma y nociones relacionadas, certificados, y prestadores de servicios de certificación), abordamos en primer lugar estos conceptos antes de analizar el contenido especifico de este precepto.

1.- Firma electrónica.

a) Concepto y clases.

Como es sabido, en el comercio electrónico el clásico documento de papel es sustituido por el novedoso documento electrónico. Correlativamente, desaparecen las tradicionales firmas manuscritas, que pueden ser remplazadas usando una variedad de métodos que son incluidos en el concepto amplio de firma electrónica, dentro del que tiene cabida, como categoría particular, el de firma digital.

El Real Decreto-ley 14/1999, establece, en su art. 2, apartado a) un concepto general de firma electrónica (coincidente básicamente con el establecido en el art. 2.1 de la directiva) que es el siguiente: "Es 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". En este concepto amplio y tecnológicamente indefinido de firma, tendrían cabida técnicas tan simples como un nombre u otro elemento identificativo (p.ej., la firma manual digitalizada) incluido al final de un mensaje electrónico, y de tan escasa seguridad que plantean la cuestión de su valor probatorio a efectos de autenticación, aparte de su nula aportación respecto de la integridad del mensaje. Tan es así que incluso podría dudarse de su condición de firma, por su utilidad más bien escasa o incluso inexistente.

Por ello, esta definición general va seguida, en el art. 2, apartado b) del Real Decreto (coincidente básicamente con el art. 2.2 de la directiva), de un nuevo concepto, el de firma electrónica avanzada, definido 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 estos". Se trata, por tanto, de una firma que debe cumplir una serie de requisitos, similares a los exigidos en el art. 2.2. de la directiva que se considera que añaden calidad a la firma electrónica, que es así una firma más segura. Obsérvese que con los tres primeras exigencias (identificación del signatario, creación por medios bajo su exclusivo control y vinculación única al mismo) lo que se pretende es garantizar la autenticación y evitar el rechazo en origen de los mensajes electrónicos; y que con el último requisito (vinculación a los datos que permite detectar cualquier alteración ulterior) se pretende salvaguardar la integridad de los documentos electrónicos.

Una clase particular de firma electrónica que podría ofrecer seguridad, por cuanto, como es sabido, puede cumplir en principio los requisitos de autoría e integridad establecidos en el art. 2 apartado b) del Real Decreto (y el art. 2.2 de la directiva) para las firmas avanzadas, es la de las firmas digitales. Estas firmas son tecnológicamente específicas, pues se crean usando un sistema de criptografía asimétrica o de clave pública (frente a las firmas electrónicas tecnológicamente indefinidas como hemos dicho, por cuanto incluyen cualquier método, incluido, pero no limitado, al de los sistemas de clave pública). No obstante, pese a la seguridad ofrecida por la firma digital, el Real Decreto-Ley 14/1999, siguiendo en este punto a la directiva comunitaria, regula, como hemos visto, la firma electrónica en general, y no sólo la firma digital en particular, en un intento de abarcar otras firmas electrónicas, basadas en técnicas distintas de la criptografía asimétrica (técnicas disponibles o en desarrollo que permitan cumplir algunas o todas las funciones características de las firmas manuscritas en un medio electrónico). Pero con el efecto ya mencionado de abarcar técnicas de escasa o incluso nula utilidad.

En definitiva, con el establecimiento de estos dos conceptos de firma electrónica, se establece la diferencia entre firmas de mayor o menor de calidad, distinción nada irrelevante, a efectos, como veremos, de reconocimiento legal de efectos. Pues el art. 3, dedicado a los efectos jurídicos de la firma electrónica equipara, como veremos, a la firma manuscrita únicamente la firma avanzada (y siempre que cumpla determinados requisitos).

b) Nociones relacionadas: datos y dispositivos de firma electrónica.

• Datos de creación y de verificación de firma. De entrada, entre los elementos que permiten la creación de una firma electrónica, el art. 2, apartado d) define los "Datos de creación de firma" que son "los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la firma electrónica". Y el apartado g) del mismo art. 2 define los "datos de verificación de firma" como "los datos, como códigos o claves criptográficas publicas, que se utilizan para verificar la firma electrónica". Por tanto, desde la perspectiva de la criptografía asimétrica en la que se basa la firma digital, se está haciendo referencia al par de claves, pública y privada.

Un tema de especial importancia es el relativo a la calidad de este par de claves, de los datos de creación y verificación de firma (en terminología del Real Decreto-Ley importada de la directiva). Lo que nos sitúa ante el delicado tema de la generación no ya de la firma sino de las claves de firma. Y, especialmente, el problema de la generación de claves no fiables (fácilmente rompibles, en el sentido de que a partir de la clave pública pudiera obtenerse la privada), previsibles (fácilmente conocibles por el proveedor del software o hardware reconstruyendo el proceso de creación) o de claves repetidas (por la no introducción de los adecuados correctores de aleatoriedad). Sea cual sea el sistema de generación (central, por la propia entidad certificadora; o local, por el propio usuario), es esencial que las claves sean únicas y estén a prueba de manipulaciones (lo cual viene dado prácticamente por la elección de una adecuada longitud de clave y un adecuado proceso de generación). En otro caso, la firma digital no podría utilizarse de forma segura en las relaciones comerciales y

jurídicas. Por ello, en relación con estos productos comerciales de generación de claves sería necesario un control o auditoría que verificara su fiabilidad, además de someter a un riguroso régimen de responsabilidad a los creadores de los instrumentos de generación de claves. Y, en este sentido, de forma más genérica o más específica, las distintas legislaciones en materia de firma contiene previsiones al respecto; y así ocurre, de forma bastante específica, en el Real Decreto-Ley español, aun cuando, como veremos, con una cierta de confusión de conceptos al establecer tales exigencias no respecto de los dispositivos de creación de datos de firma (las claves), a los que nos hemos estado refiriendo hasta ahora en este apartado, sino en relación con los dispositivos de creación de firma, que se trata de un concepto distinto, como veremos a continuación.

• Dispositivos de creación y de verificación de firma. El Real Decreto-Ley 14/1999 establece los conceptos de dispositivo de creación y verificación de firma, definidos, de forma respectiva como "un programa o un aparato informático que sirve para aplicar los datos de creación de firma" (art. 2, apartado e); y "un programa o un aparato informático que sirve para aplicar los datos de verificación de firma" (art. 2, h). Por tanto, se trataría, respectivamente, de aquellos elementos informáticos que permiten la aplicación de la clave privada sobre un mensaje electrónico por parte de su autor y remitente para la creación de una firma electrónica y la aplicación de la clave pública por parte del destinatario para la verificación de ese mensaje firmado.

Establecido así el concepto general, el art. 2, apartado f) define el "Dispositivo seguro de creación de firma" que es aquel que cumple una serie de requisitos que permiten considerarlo como seguro. Estas exigencias (establecidas en el artículo 19 que incorpora a priori al derecho español el Anexo III de la directiva comunitaria) no se predican todas ellas de los dispositivos seguros de creación de firma sino que hacen referencia a elementos distintos como los dispositivos de generación de claves (que son distintos de los de creación de firma, como hemos señalado anteriormente) (caso de los requisitos del apartado primero y segundo de unicidad o inderivabilidad de las claves) o cuestiones diferentes como la relativa a la custodia de la

clave privada (caso del requisito del apartado tercero). De modo que el enunciado del precepto no se corresponde realmente con su contenido. Y de esta forma se pone de manifiesto el ya anunciado confusionismo, si no ambigüedad calculada y necesaria, del Real Decreto-Ley a la hora de definir conceptos técnicos, achacable, no obstante, no al legislador español sino al comunitario al que se limita a seguir aquel en este punto (tanto por lo que se refiere a las definiciones del art. 2 como a los requisitos del art. 19, equivalentes a los conceptos del art. 2 y requisitos del Anexo III de la directiva).

En cualquier caso, obviando ahora estas dificultades, una vez establecidas de forma genérica y en abstracto estas exigencias en el art. 19, se trata de ver cuándo un determinado producto cumple las mismas en la práctica, a efectos de poder ser considerado un dispositivo seguro. Pues bien, a estos efectos, los art. 20 y 21 del Real Decreto-Ley establecen un procedimiento de evaluación y certificación (equivalente al establecido en los apartados 4 y 5 del art. 3 de la directiva) de la seguridad de los dispositivos de firma. Esta calificación no es irrelevante sino absolutamente transcendente, como se desprende del mismo art. 3, relativo a los efectos jurídicos de la firma electrónica. Pues, efectivamente, este precepto, que analizaremos posteriormente, otorga a la firma electrónica el mismo valor jurídico que la misma manuscrita, siempre que cumpla una serie de exigencias, entre ellas la de haber sido producida por un dispositivo seguro de creación de firma. Y se presume que el dispositivo es seguro si está certificado, presunción con que la que se evitan, como veremos, difíciles y costosas pruebas periciales para demostrar su seguridad ante un juez.

2.- Certificados. Especial referencia al certificado reconocido.

Como es sabido, en comunidades amplias, entre partes desconocidas y geográficamente distantes, la utilización de firmas electrónicas, basadas en la utilización de un par de claves o datos de firma, puede plantear problemas de identificación de las partes. Es necesaria, por tanto, una forma de distribución segura de las claves públicas, (o de los elementos de verificación de firma, en la terminología establecida

por la directiva). La solución que se ha ofrecido desde el punto de visto técnico, que ha sido acogida legalmente en diversos ordenamientos, y que contempla también el Real Decreto-Ley 14/1999, siguiendo las directrices de la normativa comunitaria, es el sistema de certificados emitidos por terceras partes de confianza (denominadas, por el Real Decreto, prestadores de servicios de certificación, art. 2.k, y proveedores de tales servicios por la directiva, art. 2.11) que vinculan de forma segura un dato de verificación de firma (una clave pública), e indirectamente su correspondiente dato de creación de firma (clave privada) a una persona determinada.

El Real Decreto-Ley español, en clave tecnológicamente neutral, define el certificado, de forma general, como aquella certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad (art. 2.5, similar al art. 2.9 de la directiva). (la versión del borrador inicial, en clave tecnológica menos neutral, lo definía como aquella declaración digital que atribuye una clave pública o un elemento similar a una persona individual y verifica la identidad de la persona, exigiendo su presencia física ante un proveedor de servicios de certificación (acreditado), o a través de otras medidas adecuadas).Se señala así la función básica de los certificados, y el elemento clave de tal función: la comprobación de la identidad del firmante, que plantea la cuestión de la responsabilidad del prestador en caso de emisión de certificados inexactos. Junto a este concepto general de certificado, en el que como acabamos de ver pueden tener cabida declaraciones electrónicas que no son verdaderos certificados ni cumplen su función esencial, el Real Decreto-Ley 14/1999, en su art. 2, j) (similar al art. 2.10 de la directiva) establece un concepto específico de certificado que es el "certificado reconocido" que ha de cumplir una serie de requisitos que se presume le darán un mayor valor. Tales requisitos son de una doble naturaleza (art. 2, j del Real Decreto-Ley): requisitos de contenido del certificado, establecidos en el art. 8 del Real Decreto; y requisitos relativos al prestador de servicios de certificados, establecidos en el art. 12, y que analizaremos posteriormente al abordar el régimen de los prestadores de servicios de certificación. De esta forma, se establecen, siguiendo las directrices comunitarias, dos categorías de certificados: un certificado ordinario y

un certificado reconocido que cumple unos requisitos superiores (tal como hemos visto que ocurría con el concepto de firma), y al que también (igual que a la firma electrónica avanzada) se reconoce un valor y eficacia superior (pues, para equiparar jurídicamente una firma electrónica avanzada a una firma manuscrita, el art. 3.1 exige, entre otros requisitos, que se trate de una firma electrónica avanzada basada en un certificado reconocido). Con las consiguientes dudas sobre la seguridad, el valor y la eficacia del resto de firmas y certificados (a los que se intenta salvaguardar, como veremos, en el art. 3.2).

3.- Prestadores.

a) Noción y funciones.

La terminología utilizada para designar a las entidades emisoras de certificados es diversa (autoridades de certificación, entidades de certificación, proveedores de servicios de certificación). La opción comunitaria (que se inclina por el término "proveedores") pone de manifiesto una voluntad de evitar siquiera la apariencia de atribución de naturaleza publica que sí podrían sugerir otras denominaciones (p.ej., autoridad de certificación), y posibilitando así su naturaleza estrictamente comercial. En la misma línea comunitaria se hallan, lógicamente, tanto la denominación como la noción de estas terceras partes de confianza emisoras de certificados en el Real Decreto español. En efecto, nuestro Real Decreto habla de prestadores de servicios de certificación que, siguiendo el art. 2.6 de la directiva, son objeto de la siguiente definición en su art. 2, apartado k): "Es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica". La definición del art. 2, apartado k) del Real Decreto 14/1999, igual que el art. 2.6 de la directiva, señala la función básica de todo prestador de servicios de certificación: la emisión de certificados. Y deja abiertas las puertas a otros servicios. Tales servicios pueden ser inherentes al propio certificado y necesarios (revocación y suspensión en caso de pérdida de la clave privada u otro elemento de firma, servicio al que se refiere el art. 11.e), 12.c, además del art. 9), otros más bien discutibles (generación de las claves, permitida al prestador tanto en el

ordenamiento comunitario como en el español, y, en particular, copia o almacenamiento de las mismas, actividad esta última respecto de la que, como veremos, existen diferencias entre ambos ordenamientos), así como otros complementarios pero igualmente necesarios para la seguridad del sistema de certificados en particular o del comercio electrónico en general (p.ej., de forma respectiva, servicio de sellado temporal, previsto siquiera de forma parcial en el art. 12.a), o actuación como notario electrónico).

b) Principios generales para la prestación de servicios de certificación.

Una de las cuestiones más debatidas respecto de las entidades encargadas de la prestación de servicios de certificación es, junto a la relativa a su naturaleza (pública o privada y comercial), la de su constitución: libre, o condicionada a la obtención previa de una autorización pública, licencia o acreditación.

A) Régimen de libre competencia. La posición del legislador español ante la cuestión del régimen de establecimiento de los prestadores de servicios de certificación se pone de manifiesto en el art. 4 del Real Decreto 14/1999, que establece el principio de libre competencia en la prestación de servicios de certificación, sin que el ejercicio de este actividad quede reservado a determinadas entidades y sin necesidad de obtención de licencia o autorización previa. Por lo que, en principio, cualquier persona, física o jurídica, puede desarrollar esta actividad (sin perjuicio de que se le exija el cumplimiento de una serie de requisitos, establecidos, como veremos, en el art. 11 del Real Decreto; y sin perjuicio de la exigencia de inscripción registral, que, como veremos, consideramos que tampoco impide la actuación de un prestador).

B) Sistemas de acreditación de prestadores de servicios de certificación (y de certificación de productos de firma electrónica). Acogiéndose al art. 3.2 de la directiva (que permite que los Estados miembros establezcan sistemas voluntarios de acreditación destinados a mejorar los niveles de provisión de servicios de certificación), el legislador español establece la existencia de posibles sistemas de acreditación de

prestadores de servicios de certificación, que, en tanto que voluntarios, son compatibles con el principio de libre constitución (art. 6 del Real Decreto 14/1999). La acreditación voluntaria, conforme al art. 2, apartado ll) del Real Decreto-Ley 14/1999, es un permiso, licencia o autorización que conlleva una serie de derechos y una serie de obligaciones para el prestador que voluntariamente la solicita y la obtiene. En realidad, más que derechos, habría de hablarse de efectos positivos; p.ej., en el caso del Real Decreto 14/1999, la presunción establecida en el art. 3.1, pfo. segundo (relativo a los efectos jurídicos de la firma electrónica) con la que se ven favorecidas aquellas firmas electrónicas avanzadas basadas en un certificado reconocido expedido, precisamente, por un prestador de servicios de certificación acreditado; en cuanto a las obligaciones, serán aquellos requisitos (a los que se refiere el art. 6.4, inciso final del Real Decreto-Ley) que se determinen reglamentariamente para poder ser acreditado. En cualquier caso, su solicitud es totalmente voluntaria, y, en ningún caso, la falta de acreditación impide el ejercicio de la actividad de prestación de servicios de certificación. Unicamente, no se beneficiará de los mencionados efectos positivos que favorecen, como hemos visto, al prestador acreditado. En cuanto a la obtención de la acreditación, sujeta al pago de la correspondiente tasa (ex art. 23), el art. 6.1 del Real Decreto establece que será el Gobierno el que, por Real Decreto, "podrá establecer sistemas voluntarios de acreditación de los prestadores de servicios de certificación de firma electrónica". De manera que, mientras no se apruebe tal Real Decreto, no podrá procederse a la acreditación de prestadores de servicios de certificación, y, por tanto, ningún prestador ya existente o de nueva constitución podrá beneficiarse, de momento, de tal calificación, que, como acabamos de señalar, no es irrelevante dada la presunción del art. 3.1, párrafo segundo.

C) Registro de Prestadores de Servicios de Certificación. Tras articular, siguiendo el régimen diseñado en la de directiva, un sistema de libre constitución combinable con un sistema de acreditación totalmente voluntaria, el Real Decreto-Ley 14/1999, de forma novedosa, crea un "Registro de Prestadores de Servicios de Certificación", cuya regulación presente (art. 7) o futura (normativa de desarrollo) debe ser conforme

a las directrices del derecho comunitario, y, en concreto, no debe constituir en ningún caso un obstáculo al principio de libre competencia y libre constitución de prestadores de servicios de certificación. Pues, en efecto, la principal cuestión que plantea la creación de este novedoso Registro es el carácter obligatorio o simplemente facultativo de la inscripción de los prestadores de servicios. De la letra del apartado primero del art. 7 del Real Decreto-Ley se deduce, en principio, la obligatoriedad de la inscripción registral de todo prestador de servicios de certificación establecido en España. No obstante, a estos efectos ha de tenerse en cuenta también el apartado segundo, párrafo segundo del mismo art. 7 que dispone que:"La formulación de la solicitud de inscripción en el Registro por los citados prestadores de servicios, les permitirá iniciar o continuar su actividad, sin perjuicio de la aplicación, en su caso, del régimen sancionador correspondiente". Por tanto, esta previsión suaviza la obligatoriedad que parece deducirse del apartado anterior, por cuanto la simple solicitud de inscripción (y no la inscripción misma) permiten al prestador solicitante iniciar, o, en su caso, continuar, el desarrollo de su actividad de prestación de servicios de certificación. Y ha de tenerse en cuenta también el análisis del régimen sancionador al que alude este apartado segundo y que demuestra que el incumplimiento de la obligatoriedad de la inscripción general tiene, en determinados supuestos, escasas consecuencias (multa económica de cuantía inferior), y no impide el ejercicio de la actividad de certificación.

c) Condiciones exigibles a los prestadores de servicios de certificación.

Con independencia del establecimiento o no de un sistema de licencia, y de los requisitos que se exijan para su obtención, todo proveedor de servicios de certificación, para ser considerado una tercera parte de confianza, debería de cumplir una serie de requisitos fundacionales, así como otros requisitos posteriores de funcionamiento, que generen una confianza y seguridad en su organización y actividades. Estos requisitos generales que debe cumplir todo prestador de servicios de certificación se establecen en el art. 11 del Real Decreto 14/1999. Junto a estos requisitos generales, el art. 12 del Real Decreto establece unos requisitos específicos de determinados prestadores:

aquellos que expiden certificados reconocidos, requisitos específicos cabe considerar que otorgan una mayor seguridad y fiabilidad a la actividad prestadora. De forma que, como ocurre con la firma (ordinaria o avanzada) y con el certificado (simple o reconocido), el legislador español, siguiendo las directrices comunitarias, establece también dos categorías de prestadores: los que emiten certificados simples y los que emiten certificados reconocidos. El cumplimiento de estas exigencias del art. 12 no es irrelevante pues recuérdese que señalábamos que para que un certificado sea reconocido es necesario no sólo el cumplimiento de los requisitos de contenido del certificado establecidos en el art. 8 ya analizados sino también el cumplimiento por parte del prestador de los requisitos establecidos en el art. 12. El cualquier caso, el control del cumplimiento de estas exigencias corresponde, según el Real Decreto-ley 14/1999, al Ministerio de Fomento a través de la Secretaría General de Comunicaciones (art. 16), y su incumplimiento constituye infracciones tipificadas y clasificadas, en función de su mayor o menor gravedad (art. 24 y 25), que dan lugar a la imposición de la correspondiente sanción, establecida en el art. 25, y que, aparte de la multa, que varía en función de la gravedad de la infracción, puede conllevar en determinados supuestos la prohibición de actuación en España por un máximo de dos años. En cualquier caso, tengas en cuenta que, tras la última reestructuración ministerial, las competencias de la Secretaría General de Comunicaciones se han atribuido al nuevo Ministerio de Ciencia y Tecnología, en concreto a la Secretaría General de Telecomunicaciones y Sociedad de la Información, y se ha acabado suprimiendo aquella primera Secretaría (RD 557/00 de 27 de abril de 2000; y RD 696/00 de 12 de mayo de 2000).

c.1.- Obligaciones exigibles a todos los prestadores de servicios de certificación.

De acuerdo con el art. 11 del Real Decreto-ley 14/1999, todos los prestadores de servicios de certificación deben cumplir las siguientes obligaciones:

A) Comprobación de identidad y de otros datos personales. Se trata de un requisito de fundamental importancia dada la función ya mencionada del certificado como instrumento de vinculación segura de un dato de verificación de firma o clave pública a una persona determinada; la no exigencia expresa de personación física puede lugar a la admisión de sedicentes certificados que no vendrían a cumplir tal función. El art. 11.a) extiende esta obligación de comprobación a aquellos otros datos personales que, a modo de atributos, se incluyan en el certificado; de forma que la entidad certificadora responde de la veracidad de tales elementos en el momento de la inclusión (pero no en un momento posterior, caso de los atributos dinámicos, p.ej., un poder de representación inicialmente existentes pero posteriormente revocado). Asimismo este precepto, al establecer la posibilidad de que esta comprobación se realice por medio de otra persona física o jurídica, admite la intervención de las denominadas autoridades de registro local

B) Puesta a disposición de los dispositivos de creación y de verificación de firma.

C) Prohibición de copia o almacenamiento de datos de creación de firma, salvo autorización del titular, pues el conocimiento por terceras personas generaría el peligro de posibles utilizaciones por parte de terceros no autorizados; sin embargo, la prohibición del art. 11 c) no es absoluta, por cuanto se establece que los prestadores de servicios de certificación podrán almacenarlas o copiarlas si así lo solicita expresamente el cliente. Y en este punto existe una divergencia entre el Real Decreto-Ley español y la directiva comunitaria, que, aunque inicialmente contemplaba esta excepción, la hace desaparecer en la posición común. De ahí que, cuanto menos, pueda dudarse de que la ley española se ajusta a la directiva. Por otra parte, a diferencia de la generalidad de obligaciones de los prestadores de servicios de certificación, establecidas en los art. 11 y 12, la infracción de esta prohibición no constituye infracción "de las normas reguladoras de la firma electrónica y los servicios de certificación" en cualquiera de sus categorías, pues de todas ellas es excluida de forma expresa (ex 25.1.a), 25.2.a) y 25.3.a) y d)). La infracción de esta obligación del art. 11.c) está prevista en el en el apartado 3 del art. 16 que opta por la

vía sancionadora al amparo de la normativa de protección de datos, opción peculiar por cuanto entendemos que el bien jurídico protegido por dicha normativa (datos personales, intimidad) no coincide en modo alguno con el bien o interés afectado en caso de copia o almacenamiento de una clave privada, pues en tal caso, se abre la vía a un posible uso ilegítimo de tal clave que afectaría no ya a la intimidad del titular de la clave sino que le ocasionaría posibles problemas de responsabilidad frente a terceros por la apariencia creada por la firma de documentos electrónicos con una clave privada de firma en principio atribuida al titular del certificado pero que ha podido ser utilizada por un tercero que dispone de una copia de la misma.

D) Información previa a la emisión del certificado sobre una serie de aspectos (precio, condiciones y límites de uso, garantía patrimonial) y en relación con el solicitante de un certificado (sea o no consumidor). No afecta, en cambio, de forma criticable, al tercero usuario de un certificado que es, sin duda, el más necesitado de información sobre determinados aspectos incluidos en el art. 11.d (especialmente, las limitaciones de uso del certificado, y la garantía de la responsabilidad patrimonial del prestador).

E) Mantenimiento de un registro de certificados (art. 11.e) donde hacer públicamente accesible y disponible determinada información como los certificados, o las listas de certificados revocados, no sólo para los titulares de certificados sino también para terceros usuarios de los mismos. El momento de publicación puede ser el momento definitorio a efectos de obligaciones o responsabilidades fundamentales de la entidad de certificación y los usuarios de certificados; así, el art. 9.3 del Real Decreto 14/1999 dispone que la extinción de la eficacia de los certificados tendrá efectos desde la fecha en que así se haga constar en el Registro. Y, a partir de ese momento, será oponible a terceros.

F) Comunicación en caso de cese de actividad. En caso de cese de su actividad, el art. 11, f) dispone que los prestadores de servicio deben comunicarlo con una antelación mínima de dos meses (art. 13.1) a los

titulares de los certificados por ellos emitidos y, si estuvieran escritos en él, al Registro de Prestadores de Servicios del Ministerio de Justicia.

G) Solicitud de inscripción registral. En cuanto a la obligación de todo prestador de servicios de certificación establecida en el art. 11.g) remitimos al análisis de la misma realizado en el apartado dedicado al Registro de Prestadores de Servicios de Certificación.

H) Cumplimiento del Real Decreto y normas de desarrollo. Finalmente, de forma residual, el art. 11. h) establece la obligación de cumplir con cualquier otra norma del Real Decreto y con las normas de desarrollo del mismo.

c.2.- Obligaciones exigibles a los prestadores de servicios de certificación que expIDAAN certificados reconocidos.

Junto a las obligaciones generales del art. 11, el art. 12 establece unas exigencias especiales para los prestadores emisores de certificados reconocidos. Tales exigencias, con las que se pretende una mayor fiabilidad y seguridad de la actividad de tales prestadores, pueden agruparse, a efectos expositivos en las siguientes categorías.

A) Requisito temporal. El Real Decreto 14/1999, en su art. 12.1, establece la obligación de los emisores de certificados reconocidos de "Indicar la fecha y la hora en las que se expidió o se dejó sin efecto un certificado". En el proyecto de Directiva se incorpora, a solicitud del Estado español, esta misma exigencia temporal. De esta forma, tanto el legislador español como el comunitario, han detectado el problema temporal del sistema de certificados, absolutamente ignorado en la primera versión de la propuesta de directiva, y puesto de manifiesto ya por entonces en nuestros trabajos en la materia, en los que denunciamos reiteradamente la grave laguna existente en esta materia, y el peligro que ello suponía para el funcionamiento del sistema de certificados. En cualquier caso, es relevante el conocimiento del tiempo no sólo de la emisión del certificado o de su revocación sino del momento en que se firma electrónicamente el mensaje que se quiere verificar, y respecto de este último sigue sin existir previsión

legislativa alguna. Con lo que pueden existir problemas a la hora de valorar la validez y eficacia de un mensaje firmado electrónicamente.

B) Requisitos técnicos y de personal. Son básicamente los siguientes. De entrada, se establece la exigencia genérica de fiabilidad de los servicios (art. 12.b). Junto a ella, se establece una exigencia de rapidez y seguridad en la prestación del servicio; y, en concreto, en casos de extinción de la eficacia de los certificados, se exige seguridad e inmediatez lo que, interpretado literalmente supondría la imposibilidad de utilización por parte de prestadores emisores de certificados reconocidos de sistemas de publicación de la revocación no inmediatos, como los sistemas de listas periódicas de revocación (art. 12.c). A continuación se exige la utilización de personal cualificado (art. 12.d). Asimismo, se exige la utilización de sistemas y productos fiables que garanticen la seguridad técnica de los procesos de certificación (art. 12.e); en concreto, se exige tomar medidas contra la falsificación de certificados, y, en caso de que el prestador genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación (art. 12.f), previsión que es criticable por cuanto afecta únicamente a los prestadores emisores de certificados reconocidos, cuando debiera extenderse a todo prestador que genera datos de creación de firma, emita o no certificados. Finalmente se exigen la utilización de sistemas fiables de almacenamiento de certificados (art. 12, i). En cualquier caso, se trata de exigencias genéricas que es de esperar sean objeto de concreción a través de reglamentación técnica de desarrollo.

C) Requisitos económicos (art. 12, g). En virtud de esta exigencia, los prestadores de servicios de certificación que emitan certificados reconocidos deben mantener recursos financieros suficientes para actuar de conformidad con lo dispuesto en el Real Decreto-Ley. En particular, dada la potencial amplitud de la responsabilidad de la entidad de certificación, a fin de proteger a los terceros que se relacionen con la misma, el Real Decreto establece, en el mismo art. 12, g), la obligación del prestador emisor de certificados reconocidos de garantizarla por dos sistemas: a través de la constitución de una fianza mercantil prestada por una entidad de crédito o contratando un

seguro adecuado. En cuanto a la cuantía de la garantía, en el caso de emisión de certificados con límite cuantitativo, será, inicialmente, de, al menos, "el 4 por 100 de la suma de los importes límite de las transacciones en que puedan emplearse el conjunto de los certificados que emita cada prestador de servicios de certificación. Teniendo en cuenta la evolución del mercado, el Gobierno, por Real Decreto, podrá reducir el citado porcentaje, hasta el 2 por 100". En caso de que no se limite el importe de las transacciones en las que puedan emplearse al conjunto de los certificados que emita el prestador de servicios de certificación, "la garantía a constituir, cubrirá, al menos, su responsabilidad por un importe de 1.000.000.000 de pesetas (6.010.121,04 euros). El Gobierno, por Real Decreto, podrá modificar el referido importe". Obsérvese que esta obligación de garantía no se establece para todo prestador sino únicamente para los prestadores emisores de certificados reconocidos, que, por ello, ofrecen de entrada, una mayor solvencia patrimonial.

D) Requisitos informativos y de documentación. El art. 12, en su apartado i), tiene una exigencia de información que cubre las lagunas que hemos criticado respecto de la obligación de información del art. 11, d) (p.ej., por lo que se refiere a los terceros usuarios del certificado, a los que expresamente alude el art. 12, i). Finalmente, el art. 12, h) exige el registro de toda la información y documentación relativa a un certificado reconocido durante un periodo de tiempo adecuado (15 años). La finalidad de esta previsión se establece, en particular, a efectos de utilización como medio de prueba de la certificación en el ámbito de una reclamación o procedimiento judicial (en los que la cuestión de la prueba puede resultar de especial importancia).

III.- EFECTOS LEGALES DE LA FIRMA ELECTRÓNICA.

Analizamos, en este último apartado, la forma en que el Real Decreto 14/1999 pretende dar cumplimiento al que se configura como su principal objetivo, tal como establece expresamente su Preámbulo: el Real Decreto-ley persigue establecer una regulación clara del uso de la firma electrónica, atribuyéndole eficacia jurídica. Y lo hacemos en último lugar porque, como

veremos a continuación, el reconocimiento de esa eficacia jurídica depende en buena parte de conceptos previos, como el de firma electrónica y firma electrónica avanzada, dispositivo de creación de firma seguro y dispositivo seguro certificado, certificado y certificado reconocido, prestador, prestador que expide certificados reconocidos y prestador acreditado.

1.- Regla del equivalente funcional. Requisitos. Problema de la prueba de la existencia de tales requisitos. Como se ha visto, la firma electrónica, y, en concreto, la firma digital consigue iguales, si no superiores efectos, que los de la firma manuscrita pues puede proporcionar integridad, autenticidad, y, en definitiva, no rechazo de origen. Por ello, el Real Decreto-Ley 14/1999, siguiendo la directiva comunitaria, y al igual que algunas de las iniciativas legislativas existentes sobre firma digital, realizan un reconocimiento de los efectos de la misma equiparándola, con más o menos exigencias, a la firma manuscrita. En concreto, el art. 3.1, pfo. primero, basado en el art. 5 de la directiva, establece que "La firma electrónica ... tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose esta según los criterios de apreciación establecidos en las normas procesales". Es, en suma, la regla del equivalente funcional entre firma electrónica.

Para que se produzca esta equiparación es necesario el cumplimiento de una serie de requisitos: a) debe tratarse de una firma electrónica avanzada, es decir, aquella que cumple los requisitos establecidos en el art. 2, b), relativos, básicamente, a la autenticidad e integridad del mensaje y que nos sitúan ante la firma digital; b) dicha firma electrónica avanzada ha de estar basado en un certificado reconocido, es decir, aquel que cumple los requisitos de contenido del art. 8 y ha sido expedido por un prestador que cumple los requisitos del art. 12; c) dicha firma electrónica avanzada, además, ha de haber sido producida por un dispositivo seguro de creación de firma, que es aquel que cumple los requisitos del art. 19. El problema es, entonces, la acreditación o demostración de la existencia de estos requisitos establecidos en el art. 3.1 pfo. primero. Piénsese que en caso de presentar un mensaje firmado electrónicamente como prueba en juicio, habrán de ser necesarios complejos y dificultosos informes técnicos para

demostrar ante el juez la existencia de tales requisitos, y aun así puede resultar prácticamente imposible su prueba.

2.- Presunción de cumplimiento de los requisitos. Para evitar estas dificultades de acreditación del cumplimiento de los requisitos, el art. 3.1, pfo. segundo dispone que "Se presumirá que la firma electrónica avanzada reúne las condiciones necesarias para producir los efectos indicados en este apartado, cuando el certificado reconocido en que se base haya sido expedido por un prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma con el que esta se produzca se encuentre certificado, con arreglo a lo establecido en el artículo 21". De esta forma, se evitan los problemas de acreditación de tales requisitos, pues se establece una presunción de cumplimiento de los mismos ligada a la satisfacción de otras exigencias superiores: certificado reconocido emitido por un prestador acreditado y dispositivo seguro de creación de firma certificado. No obstante, obsérvese que, de momento, ninguna firma electrónica avanzada se puede beneficiar de tal presunción, pues no es posible el cumplimiento de uno ni de otro requisito, dependiendo, el primero de ellos, del Real Decreto de desarrollo de los sistemas de acreditación a que remite el art. 6; y el segundo, básicamente, de la publicación en el DOCE de las normas técnicas a las que como hemos visto se refiere el art. 21 del Real Decreto-Ley.

En cualquier caso, una vez acreditado el cumplimiento de los requisitos del art. 3.1, pfo. primero, sea por prueba directa (de especial dificultad) o por el juego de la presunción del párrafo segundo, estaremos ante un mensaje electrónico admitido, inicialmente, como prueba en juicio, pero cuya valoración, conforme el inciso final del art. 3.1. pfo. primero, se realizará "según los criterios de apreciación establecidos en las normas procesales". De manera que el juez, a la vista de las circunstancias del caso alegadas podrá dar plena eficacia jurídica a la firma o negársela, porque, p.ej., el mensaje fue firmado utilizando una clave privada que habiendo sido extraviada fue utilizada por un tercero en los momentos previos a la revocación; o bien porque el mensaje fue firmado con posterioridad la extinción del certificado, supuesto especialmente problemático puesto que el Real Decreto-Ley sólo exige prueba del tiempo respecto de la emisión y

revocación del certificado, pero no respecto del momento que se firma electrónicamente un mensaje, circunstancia que podría utilizarse tanto por el emisor como por el receptor si uno u otro tuviera interés en negar validez al mensaje; de ahí la conveniencia de sellar temporalmente aquellos mensajes especialmente relevantes si se quieren evitar problemas en caso de litigio.

3.- El problema de la firma electrónica que no reúna los requisitos de equiparación. La declaración expresa de admisibilidad de la firma electrónica como medio de prueba puede tener sentido en determinadas legislaciones, restrictivas respecto de los medios probatorios; no es el caso, sin embargo, del derecho español, donde parece admisible, y así se considera doctrinalmente, de acuerdo con la Ley de Enjuiciamiento Civil, la presentación de un documento electrónico, firmado digitalmente, como medio de prueba de la celebración de un contrato o de la existencia de una declaración por medios electrónicos. Y téngase en cuenta, que, como señalamos a continuación, esta declaración no sólo no abre puertas en ordenamientos como el español sino que, por si sola, y en los términos en que se ha establecido, puede incluso cerrarlas. En efecto, recuérdese que este reconocimiento legal de efectos del art. 5.1 (tanto su equiparación a la firma manuscrita como su admisibilidad como medio de prueba) se establece sólo respecto de firmas electrónicas que cumplan determinadas exigencias. Y resulta así que tales exigencias podrían venir a disminuir, si no negar, la eficacia legal de firmas electrónicas en las que faltara, p.ej., el requisito del certificado; de forma que una firma digital en la que las partes, conocidas y de confianza, se han intercambiado manualmente de forma segura sus claves, y han acordado que las firmas digitales creadas con los mismas serían vinculantes para las partes, no se consideraría equivalente a una firma manuscrita, ni podría ser aportadas como medio de prueba (cosa actualmente posible en el derecho español de no existir tal previsión).

Para evitar este posible resultado, restrictivo y excluyente, se establece un apartado 2 en el mismo art. 3 (equivalente al art. 5.2 de la directiva) que dispone que "A la firma electrónica que no reúna todos los requisitos previstos en el apartado anterior, no se le negaran efectos jurídicos ni será excluida como prueba en juicio, por el mero

hecho de presentarse en forma electrónica". ¿Qué significado y alcance tiene esta cláusula de salvaguarda de estas firmas electrónicas que no cumplen los requisitos establecidos para las firmas reconocidas? Porque si no se les puede negar eficacia, ¿acaso significa que tienen la misma eficacia que las que cumplen tales requisitos?, Si no pueden ser excluidas como prueba en juicio, por el mero hecho de presentarse en forma electrónica ¿acaso significa que son admisibles? ¿Cuál es, entonces, y, en definitiva, la diferencia, a estos efectos, entre una firma que cumple los requisitos del apartado primero y una firma que no cumple tales requisitos?

IV.- CONCLUSIONES

A la vista de lo expuesto, y, en especial, de este último apartado dedicado a los efectos jurídicos de la firma electrónica, puede concluirse que el Real Decreto-Ley no cumple, al menos de forma inmediata, su objetivo de regular y dar seguridad al tema de la validez de los efectos jurídicos de la firma electrónica. Pues, para que sea admitida como medio de prueba, se exigen una serie de requisitos que requerirán de numerosas y difíciles pruebas periciales. Y, aun cuando es cierto que, de forma adecuada, el legislador español establece en el art. 3.1, pfo. segundo una presunción que elimina buena parte de esas dificultades probatorias, no es menos cierto tampoco que tal presunción no se puede aplicar, de momento, pues los elementos en que se basa están pendientes de regulación y desarrollo no sólo por las autoridades nacionales sino incluso también por las comunitarias. Y esta necesidad de desarrollo ulterior afecta, como hemos visto, a otros muchas cuestiones contempladas en el Real Decreto.

Es por ello que no se comprende la urgencia en la tramitación de este Real Decreto (que lo ha sustraído de un debate parlamentario que hubiera podido resultar clarificador especialmente en un tema de la complejidad de la firma electrónica). Aunque, con base a esta urgencia alegada por el legislador (que, como hemos visto, ha planteado dudas sobre la constitucionalidad del procedimiento elegido), cabe demandarle una rápida actuación en el desarrollo y concreción los aspectos pendientes del Real Decreto-ley que permita una efectiva aplicación del mismo. Demanda ya tenida en cuenta por el legislador

con aprobación de la Orden Ministerial de 21 de febrero de 2000 que regula la acreditación de los prestadores y la certificación de los dispositivos seguros de firma, conceptos de los que depende en buena medida el juego de la presunción del art. 3.1 pfo. segundo. Pero quedan todavía diversos aspectos pendientes de desarrollo.

LA FIRMA ELECTRONICA EN EL PROCEDIMIENTO ADMINISTRATIVO

Universidad de Murcia
Murcia, 6 de junio de 2000

Maximino I. Linares Gil
Subdirector General de Organización y Asistencia Jurídica
Servicio Jurídico de la AEAT

I.- INTRODUCCION: LA NUEVA ADMINISTRACION PUBLICA.

El extraordinario desarrollo de la informática y su maridaje con los telecomunicaciones en la denominada "telemática", incide muy considerablemente y de un doble modo en la actividad administrativa. La posibilidad de recoger, almacenar, modificar y enviar - de manipular en definitiva- cantidades asombrosas de información en un tiempo casi despreciable -se habla de comunicación en tiempo real- no puede por menos que tener una crucial influencia en la manera en que las Administraciones Públicas sirven con objetividad los intereses públicos a los que están llamadas, de acuerdo con el artículo 103.1 de nuestra Constitución de 1978.

Este impacto, ya avanzamos, tiene lugar de manera dual. Primeramente, porque la posibilidad técnica de llevar a cabo el tratamiento automático y exhaustivo de información pone en riesgo evidente el respeto y la protección de la personalidad de los ciudadanos, que observan cómo innumerables datos que les conciernen se van acopiando por doquier en bases de datos y viajan

de un lado a otro con ignorados propósitos. Esta amenaza trata de ser conjurada con el reconocimiento de un denominado derecho al libre desenvolvimiento de la personalidad o derecho de autodeterminación informativa, en cuya virtud el ciudadano tiene derecho a conocer qué información sobre él mismo es objeto de tratamiento automatizado y qué uso recibe aquélla, a fin de que, en todo caso, se preserve su intimidad y privacidad2.

Junto a esta incidencia, que podemos denominar material o sustantiva, hay una segunda no menos relevante, de carácter formal o procedimental. La introducción de máquinas en el quehacer administrativo que sean capaces de recibir y almacenar información, reproducirla cuantas veces se antoje y enviarla por medios electrónicos supone una mutación trascendental en el vehículo que históricamente ha utilizado la Administración Pública en la tramitación de los procedimientos administrativos, materializados en una sucesión de documentos escritos. Se hace necesario evitar que el avance tecnológico merme las garantías que para Administración y ciudadanos ha venido constituyendo la constancia documental e indeleble de los procedimientos tramitados. El tránsito de un procedimiento que se articula materialmente en torno al expediente (con sus carpetas), integrado por documentos materiales tangibles a los sentidos humanos, a otro en el que se admiten los documentos intangibles, sólo accesibles por medios electrónicos, ajenos ya definitivamente a la autografía humana -al puño y letra-, exige imperiosamente arbitrar mecanismos que aseguren la autenticidad de tales documentos, junto con su integridad y conservación.

La necesidad de dar una adecuada respuesta a tales retos resulta estimulada por la formidable oportunidad que la plena incorporación de la telemática supone para la actividad administrativa. (1) La mejora del servicio público, (2) la reducción en los plazos de tramitación de los procedimientos administrativos, (3) el incremento de la eficiencia mediante una drástica reducción de costes y (4) la mejor gestión del

[2] El artÌculo 18.4 de la ConstituciÛn espaÒola de 1978 dispone que la Ley limitar· el uso de la inform·tica para garantizar el honor y la intimidad personal y familiar de los ciuadanos y el pleno ejercicio de sus derechos. Debe citarse la Ley Org·nica 15/1999, de 13 de diciembre, de ProtecciÛn de Datos de Car·cter Personal.

conocimiento en las organizaciones públicas permiten presagiar la aparición en el corto plazo de una nueva Administración Pública, la Administración Pública Electrónica, caracterizada por el predominio de los procedimientos, actuaciones y documentos electrónicos.

II.-EL DOCUMENTO ADMINISTRATIVO ELECTRONICO: MARCO NORMATIVO GENERAL3.

II.1.- La necesidad de que la Administración Pública se sujete en su actuación a un determinado procedimiento no obedece a un capricho burocratizador de otra época sino que -a imagen y semejanza del proceso judicial- constituye una de las principales garantías con que cuenta la sociedad para que aquélla acierte en su pronunciamientos y para que se respeten los derechos de los particulares interesados4.

Pues bien, uno de los principios tradicionales del procedimiento administrativo es el principio de escritura (cfr.art.55.1 Ley 30/1992). Los derechos de los administrados y las potestades administrativas se obtienen, ejercitan y defienden casi exclusivamente por medio de la escritura, de documentos hasta ahora extendidos en soporte material (papel) y autenticados mediante la firma, sello o cualquier otro procedimiento asimismo material.

La informática y la telemática obligan a reformular este principio y a arbitrar los medios que permitan incorporar a los procedimientos administrativos la información obtenida, producida o remitida mediante el tratamiento automatizado5. En definitiva, hay que incorporar al procedimiento administrativo el ya denominado documento electrónico, sólo legible mediante el empleo de ordenadores y cuyo contenido no

---

[3] Dejamos fuera de nuestra atenciÛn, salvo las menciones que se estimen imprescindibles, a los marcos normativos especÌficos existentes en materia tributaria (con punto de partida en la DisposiciÛn Adicional 5™ de la Ley 30/1992); en materia de seguridad social (ex D.A.6™ y 7™ de la misma Ley) o en materia procesal (art.230 LOPJ).

[4] Conforme al artÌculo 105 de la ConstituciÛn espaÒola de 1978 la ley regular· el procedimiento a travÈs del cual deben producirse los actos administrativos, garantizado, cuando proceda, la audiencia del interesado.

[5] La Ley Modelo de la ComisiÛn de Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL-CNUDMI) prevÈ en su artÌculo 6 que cuando la Ley requiera que la informaciÛn conste por escrito, ese requisito quedar· satisfecho con un mensaje electrÛnico si la informaciÛn que Èste contiene es accesible para su ulterior consulta.

se limita a la escritura sino que puede extenderse a la imagen y al sonido.

II.2.- El legislador español ya percibió esta nueva realidad en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LPAC), cuya Exposición de Motivos declara la necesaria y abierta incorporación de las técnicas informáticas y telemáticas en la relación ciudadano-Administración, haciéndose necesario el reconocimiento formal de la validez de los documentos y, comunicaciones emitidos por vías informáticas. Se plasma esta voluntad en el artículo 45, titulado "Incorporación de medios técnicos" que es del siguiente tenor:

"1. - Las Administraciones públicas impulsarán el empleo y aplicación de las técnicas o medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que a la utilización de estos medios establecen la Constitución y las leyes.

2. - Cuando sea compatible con los medios técnicos de que dispongan las Administraciones públicas, los ciudadanos podrán relacionarse con ellas para ejercer sus derechos a través de técnicas y medios electrónicos, informáticos y telemáticos con respeto de las garantías y requisitos previstos en cada procedimiento.

3. - Los procedimientos que se tramiten y terminen en soporte informático garantizarán la identificación y el ejercicio de la competencia por el órgano que la ejerce.

4. - Los programas y aplicaciones electrónicos, informáticos y telemáticos que vayan a ser utilizados por las Administraciones Públicas para el ejercicio de sus potestades, habrán de ser previamente aprobados por el órgano competente, quien deberá difundir públicamente sus características.

5. - Los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las

Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por ésta u otras Leyes".

Sobre este precepto hay que subrayar en este momento:

a) Centra su atención en los actos jurídicos procedentes de las Administraciones Públicas y originados por procedimientos informáticos. Se trata de asegurar que efectivamente procedan de quien tiene competencia para ello, que el ejercicio de potestades se sujete a la previa publicidad del software electrónico que se emplee -pues la seguridad no la obtiene el destinatario tan intuitivamente como sucede con el papel-, y que los documentos tengan autenticidad.

b) Sin embargo la LPAC reconoce indirectamente la utilización de los medios telemáticos por parte de los ciudadanos cuando el art.70 LPAC señala como requisito del escrito de iniciación del procedimiento "Firma del solicitante o acreditación de la autenticidad de su voluntad expresada por cualquier medio".

c) El desarrollo de la Ley se ha llevado a cabo en este punto mediante 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.

II.3.- El Real Decreto 236/1996 acoge una nueva definición del documento como "entidad identificada y estructurada que contiene texto, gráficos, sonidos, imágenes o cualquier otra clase de información que puede ser almacenada, editada, extraída e intercambiada entre sistemas de tratamiento de la información o usuarios como una unidad diferenciada". Con ello se da el paso definitivo a la incorporación del documento electrónico en la actividad administrativa. Una concepción del documento más amplia que la

prevista en el artículo 49 de la Ley de Patrimonio Histórico Artístico Español (LPHE) de 1985 ("toda expresión en lenguaje natural o convencional, y cualquiera otra expresión gráfica, sonora o de imagen, recogida en cualquier tipo de soporte material, incluído el informático")y que incluso ha adquirido reconocimiento expreso en el artículo 26 del nuevo Código Penal de 1995 ("A los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica").

Interesa, asimismo destacar que el artículo 4 admite la utilización de medios telemáticos en cualquier actuación administrativa "y, en particular, en la iniciación, tramitación y terminación de los procedimientos administrativos".

Cuando las Administraciones Públicas ejerciten potestades administrativas (en la práctica, cuando actúen en los procedimientos administrativos) con medios electrónicos, informáticos y telemáticos (EIT) la aprobación y difusión pública de aquellos programas y aplicaciones que efectúen tratamientos de información cuyo resultado sea utilizado para ello deberán ser aprobadas mediante resolución del órgano administrativo que tenga atribuida la competencia para resolver el procedimiento mediante Orden Ministerial en ciertos casos de pluralidad de órganos competentes (cfr.art.9). Tanto las Ordenes ministeriales como las Resoluciones de aprobación se publicarán en el Boletín Oficial del Estado.

Por lo que respecta a las comunicaciones informatizadas entre la Administración Pública y los ciudadanos se sujeta, además de a la disponibilidad y compatibilidad de medios, a la "Existencia de medidas de seguridad tendentes a evitar la interceptación y alteración de las comunicaciones, así como los accesos no autorizados". Se alude de este modo a la confidencialidad, extremo no contemplado en el artículo 45 LPAC.

Las comunicaciones y notificaciones efectuadas en soportes magnéticos o a través de medios y aplicaciones informáticos, electrónicos y telemáticos serán válidos siempre que:

a) Exista constancia de la transmisión y recepción, de sus fechas y del contenido íntegro de las comunicaciones (integridad y no repudio).

b) Se identifique fidedignamente al remitente y al destinatario de la comunicación (autenticidad).

c) En los supuestos de comunicaciones y notificaciones dirigidas a particulares, que éstos hayan señalado el soporte, medio o aplicación como preferente para sus comunicaciones con la Administración General del Estado en cualquier momento de la iniciación o tramitación del procedimiento o del desarrollo de la actuación administrativa (voluntariedad)

Cuestión crucial es la de la fecha, y el artículo 7.4 del R.D.236/1996 que examinamos señala que las fechas de transmisión y recepción acreditadas en las comunicaciones reseñadas en los apartados anteriores serán válidas a efectos de cómputo de plazos y términos, a cuyos efectos se anotarán en los registros generales o auxiliares a que hace referencia el artículo 38 LPAC6.

Finalmente, se admite sin ambages el almacenamiento por medios o soportes electrónicos, informáticos o telemáticos de todos los documentos utilizados en las actuaciones administrativas, siempre y cuando cuenten con medidas de seguridad que garanticen la integridad, autenticidad, calidad, protección y conservación de los documentos -en particular han de asegurar la identificación de los usuarios y el control de accesos-, si bien cuando se trate de

[6] La reciente reforma de la Ley 30/1992, llevada a cabo por la Ley 4/1999, de 13 de enero modifica el artículo 38.4 a fin de impulsar nos recuerda la Exposición de Motivos- el empleo y aplicación de las técnicas y medios informáticos y telemáticos por parte de la Administración. La Ley se remite a convenios de colaboración suscritos entre las Administraciones Públicas para establecer sistemas de intercomunicación y coordinación de registros que garanticen su compatibilidad, así como la transmisión telemática de los asientos registrales y de las solicitudes, escritos, comunicaciones y documentos que se presenten en cualquiera de los registros. La proliferación en la suscripción de estos convenios avanza hacia la construcción del sistema global e intercomunicado de registros.

documentos que contengan actos administrativos que afecten a derechos e intereses de los particulares la conservación se hará en el mismo formato o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo.

II.4.- Dentro de este marco normativo general del procedimiento administrativo electrónico hay que traer a colación el reciente Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro.

Con total naturalidad, el artículo 3 de este Real Decreto indica los medios de presentación de solicitudes, escritos, comunicaciones y documentos, que se podrá efectuar (a) en soporte papel y (b) por medios informáticos, electrónicos o telemáticos, de acuerdo con lo previsto en el Real Decreto 263/1996, de 16 de febrero, ya visto. En el segundo caso se expedirá el correspondiente recibo de presentación de acuerdo con las características del soporte, medio o aplicación y deberá reunir los mismos requisitos que el artículo 6 establece para las presentaciones en soporte papel.

II.5.- Mientras que el artículo 45 de la Ley 30/1992 es norma legal de aplicación a todas las Administraciones Públicas españolas, tanto el Real Decreto 263/1996, de 16 de febrero como el Real Decreto 772/1999, de 7 de mayo, se ciñen al ámbito de la Administración General del Estado . No obstante, en tanto no exista una regulación específica en aquellas Comunidades Autónomas que tengan competencia para ello, podría acudirse a la aplicación supletoria ex art.149.3 de la Constitución de la norma estatal.

III.- ESCALA DE LA ADMINISTRACION PUBLICA ELECTRONICA.

La progresiva incorporación en la actividad de las Administraciones Públicas de las técnicas EIT (electrónicas, informáticas y telemáticas) nos permite elaborar una escala telemática de la Administración Pública y que comprendería, en grandes trazos, los siguientes niveles:

NIVELES INTERNOS

1º.- INFORMATIZACION INTERNA.

Presupuesto de la Administración Pública electrónica es su informatización interna, mediante el establecimiento de redes internas que permitan la generación, flujo y almacenamiento de los documentos electrónicos así como la conexión con redes externas (p.e. Internet).

En este sentido cabe destacar el mandato que la LPAC hace ordenando que los registros se instalen en soporte informático (art.38.3) y el esfuerzo realizado por la práctica totalidad de las Administraciones Públicas españolas así como por los registros públicos (en especial, el Registro Civil y los Registros de la Propiedad y Mercantiles).

En esta etapa hay que prestar atención a los problemas derivados de la contratación administrativa informática (para el suministro y mantenimiento de bienes y material informático), hay que velar por la protección de datos de carácter personal que se incorporen a los ficheros informáticos y, sobre todo, ha de establecerse un sistema de seguridad de la información7-imprescindible para el procedimiento administrativo electrónico-. También debe resaltarse la necesaria coordinación interadministrativa en materia de registros o de cesión de información por medios telemáticos.

2º.- PROCEDIMIENTOS ADMINISTRATIVOS INTERNOS.

La tramitación de actuaciones administrativas internas exige la comunicación de documentos electrónicos entre los distintos órganos administrativos que intervienen en el procedimiento, lo que exige añadir al contenido del nivel actual un adecuado sistema de autenticación de los documentos. Ello puede conseguirse básicamente a través de dos medios:

[7] Con observancia, en su caso, de lo dispuesto en el Real Decreto 994/1999, de 11 de junio, de Medidas Técnicas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal.

A) Mediante sistemas internos de identificación en redes internas. Así sucede con la Agencia Tributaria, donde cada usuario tiene asignado un código de identificación (login) y una password para intervenir en el sistema interno de correo electrónico (dotado de un férreo sistema de control de accesos), sistema utilizado en la reciente Resolución de 3 de mayo de 2000 de su Director General para garantizar la expedición por el órgano competente de certificaciones tributarias, a las que posteriormente haremos referencia.

B) Mediante la asignación de firmas electrónicas a los órganos o a los titulares de los órganos o incluso a los funcionarios individuales, según se empleen certificados simples o de atributos. Esta opción plantea el problema de la obtención de los dispositivos de generación y verificación de firma (a través de contratación administrativa o de convenio con una Administración Pública que actúe como entidad de certificación).

NIVELES EXTERNOS

1º.- SERVICIOS DE INFORMACION GENERAL.

En un segundo peldaño de la escala encontramos los servicios de información por medios telemáticos. Ello da lugar a relaciones por medios telemáticos entre la Administración Pública y los particulares pero sin integrar formalmente un procedimiento administrativo destinado a producir un determinado acto jurídico. Así, por ejemplo, el artículo 4 de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado (LOFAGE), recoge como manifestación del principio de servicio a los ciudadanos el que la oficina administrativa se organice de manera que los ciudadanos puedan resolver sus asuntos, ser auxiliados y recibir información de interés general por medios telefónicos, informáticos y telemáticos. Es más, el artículo 35.g LPAC reconoce el derecho de los ciudadanos a obtener información y orientación acerca de los requisitos jurídicos o

técnicos que las disposiciones vigentes impongan a los proyectos, actuaciones o solicitudes que se propongan realizar8.

En este sentido puede traerse a colación las numerosas páginas administrativas abiertas en la World Wide Web, donde los ciudadanos pueden obtener información sin entablar una relación jurídica con la Administración Pública9. Asimismo pueden formularse consultas a través de correo electrónico pero sin que sea preciso que conste la autenticidad del consultante (preguntas de interés general)

En esta etapa la Administración Pública (1) ha de disponer de un nombre de dominio10, (2) debe preocuparse por el respeto a la propiedad intelectual e industrial relacionado con la página Web y (3) puede incurrir ocasionalmente en responsabilidad patrimonial en ciertos casos.

2º.- SERVICIOS DE CONSULTA PERSONALIZADA.

El siguiente nivel de la escala lo constituyen aquellas relaciones telemáticas entabladas entre la Administración Pública y los ciudadanos con la finalidad de que éstos obtengan información particular con relación a cuestiones o expedientes que les atañen (p.e. conocer el estado de tramitación del procedimiento es un derecho reconocido al ciudadano en el artículo 35.a LPAC).

Este escalón exige acreditar la identidad del interesado y aconseja utilizar medios de comunicación seguros. En la práctica se acredita la

[8] El Real Decreto 208/1996, de 9 de febrero, por el que regulan los servicios de información administrativa y atención al ciudadano distingue entre esta información general, que se facilitar a los ciudadanos sin exigir para ello la acreditación de legitimación alguna, y la información particular sobre procedimientos en tramitación que sólo se puede facilitar a los interesados.

[9] P.e. la Resolución de 17 de marzo de 1997 de la Dirección General del Instituto Nacional de Empleo (BOE de 7 de abril; Ar.829) acuerda facilitar información al público, a través de las redes de telecomunicación, sobre los servicios que presta el mismo a los ciudadanos, derechos y obligaciones básicas de los beneficiarios de sus prestaciones, régimen jurídico de Éstas, normativa vigente, recursos económicos y estadísticos y demás extremos que se consideren adecuados y no afecten a datos de carácter personal. La información se encuentra disponible en el servidor del Instituto Nacional de Empleo: http://www.inem.es, facilitándose a través de la red Internet. De modo análogo en materia de Seguridad Social, la Resolución de 17 de enero de 1996, a través del servidor http://www.seg-social.es

[10] La Orden de 21 de marzo de 2000 regula el sistema de asignación de nombres de dominio de Internet bajo el código de país correspondiente a España (.es) (BOE 30 Mar.).

identidad mediante datos de identificación personal (DNI, NIF, otros) y el uso de palabras de paso o passwords[11].

Surge en este nivel el riesgo de una cesión indebida de datos personales, tipificada como infracción administrativa en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, que puede dar lugar a la correspondiente sanción así como a la exigencia de responsabilidad patrimonial.

3º.- PUBLICIDAD FORMAL REGISTRAL

Un caso singular es la implantación de la publicidad directa de los Registros Públicos, permitiendo la consulta telemática de los datos del archivo, a partir de la Instrucción de 17 de febrero de 1998 de la Dirección General de los Registros y del Notariado, Ar.54612). Cabe destacar el reciente servicio de acceso a la información de los Registros Mercantiles (ver http://www.registradores.org).

4º.- SERVICIOS DE REGISTRO.

El siguiente paso en la configuración de la Administración Pública electrónica es la posibilidad de que los ciudadanos presenten por medios telemáticos sus escritos, solicitudes y comunicaciones, dando lugar a la iniciación de un procedimiento administrativo.

Las exigencias de seguridad alcanzan casi su total plenitud. La relación jurídica entablada exige la acreditación de las partes intervinientes,

---

La AEAT autentica estos servicios de consulta personalizada mediante el empleo de los certificados de usuarios expedidos por la FNMT-RCM expedidos al amparo de la normativa tributaria y a través de un canal cifrado de comunicación.

[12] En los supuestos de consulta telemática de los datos del archivo, el Registrador asegurar, en todo caso, la imposibilidad de su manipulación o televaciado. Se prohibe, en consecuencia, el acceso directo, por cualquier medio, físico o telemático, a la base de datos contenida en los Archivos de los Registradores de la Propiedad y Mercantiles. Los Registradores responden, impidiendo accesos externos a las redes durante la telecomunicación, así como a los programas y a las barreras codificadas.

La solicitud por vía telemática supondrá la remisión inmediata de la información registral por correo electrónico o por otro medio, siempre que exista ruptura instantánea entre el nexo informático de solicitud y respuesta.

La intercomunicación de los Registradores por redes telemáticas utilizar técnicas de criptografía (Tercero). La Resolución de 10 de abril de 2000 de la Dirección General de los Registros y del Notariado obliga a los Registradores de la Propiedad a disponer de correo electrónico en sus oficinas para formar una red telemática de información registral inmobiliaria que permita la comunicación con cualquier interesado.

Administración Pública y ciudadano, así como la salvaguarda de la integridad de la comunicación y su confidencialidad. Lo que puede lograrse con la combinación de técnicas de firma digital o electrónica y cifrado de la comunicación.

En esta etapa se suscitan plenamente todos los problemas del procedimiento administrativo electrónico (registro, almacenamiento) y el riesgo específico que se plantea es el repudio por parte de la Administración Pública destinataria, lo que se evita con la obtención de un recibo electrónico de presentación.

Una de la manifestación más conocida de este nivel es la presentación de declaraciones tributarias por medios telemáticos ante la Agencia Estatal de Administración Tributaria.

5º.- ACTUACION ADMINISTRATIVA.

El quinto nivel de la Administración Pública Electrónica sería aquel en que la telecomunicación no sólo tiene lugar en sentido ciudadano-Administración sino también en el contrario, de manera que la Administración Pública realiza actuaciones administrativas telemáticas, lo que permite tramitar por este medio la totalidad del procedimiento administrativo.

A su vez podemos distinguir dos subniveles, según que la eficacia de la actuación administrativa dependa o no de su notificación al interesado ex artículo 57 Ley 30/1992.

En efecto, existen determinados actos administrativos que pueden ser considerados válidos y eficaces sin necesidad de su notificación al interesado. Es el caso usual de las certificaciones administrativas. Una vez producido el acto administrativo electrónico quedará a disposición del interesado para que pueda recogerlo por vía telemática, circunstancia que quedará acreditada electrónicamente. Algo similar sucede con la documentación de un procedimiento de contratación administrativa, que puede ser consultada por los interesados.

Una reciente manifestación de esta actividad administrativa la encontramos en la Resolución de 3 de mayo de 2000 del Director General de la AEAT sobre expedición por medios telemáticos de certificaciones de estar al corriente en el cumplimiento de obligaciones tributarias u otras circunstancias de carácter tributario. La autenticación del solicitante se hace mediante la utilización del certificado de usuario expedido por la FNMT al amparo de la normativa tributaria, lo que supone una utilidad añadida a la de vincular una clave pública a una persona determinada (aquí hace las funciones de DNI electrónico). La certificación es expedida por el órgano competente, quien no firma digitalmente el documento, sino que su intervención se constata mediante un código de acceso personal al que queda vinculada de manera segura cada certificación expedida utilizando dicho código de acceso13. Se trata, que conozcamos, de la primera manifestación de documentos públicos electrónicos regulados en nuestro ordenamiento jurídico14.

Por el contrario, la mayoría de los actos administrativos que afectan a los ciudadanos requieren para lograr plena eficacia de su notificación al interesado (p.e. una sanción administrativa, resolución de un recurso administrativo,…). Esta circunstancia plantea el complicado problema de las notificaciones telemáticas y la garantía de su constancia o no repudio por el destinatario .

6º.- SERVICIOS DE VALOR AÑADIDO: PAGOS ELECTRONICOS.

[13] Código alfanumérico personal proporcionado por el Departamento de Informática Tributaria de la AEAT al titular de cada Órgano competente para la expedición de certificaciones tributarias electrónicas y que permite acceder a la aplicación informática correspondiente. Este código debe mantenerse bajo exclusivo control de su titular sin perjuicio de su almacenamiento y custodia por el mencionado Departamento de Informática Tributaria a efectos exclusivamente probatorios.

[14] De conformidad con la Exposición de Motivos la certificación tributaria electrónica reúne las características precisas para gozar de la validez propia de los actos administrativos. Ahora bien, mientras no se logre la plena tramitación telemática de los procedimientos administrativos su eficacia práctica depende en gran medida de que el ordenamiento jurídico reconozca los mismos efectos a la certificación administrativa expedida en soporte papel por el Órgano competente y al documento impreso en el que se exprese el contenido propio de dicha certificación donde se sustituya la firma manuscrita por un código seguro de verificación, generado electrónicamente, que permita acceder a la certificación electrónica archivada por la Agencia Estatal de Administración Tributaria y proceder a su cotejo.

La tramitación electrónica de los procedimientos administrativos puede verse completada o enriquecida con distintos servicios de valor añadido, tales como la posibilidad de efectuar pagos directos a la Administración Pública por vía telemática (Caja Electrónica, cuestión distinta de las órdenes de pago en canales tradicionales a través de la banca electrónica) o de mantener videoconferencias con la Administración Pública, celebración de subastas electrónicas,…

IV.- CURIOSA RECEPCION DE LA FIRMA DIGITAL EN LA ADMINISTRACION PUBLICA ESPAÑOLA.

Como ya hemos comprobado, ante el tránsito de un procedimiento que se articula materialmente en torno al expediente (con sus carpetas), integrado por documentos materiales tangibles a los sentidos humanos, a otro en el que se admiten los documentos intangibles, sólo accesibles por medios electrónicos, ajenos ya definitivamente a la autografía humana -al puño y letra-, la ley exige imperiosamente arbitrar mecanismos que aseguren la autenticidad de tales documentos, junto con su integridad y conservación proporcionando la adecuada seguridad jurídica.

La principal solución que la técnica ofrece actualmente para lograr esta seguridad en el conjunto de las relaciones jurídicas telemáticas (no sólo administrativas sino también comerciales) es la firma digital, entendida como criptograma electrónico vinculado o anejo al documento que se "firma". La firma digital tiene así un carácter instrumental en las relaciones jurídicas y no es el único medio o herramienta para tratar de lograr esta seguridad (p.e. en las relaciones bancarias es habitual el uso de tarjetas de créditos con empleo de un P.I.N. o Número de Identificación Personal).

Antes de la plena incorporación de la firma digital la realidad jurídica española había acogido la existencia de documentos en soporte distinto del papel. Así, por ejemplo, la definición de documento del ya citado art.45 de la LPHE de 1985, el Sistema de Interconexión Bursátil establecido por la Ley del Mercado de Valores de 1988, los distintos pronunciamientos judiciales que admitieron como medios de prueba el

vídeo o el fichero informático o la propia normativa administrativa a que ya nos hemos referido.

Por otro lado numerosas actividades administrativas admiten el empleo de soportes magnéticos o disquetes (p.e. para la remisión de datos de los Registros Mercantiles al Registro Mercantil Central en el art.385 Reglamento del Registro Mercantil; para notificar a la Agencia de Protección de Datos los ficheros automatizados de datos de carácter personal en Resolución de 22 de junio de 1994 de dicha Agencia; para la presentación de declaraciones tributarias en numerosas Ordenes del Ministro de Economía y Hacienda15).

Asimismo se han implementado comunicaciones por medios telemáticos en redes cerradas, es decir, donde las partes intervinientes acuerdan previamente unas determinadas reglas o normas de comunicación (así el sistema Electronic Data Interchange –EDI- para la presentación telemática del Documento Unico Administrativo en el ámbito aduanero, para la remisión electrónica de datos –RED- establecido por la Tesorería General de la Seguridad Social a partir de la Orden de 3 de abril de 1995, o par la facturación electrónica desarrollada por la Orden de 22 de marzo de 1996). Este sistema se caracteriza por una importante intervención administrativa a través de la técnica de la autorización.

Sin embargo podemos afirmar que ha sido en el último trienio cuando la firma digital ha adquirido plena carta de naturaleza en el ordenamiento jurídico español. Como sabemos, la LPAC se abrió en 1992 a la nueva realidad que se avecinaba, si bien limitándose a establecer los requisitos para la admisión de los documentos administrativos electrónicos. En el mismo plano, si bien con mayor

[15] Prescindiendo de antecedentes podemos citar las Ordenes de 7 de junio de 1995; 23 de febrero y 24 de junio de 1996; 8 de mayo, 29 se septiembre, 6 de octubre y 23 de diciembre de 1997;Ö

La presentación de declaraciones tributarias en soporte magnético, que deben ser considerados como documentos presentados por los contribuyentes, presenta como principales cuestiones a resolver la del destino de los propios soportes una vez se ha incorporado la información al sistema informático de la Administración tributaria, su posible borrado siempre y cuando el sistema informático administrativo garantice el almacenamiento seguro y la obtención de copias y la prueba de la identidad y fecha de la presentación, que se obtiene por medios distintos del propio soporte magnético, al acompañarse el mismo de otros documentos en soporte papel.

detalle, se situó el R.D. de desarrollo de 1996. En esta época encontramos alguna mención de la firma electrónica, sin que conste su efectiva implementación16

Merece la pena repasar el curioso procedimiento seguido en la incorporación normativa de la firma digital al derecho español. Conforme al principio de jerarquía normativa consagrado en el artículo 9.3 de nuestra Constitución y el principio de primacía del derecho comunitario europeo el proceso normativo lógico sería el siguiente: norma comunitaria (Reglamento o Directiva); ley interna; reglamento de desarrollo de rango superior; reglamento de desarrollo de rango inferior; aplicación de las normas por los órganos judiciales. Sin embargo, como enseguida veremos, respecto de la firma digital ha operado una auténtica "inversión del proceso normativo":

1º) LA JURISPRUDENCIA DEL TRIBUNAL SUPREMO DE 1997.

Sobre este tema no podemos dejar de traer a colación la importante Sentencia del Tribunal Supremo de 3 de noviembre de 1997 (Ar.8251.P.ROUANET), donde el Alto Tribunal aborda las críticas que se vierten por el recurrente al artículo 76.3c).2 del Reglamento de ITPAJD ("a efectos de lo dispuesto anteriormente, se entenderá por documento cualquier soporte escrito, incluidos los informáticos, por los que se prueba, acredita o haga constar alguna cosa") al incluir el soporte informático con los siguientes razonamientos:

Estamos asistiendo, en cierto modo, en algunas facetas de la vida, incluso jurídica, al ocaso de la civilización del papel, de la firma manuscrita y del monopolio de la escritura sobre la realidad documental. El documento, como objeto corporal que refleja una realidad fáctica con trascendencia jurídica, no puede identificarse, ya,

[16] Es el caso de la Disposición de la Ley Catalana 19/1996, de 27 de diciembre, de Presupuestos Generales de la Generalitat para 1997, que dice así: Se autoriza al Departamento de Economía y Finanzas para que pueda establecer la utilización de un sistema de intercambio electrónico de documentos con los proveedores de la Generalidad. Este sistema debe permitir la sustitución de documentos impresos en papel por documentos grabados en soporte electrónico y la sustitución de los sistemas de autorización y control instrumental mediante sellos y diligencias por autorizaciones y controles establecidos por las mismas aplicaciones informáticas, así como, o en sustitución de los controles, validaciones de acceso restringido o firma electrónica.

en exclusiva, con el papel, como soporte, ni con la escritura, como unidad de significación. El ordenador y los ficheros que en él se almacenan constituyen, hoy día, una nueva forma de entender la materialidad de los títulos valores y, en especial, de los documentos mercantiles."

Seguidamente recorre la Sentencia la proliferación de normas legales y reglamentarias que han venido patrocinando y reconociendo el uso, con los efectos jurídicos pertinentes, del documento en soporte electrónico para señalar: "De todo ello se desprende que la admisión del documento electrónico es una realidad en nuestro ordenamiento, "sub conditione", sin embargo, de acreditar su autenticidad". El documento ha de reunir, para gozar de predicamento jurídico, "los elementos determinantes de su autenticidad y de su autoría y, en especial, la firma de quien asume su contenido y la efectividad de su clausulado".

Sigue diciendo esta interesante Sentencia -auténtico leading case-:

"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 ologrāfía, 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.

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 son 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 firma 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 (y, en especial, el documento electrónico con función de giro mercantil) 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 alfa-numéricos que permitan asegurar la procedencia y veracidad de su autoría y la autenticidad de su contenido.

Por lo tanto, si se dan todas las circunstancias necesarias para acreditar la autenticidad de los ficheros electrónicos o del contenido de los discos de los ordenadores o procesadores y se garantiza, con las pruebas periciales en su caso necesarias, la veracidad de lo documentado y la autoría de la firma electrónica utilizada, el documento mercantil en soporte informático, con función de giro, debe gozar, como establece el artículo 76.3.c del Reglamento de 1995, de plena virtualidad jurídica operativa".

En una segunda sentencia de igual fecha (Ar. 8252.P. SALA) vuelve a reiterarse por el Tribunal Supremo "la realidad de la admisión del documento electrónico, bajo condición de que quede garantizada su autenticidad, y que esto es factible, inclusive mediante lo que podría calificarse hoy de firma electrónica -cifras, códigos, claves y similares procedimientos-, es algo universalmente admitido".

Hay que llamar la atención sobre lo siguiente. El Tribunal Supremo admite la existencia la del documento electrónico y su posible autenticidad a través de medios criptográficos sin que al tiempo de dictarse la sentencia existiera en España una regulación legal específica. El documento electrónico es admisible cuando su autenticidad quede garantizada, de conformidad con los principios

generales de nuestro ordenamiento jurídico y sin necesidad de que una norma legal así lo establezca[17].

2º) ACUERDO DE 11 DE MARZO DE 1998 DE LA COMISION NACIONAL DEL MERCADO DE VALORES

El Acuerdo de 11 de marzo de 1998, de la Comisión Nacional del Mercado de Valores, implanta el sistema de CIFRA-DOC, para intercambio de información por vía telemática basado en tecnologías de cifrado y firma electrónica.

Como características principales de este sistema hemos de subrayar que la Comisión Nacional del Mercado de Valores actúa como "autoridad o entidad de certificación" (podríamos hablar en este sentido de una comunidad cerrada), siendo que gestiona las claves públicas, y que tiene un carácter hoy por hoy limitado a los envíos periódicos que venían realizándose anteriormente en soporte disquete por ciertos tipos de entidades[18].

El sistema se fundamenta directamente en el artículo 45 de la Ley 30/1992, de 26 de noviembre, y en su reglamento de desarrollo (R.D.263/1996).

3ſ) ORDEN DEL MINISTRO DE ECONOMIA Y HACIENDA DE 13 DE ABRIL DE 1999.

Con base en la habilitación genérica contenida en el artículo 79.4 de la Ley 40/1998, de 9 de diciembre, del IRPF19 (que no hacía mención alguna de la firma digital), la OM 13 abril de 1999 aplica la firma digital (que define como representación matemática cifrada de una determinada información que garantiza tanto la integridad de

[17] Ello no impide que, por razones de seguridad jurídica, el artículo 3 del reciente RD-L 14/1999 establezca la equivalencia funcional entre la firma manuscrita y la firma digital en ciertos casos.
[18] Una información más detallada del sistema en la página web de la CNMV: www.cnmv.es
[19] Los modelos de declaración se aprobarán por el Ministro de Economía y Hacienda, que establecen la forma y plazos de su presentación, así como los supuestos y condiciones de presentación de las declaraciones por medios telemáticos

dicha información como la identidad de quien la firma) para la presentación de la declaración de la renta[20].

A diferencia del sistema establecido por la CNMV ahora se configura una comunidad más abierta con la participación de una entidad distinta de la propia Administración Pública actuante y que desempeñará el papel de TTP. (Trusted Third Party) o tercero de buena fe que acredita la identidad de los comunicantes.

En efecto, las funciones de entidad certificadora se encomiendan a la Fábrica Nacional de la Moneda y Timbre, actualmente entidad pública empresarial adscrita al Ministerio de Economía, que contaba lisa y llanamente con una habilitación genérica en el art.81 Ley 66/1997 para prestar los servicios técnicos y administrativos necesarios para dar seguridad a las comunicaciones electrónicas, informáticas y telemáticas de las Administraciones Públicas con sus ciudadanos.

El procedimiento diseñado por la OM 13 abril 1999 se base en la utilización de unos certificados específicos de la FNMT (denominados X.509.V3 Clase 2) en cuya obtención actúa la propia AEAT como entidad de registro (que identifica a los interesados que desean obtener un certificado). Las relaciones jurídicas que se establecen entre la AEAT, la FNMT y los solicitantes de los certificados son de naturaleza jurídico-pública y no contractual.

4º) REAL DECRETO 1290/1999, DE 23 DE JULIO.

Posteriormente se aprueba el Real Decreto 1290/1999, de 23 de julio, por el que se desarrolla el artículo 81 de la Ley 66/1997, en materia de prestación de servicios de seguridad por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM), en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT), con las Administraciones Pública.

---

[20] . Aunque previamente ya existían comunicaciones telemáticas (p.e. declaraciones aduaneras vía E.D.I. Electronic Data Interchange; empleo de Número de Referencia Completo -NRC- por las grandes empresas conforme a la Orden Ministerial de 29 de junio de 1998[20]) los mecanismos de seguridad empleados no pueden ser calificados propiamente de firmas digitales.

Los servicios de seguridad pueden prestarse por la FNMT como autoridad o entidad de certificación no sólo en el ámbito de la Administración General del Estado y sus organismos públicos sino también respecto de las Comunidades Autónomas, entidades locales y sus correspondientes entidades de derecho público "cuando se hubiere formalizado los correspondientes convenios o acuerdos con la FNMT".

Para la prestación de los servicios de seguridad (básicamente, autenticidad y confidencialidad) la FNMT-RCM proporcionará a cada usuario un certificado electrónico previa comprobación de su identidad y capacidad, para lo que se prevé la colaboración de la entidad pública empresarial Correos y Telégrafos.

Este reglamento admite expresamente la prestación de tales servicios cuando, para el cumplimiento de las obligaciones tributarias o el pago de cualquier otro derecho económico a favor de las Administraciones Públicas incluidas en su ámbito de aplicación o, en su caso, de la propia entidad jurídica se empleen técnicas y medios EIT. Ahora bien, el segundo apartado de esta Disposición adicional declara que ello se entiende "sin perjuicio de lo que disponga la legislación tributaria". Esta declaración deja subsistentes las especialidades que respecto del régimen general diseñado en el RD 1290/1999 se contienen en la OM 13 abril 199921.

5º) REAL DECRETO-LEY 14/1999, DE 17 DE SEPTIEMBRE, DE FIRMA ELECTRONICA.

Dos meses después se promulga el Real Decreto-Ley 14/1999, de 17 de septiembre, que regula el uso de la firma electrónica, el

[21] Por tanto, a partir de julio de 1999 la prestación de servicios administrativos y técnicos de seguridad por la FNMT-RCM quedan sujetos a dos regímenes distintos. El general, previsto en el RD 1290/1999, y el específico tributario regulado por el Ministro de Economía y Hacienda en desenvolvimiento de la habilitación legal expresa contenida en el artículo 79 de la Ley 40/1998. La principal diferencia entre uno y otro régimen es el sistema de acreditación, que la OM 13 abril 1999 exige se haga mediante personación ante las oficinas de la AEAT. Esta dualidad de regímenes se consolida con las **OM de 30 septiembre y 18 noviembre de 1999** que, siguiendo el modelo de la OM 13 abril de 1999, establece las condiciones generales y el procedimiento para la presentación telemática de las declaraciones-liquidaciones correspondientes a los modelos 110, 130, 300 y 330, y al modelo 190, respectivamente.

reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación.

Uno de los principios básicos del RD-L es el régimen de libre competencia establecido en su artículo 4, que dice así: "La prestación de servicios de certificación no está sujeta a autorización previa y se realiza en régimen de libre competencia, sin que quepa establecer restricciones para los servicios de certificación que procedan de alguno de los Estados miembros de la Unión Europea."

La Disposición transitoria única del RDLey 14/1999 establece un año para que los prestadores de servicios de certificación ya establecidos en España cuya actividad se rija por una normativa específica se adapten a la nueva normativa e indica que los certificados ya expedidos que hayan surtido efectos conservarán su validez.

Por tanto nos encontramos al menos con tres regímenes normativos relativos a la firma electrónica simultáneamente vigentes. El (1) primero, establecido por Orden Ministerial; (2) el segundo, regulador por Real Decreto pero manteniendo la validez del anterior; y (3) el tercero, previsto por norma con rango de Ley y que tolera regímenes especiales en su derecho transitorio.

6º) DIRECTIVA 1999/93/CE, DE FIRMA ELECTRONICA.

En este peculiar proceso invertido de producción normativa el Real Decreto-Ley 14/1999 ha llevado a cabo una transposición anticipada al ordenamiento jurídico español de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica. Ciertamente los trabajos estaban muy avanzados y posteriormente a la norma legal española no ha experimentado cambios sustanciales.

En cualquier caso existe de plazo hasta el 19 de julio de 2001 para adoptar las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la Directiva en la

medida en que no haya sido reflejado previamente en el Real Decreto-Ley.

Como puede observarse el proceso de producción normativa se ha invertido de un modo casi perfecto, lo que sólo es explicable por la extraordinaria presión que la realidad social y económica ha generado sobre las Administraciones Públicas. Una vez el Tribunal Supremo admitió la realidad jurídica del documento electrónico quedaba despejado un camino que las Administraciones Públicas han comenzado a recorrer. La aparición sucesiva de una norma de rango superior a la anterior ha ido extendiendo progresivamente el uso de la firma digital en el conjunto de las relaciones jurídicas hasta lograr un marco común comunitario que proporcione la necesaria confianza entre todos los ciudadanos.

Establecidas las reglas jurídicas en la Directiva comunitaria y en el Real Decreto-Ley 14/1999, los distintos regímenes administrativos singulares de firma digital que iniciaron su andadura huérfanos de una norma de superior rango, deberán adecuarse a las nuevas exigencias en los plazos correspondientes (p.e. el Acuerdo de 11 de marzo de 1998 de la CNMV prevé su adaptación al régimen de prestación de servicios de seguridad por la FNMT cuando el artículo 81 de la Ley 66/1997 fuera desarrollado).

Para ello es necesario que culmine el desarrollo reglamentario del Real Decreto-Ley 14/1999, iniciado recientemente con la Orden de 21 de febrero de 2000 del Ministerio de Fomento por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica.

En el estado actual de la ciencia parece ser que el medio llamado a proporcionar en los procedimientos administrativos telemáticos la seguridad requerida es sin duda la denominada firma electrónica avanzada (dentro de la cual podemos incluir la firma digital de clave asimétrica), que podemos definir como aquel conjunto de datos, en forma electrónica (se trata de un criptograma o mensaje cifrado), anejos a otros datos electrónicos o asociados funcionalmente con ellos

(en el caso que nos ocupa, al documento electrónico que se incorpora al procedimiento administrativo), que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control (la denominada clave privada), 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 éstos22.

Mientras tanto, la celeridad con que la realidad social y política exige una actuación de las Administraciones Públicas hace que se mantenga una situación transitoria no todo lo clara que sería de desear. Las últimas manifestaciones de esta pluralidad de regímenes normativos se pone de manifiesto con dos normas:

- El artículo 51 de la Ley 55/1999 ha dispuesto que los servicios técnicos y administrativos prestados por la FNMT podrán prestarse por cualesquiera otros proveedores de servicios de certificación electrónica distintos de la FNMT-RCM y de la entidad pública empresarial Correos y Telégrafos, en condiciones no discriminatorias respecto a las establecidas en la normativa aplicable a los mismos, añadiendo que hasta tanto se lleve a cabo el desarrollo normativo del Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica, dichos proveedores de servicios de certificación podrán acogerse a lo dispuesto en la normativa establecida para la FNMT-RCM, en aquellos aspectos técnicos, informáticos y de seguridad que les sean de aplicación.

- La Orden de 28 de febrero de 2000 ha establecido las condiciones generales y el procedimiento para la renovación y revocación del certificado de usuario X.509.V3 expedido por la FNMT-RCM al amparo de la normativa tributaria, es decir,

[22] Esta definición, tomada del artículo 2 del RDLey 14/1999, de 17 de septiembre, sobre firma electrónica y 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, pone de relieve cómo la firma electrónica asegura tanto la identidad de quienes intervienen en la comunicación como su integridad, detectando cualquier manipulación o modificación de la misma. Si a ello se añade el encriptado del documento se lograría también la confidencialidad.

conforme a lo establecido en las Ordenes de 13 de abril y 30 de septiembre de 1999.

- La Orden de 24 de abril de 2000 por la que se establecen las condiciones generales y el procedimiento para la presentación telemática de las declaraciones del IRPF. Como principal novedad cabe citar la participación de las Oficinas Consulares de carrera de España en la tarea de identificación de los solicitantes de certificados.

- La Orden de 28 de abril de 2000 por la que se establecen las condiciones generales y el procedimiento para la presentación telemática de declaraciones del Impuesto sobre el Patrimonio.

Al mismo tiempo empiezan a promulgarse normas que tratan de incorporar el sistema de la firma electrónica contenido en el Real Decreto-Ley 14/1999. Así, el Real Decreto 1891/1999, de 10 de diciembre, que modifica el Reglamento General de la Gestión Financiera de la Seguridad Social, prevé que las actuaciones relativas al pago de las obligaciones de la Seguridad Social podrán ser realizados por técnicas y medios electrónicos, informáticos, "en los términos establecidos en el artículo 5 del Real Decreto-Ley 14/1999 (…) en relación con el artículo 45 de la Ley 30/1992"23. En este sentido debe destacarse la recientísima Resolución-Circular de 26 de abril de 2000 de la Dirección General de los Registros y del Notariado, sobre el ámbito de aplicación del Real Decreto-ley 14/1999, en relación con la actuación profesional de los Registradores de la Propiedad y Mercantiles (BOE 18 May). Esta Resolución-Circular admite la utilización de la firma electrónica para, en lo que nos interesa:

a) La remisión de Comunicaciones administrativas a los Registros por vía telemática y con firma electrónica avanzada.

---

[23] *Los documentos en los que se formalicen o se notifiquen a los interesados los actos a que se refiere este Reglamento, producidos o reproducidos, incluida la firma, por medios electrónicos, informáticos o telemáticos, gozarán de la validez y eficacia de los documentos originales siempre que en ellos figure la impresión mecánica del número secuencial del documento, incluidos los dígitos de verificación y la clave de identificación del centro o unidad emisor y del titular del Órgano del que emana el acto o documento de que se trate.*

b) La remisión de Documentos administrativos firmados electrónicamente y remitidos por vía telemática que deban ser calificados.
c) La emisión de publicidad formal por los Registradores con firma electrónica[24].

V.- ESPECIALIDADES DE LA FIRMA ELECTRONICA RESPECTO DE LAS ADMINISTRACIONES PUBLICAS.

Prescindiendo del ajetreado proceso de recepción de la firma digital en la actividad de la Administración Pública española es preciso examinar seguidamente de qué manera afecta el Real Decreto-Ley 14/1999 y la Directiva 1999/93/CE a la utilización de la firma digital por las Administraciones Públicas.

Una cosa debe quedar clara. Las Administraciones Públicas no han necesitado la aprobación de estas dos normas para utilizar en sus procedimientos la firma digital como mecanismo para lograr la necesaria seguridad. El artículo 45 de la Ley 30/1992 y su desarrollo reglamentario de 1996 constituyen el marco normativo general de cobertura para ello (y así se entendió por la CNMV[25]).

Más bien el nuevo marco comunitario y su anticipada transposición al derecho español viene a imponer ciertas limitaciones a las Administraciones Públicas con el propósito de salvaguardar los principios propios del mercado único. Lo que preocupa realmente al legislador es el comercio electrónico y no la Administración Pública electrónica. Pero sería ingenuo no tener en cuenta que la actitud de la segunda puede influir en el primero, por ejemplo, favoreciendo a las empresas nacionales o vulnerando las reglas propias de la

[24] Ha de subrayarse que cuando se expidan certificaciones, se aconseja que al tiempo de su expedición y antes de la remisión telemática al solicitante, su contenido íntegro y literal sea objeto de un traslado a papel y firmado con firma manuscrita por el Registrador, asignándole un número identificativo que se ha de consignar en la certificación electrónica, archivando la copia en papel (con valor de original) en el legal correspondiente por orden correlativo. Con ello se favorece su valor probatorio facilitando el cotejo. Se trata, por tanto, de una solución distinta a la prevista en la Resolución de 3 de mayo de 2000 de la AEAT respecto de la emisión de certificaciones tributarias electrónicas, donde no se prevé la conservación en soporte papel sino su archivo informático.

[25] En el caso de la Orden de 13 de abril de 1999 la cobertura, como ya vimos, procede de la habilitación específica del legislador a favor del Ministro de Economía y Hacienda.

competencia. Por ello la Directiva es plenamente consciente de que la firma electrónica se utilizará en el sector público en el marco de las administraciones nacionales y comunitaria y en la comunicación entre dichas administraciones y entre éstas y los ciudadanos y agentes económicos, por ejemplo en la contratación pública, la fiscalidad, la seguridad social, la atención sanitaria y el sistema judicial (Considerando 19 de la Exposición de Motivos).

Por otro lado, el Real Decreto-ley 14/1999 es de aplicación al conjunto de Administraciones Públicas españolas, declarando su Disposición Final Primera que encuentra su fundamento constitucional en el artículo 149.1.8ª, 18ª y 21ª de la Constitución, que atribuye competencia exclusiva al Estado en materia de legislación civil, de bases del régimen jurídico de las Administraciones Públicas y de telecomunicaciones.

Las especialidades establecidas por la Directiva comunitaria y por el Real Decreto-Ley 14/1999 respecto de la firma electrónica y la Administración Pública se caracterizan por lo siguiente:

1º.- POSIBLES REGIMENES ESPECIFICOS.

La principal especialidad relacionada con la Administración Pública es la admisión incondicionada de regímenes específicos para la utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa.

2º.- POSIBLE SUPEDITACION DEL USO DE FIRMA ELECTRONICA A PRESCRIPCIONES ADICIONALES.

Tanto la Directiva como el Real Decreto-Ley establecen un régimen de firma electrónico muy abierto, basado en la libre competencia y en la no sujeción a autorización previa de la prestación de servicios de certificación, entre los que destaca sin duda la expedición de certificados (certificación electrónica que vincula unos datos de verificación de firma –clave pública- a una persona –que firma el

mensaje con su clave privada- y confirma la identidad de ésta y que constituye la clave de bovedad del sistema de firma digital).

No obstante, frente al régimen general, el artículo 3.7 de la Directiva admite que "Los Estados miembros podrán supeditar el uso de la firma electrónica en el sector público a posibles prescripciones adicionales. Tales prescripciones serán objetivas, transparentes, proporcionadas y no discriminatorias, y sólo podrán hacer referencia a las características específicas de la aplicación de que se trate. Estas prescripciones no deberán obstaculizar los servicios transfronterizos al ciudadano".

Acogiendo este precepto el artículo 5 del Real Decreto-Ley español, rubricado "Empleo de la firma electrónica por las Administraciones públicas" establece las siguientes normas:

A) Se podrá supeditar por la normativa estatal o, en su caso, autonómica el uso de la firma electrónica en el seno de las Administraciones públicas y sus entes públicos y en las relaciones que con cualesquiera de ellos mantengan los particulares, a las condiciones adicionales que se consideren necesarias para salvaguardar las garantías de cada procedimiento.

De aquí interesa destacar en primer lugar el reconocimiento de la posible intervención normativa no sólo del Estado sino también de las Comunidades Autónomas, cosa lógica habida cuenta del reparto competencial establecido por la Constitución española y los Estatutos de Autonomía con respecto al procedimiento administrativo (cfr.art.149.1.18 CE).

Por otro lado, aunque nada se diga parece lógico incluir en esta norma el uso de la firma electrónica en las relaciones interadministrativas.

B)Las condiciones adicionales deberán garantizar el cumplimiento de lo previsto en el artículo 45 de la Ley 30/1992, de 26 de noviembre, serán objetivas, razonables y no discriminatorias y no obstaculizarán la prestación de servicios al ciudadano, cuando en ella intervengan distintas Administraciones públicas nacionales o extranjeras.

La referencia al artículo 45 es obligada, toda vez que se trata del precepto que establece en qué condiciones el documento electrónico gozará de validez y eficacia en los procedimientos administrativos.

El resto de limitaciones previstas tratan de evitar la generación de barreras que, so capa de proporcionar seguridad, actúen como medidas de efecto equivalente en contra de la libre competencia.

C) Las normas estatales que regulen las condiciones adicionales sobre el uso de la firma electrónica sólo podrán hacer referencia a las características específicas de la aplicación de que se trate y se dictarán a propuesta del Ministerio de Administraciones Públicas y previo informe del Consejo Superior de Informática.

Llama la atención que en el RDLey figure esta limitación predicable exclusivamente de las normas estatales, lo que induce a pensar que la norma autonómica puede disponer de superior margen de maniobra. No obstante si reparamos en que el artículo 3.4 de la Directiva impone esta limitación al conjunto de Estados miembros, sin distinción, consideramos que debe aplicarse tanto a las normas estatales como a las normas autonómicas, a pesar del tenor de la norma.

Un segundo problema interpretativo, de mayor calado a nuestro entender, es qué se quiere decir por "características específicas de la aplicación de que se trate". ¿Se está pensando en la aplicación de la firma electrónica entendida como finalidad o clase de procedimiento en que se utiliza? ¿O, por el contrario, se está aludiendo a la aplicación "informática" a utilizar para generar la firma electrónica?

Poca ayuda encontramos del resto de la norma. Contamos tan sólo con la previsión contenida en el Real Decreto-Ley 14/1999, y que no figura en la Directiva comunitaria, relativa al sellado de fecha.

Puede afirmarse, en nuestra opinión, que las Administraciones Públicas podrían, y seguramente deberían, admitir exclusivamente la denominada firma electrónica avanzada por ser la única susceptible de

garantizar la autenticidad del documento. Pueden traerse a colación, en este sentido, dos Instrucciones de la Dirección General de los Registros y del Notariado sobre presentación de las cuentas anuales y legalización de los libros en los Registros Mercantiles a través de procedimientos telemáticos, de 30 y 31 de diciembre de 1999, respectivamente, disponiendo que las firmas de quienes autoricen la solicitud y la relación de firmas digitales generadas por los libros cuya legalización se solicita deberán reunir los requisitos sobre firma electrónica avanzada recogidos en el Real Decreto-ley 14/1999. Es más, la ya citada Resolución-Circular de 26 de abril de 2000, de la Dirección General de los Registros y del Notariado, sobre el ámbito de aplicación del Real Decreto-Ley 14/1999 en relación con la actuación profesional de los Registradores de la Propiedad y Mercantiles (BOE 18 May) señala que la única firma electrónica que cabe aceptar en el ámbito de los Registros de la Propiedad y Mercantiles es aquella que cumpla las cuatro condiciones siguientes por razón del principio de seguridad jurídica y de titulación auténtica:

a) Estar basada la firma en un certificado "reconocido", esto es, que cumpla los requisitos establecidos en el artículo 8 del Real Decreto-ley 14/1999.
b) Haber sido producida por un dispositivo seguro de creación de firma, entendiendo por tales los que cumplen las exigencias previstas por el artículo 19 del Real Decreto-ley 14/1999.
c) Que el certificado reconocido en que esté basada la firma electrónica hay sido expedido por un prestador de servicios de certificación "acreditado", conforme al procedimiento previsto en el artículo 6 del Real Decreto-ley y a las normas que en desarrollo del mismo puedan dictarse.
d) Que el dispositivo seguro de creación de firma con el que ésta se produzca se encuentre certificado, con arreglo a lo establecido en el artículo 21 del Real Decreto-ley.

Aunque incurre en cierta confusión, toda vez que la Circular entiendo que la firma electrónica avanzada es la que cumple estos cuatro requisitos, cuando no es así, lo cierto es que sólo se admite en el

ámbito registral la firma electrónicas que goce de la presunción de equivalencia funcional establecida en el artículo 3 del Real Decreto-ley.

Y ante las grandes dificultades prácticas que puede suscitar determinar cuándo se trate de una firma electrónica avanzada y cuándo no, las Administraciones Públicas se inclinarán por admitir exclusivamente aquellas firmas basadas en un certificado reconocido expedido por un prestador de servicios de certificación acreditado y donde el dispositivo seguro de creación de firma con el que ésta se produzca se encuentre certificado, con el objeto de disfrutar de la presunción establecida en el segundo párrafo del artículo 3 del Real Decreto-Ley (equivalencia funcional con la firma manuscrita).

D) Las condiciones adicionales que se establezcan podrán incluir la prestación de un servicio de consignación de fecha y hora, respecto de los documentos electrónicos integrados en un expediente administrativo. El citado servicio consistirá en la acreditación por el prestador de servicios de certificación, o por un tercero, de la fecha y hora en que un documento electrónico es enviado por el signatario o recibido por el destinatario.

Esta singularidad de la norma española respecto de la comunitaria suscita numerosas cuestiones, todas ellas de gran interés. Quizá lo más relevante sea advertir que de hecho esta previsión puede condicionar enormemente el uso de la firma digital en los procedimientos administrativos, en la medida en que se puede exigir que su utilización vaya acompañada de un servicio de valor añadido como es el sellado de tiempo o time-stamping –por parte incluso de una persona distinta de la autoridad certificadora de la firma digital-.

Admitir el servicio de sellado de fechas como una de las condiciones adicionales que pueden establecer las Administraciones Pública, teniendo en cuenta que no se trata de una característica específica de la aplicación informática que genera la firma electrónica, permite colegir que la expresión utilizada por la norma es susceptible de interpretación en un sentido razonablemente amplio.

En cuanto al servicio propiamente dicho de la acreditación de la fecha y hora en que un documento electrónico es enviado por el signatario o recibido por el destinatario, da lugar a ciertas dudas en el ámbito de actuación de las Administraciones Públicas:

a) ¿Qué relación existirá entre esta acreditación y la que corresponde a los registros administrativos? En relaciones entre particulares es clara la utilidad de este servicio. Pero cuando interviene la Administración Pública, en un régimen como el español donde se aplica la presunción de validez de la actuación administrativa y el valor probatorio del documento público, parece más lógico que este servicio, al menos en lo que se refiere a la presentación de escritos ante las oficinas y registros telemáticos, corresponda a la propia Administración Pública (como sucede actualmente con los registros convencionales).
b) Desde la perspectiva del procedimiento administrativo es poco relevante el momento en que un documento electrónico es enviado. Lo realmente importante es cuándo ha sido recibido por el destinatario, ya se trate de la presentación en un registro administrativo o de la notificación o recepción por el ciudadano.
c) Finalmente hay que recordar la mención no sólo a la fecha sino también a la hora de la comunicación. Hoy en día la hora tiene menor relevancia en materia de cómputo de plazos (tanto el Código civil como la legislación administrativa contempla los plazos por años, meses y días, pero no por horas26) que en cuestiones tales como la apertura de oficinas al público.

E) ¿PUEDE EXTENDERSE LAS PRESCRIPCIONES O CONDICIONES ADICIONALES A LOS REQUISITOS DE IDENTIFICACION DE LOS SIGNATARIOS?

[26] Una de las excepciones en esta materia es la regulación de los Registros de la Propiedad y Mercantiles, por la importancia del principio de prioridad.

La seguridad de las relaciones jurídicas telemáticas se logra porque un tercero (proveedor de servicios de certificación) acredita mediante un certificado la procedencia de un determinado mensaje. Este certificado vincula una clave pública a una persona determinada; con dicha clave pública sólo se podrá descifrar el mensaje si ha sido encriptado con la clave privada asociada correspondiente. Si así fuera podrá colegirse que el mensaje proviene de la persona identificada en el certificado.

Este sistema tiene por tanto una de sus claves de bóveda en la identificación de la persona determinada en el certificado con la que la entidad de certificación establece la vinculación de las claves. Sin una identificación segura será imposible atribuir un mensaje al titular del certificado, toda vez que no se sabe con certeza que la clave pública corresponde realmente a quien formalmente figura como tal en el certificado.

Por ello, el artículo 11 del Real Decreto-Ley 14/1999 incluye como primera obligación de todo prestador de servicios de certificación el "Comprobar por sí o por medio de una persona física o jurídica que actúe en nombre y por cuenta suyos, la identidad y cualesquiera circunstancias personales de los solicitantes de los certificados relevantes para el fin propio de éstos, utilizando cualquiera de los medios admitidos en derecho"[27]. Este precepto plantea dos problemas distintos: por un lado, los medios empleados para la identificación; por otro, la persona que lleva a cabo la identificación.

La profesora MARTINEZ NADAL considera que en la práctica se utilizan distintos sistemas de verificación de la identidad del solicitante de un certificado, basados en el uso de una o más técnicas, o de la combinación de varias de ellas: la presencia personal junto con la presentación de documentos identificativos, los documentos acreditativos o la confirmación de datos personales por una tercera parte. Tras estudiar los medios admitidos actualmente en el derecho

[27] La Directiva, en este punto es si cabe más laxa en cuanto se limita a establecer la responsabilidad del proveedor de servicios de certificación por el perjuicio causado a quien confíe razonablemente por lo que respecta a la veracidad, en el momento de su expedición, de toda la información contenida en el certificado reconocido y la inclusión en el certificado de toda la información prescrita para los certificados reconocidos (cfr.art.6.1)

español para identificar personas, concretamente el artículo 23 de la Ley Notarial, concluye el artículo 11 excluiría cualquier otro medio de identificación en el que no exista tal personación física. "No serán admisibles, pues, no sólo los registros on-line sino tampoco las identificaciones basadas en la remisión de documentación acreditativa". Sin embargo, la propia autora entiende que ello colisionaría con la flexibilidad de la práctica, por lo que habrá que esperar al desarrollo reglamentario28.

Parece de sentido común que las Administraciones Públicas admitan exclusivamente, en aquellos procedimientos en que debe acreditarse la legitimación del interesado, aquellos certificados basados en una identificación personal y rigurosa de su titular. Lo contrario pugnaría contra principios de marcado carácter constitucional como puede ser la seguridad jurídica y la igualdad de los ciudadanos en el ejercicio de sus derechos y en el cumplimiento de sus deberes. Ahora bien, ¿estamos ante características específicas de la aplicación de que se trate?

En cualquier caso, mientras no tenga lugar un desarrollo reglamentario general del artículo 11 del Real Decreto-Ley 14/1999 es aconsejable que las Administraciones Públicas sólo consideren admisible en derecho la identificación mediante la identificación personal.

El segundo problema que suscita el artículo 11, con relación a las Administraciones Públicas es el precisar quién puede llevar a cabo la identificación de los solicitantes de certificados, es decir, quién puede actuar como entidad o autoridad de registro. Nada dice el Real Decreto-Ley ni, por supuesto, la Directiva. Pero el derecho español sólo reconoce –salvo ciertas excepciones, por ejemplo, en materia de testamentos especiales- plena validez y eficacia jurídica a las identificaciones realizadas ante un funcionario público. Principalmente a las recogidas en acta notarial y autorizadas por el Notario, pero también a las practicadas por funcionarios y plasmadas en documento público (p.e. se admite el apoderamiento mediante comparecencia

[28] Para un estudio más detallado vid. MARTINEZ NADAL, Apollónia. La Ley de Firma Electrónica. Civitas, 2000. P·g.166 y ss.

ante el órgano administrativo para la intervención en un procedimiento de tal naturaleza).

¿Puede en consecuencia exigir una Administración Pública que la identificación y el registro se haga mediante personación ante un Notario o un funcionario público? Mientras no exista un desarrollo reglamentario de la ley española entendemos que sí puede ser exigido, con el escollo que puede plantearse respecto de certificados "comunitarios" no españoles, por lo siguiente:

a) Es coherente con una adecuada interpretación del artículo 11 del Real Decreto-Ley 14/1999 en cuanto se trata del medio admitido en derecho para identificar fehacientemente a una persona.
b) Se trataría de una condición adicional exigida para salvaguardar las garantías de los procedimientos administrativos y garantizar la autenticidad exigida por el artículo 45 de la Ley 30/1992.
c) Proporciona una mayor seguridad jurídica en las relaciones jurídicas electrónicas.

Precisamente una de las principales especialidades del sistema de firma digital actualmente utilizado por la Agencia Estatal de Administración Tributaria descansa en el sistema de identificación del solicitante del certificado. Se exige su personación física ante oficinas de la propia Agencia Tributaria o ante Oficinas Consulares de carrera españolas, lo que constituye una especialidad incluso respecto del régimen general de certificados expedidos por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

Por lo que respecta al ámbito registral, la Resolución-Circular de 26 de abril de 2000 aconseja que el Colegio de Registradores de la Propiedad y Mercantiles de España asuma mediante Convenio celebrado con una entidad prestadora del servicio de certificación "acreditada" (cfr.art.6 RDLey 14/1999) la función denominada "autoridad de registro" (o entidad identificadora) en relación con los propios Registradores.

3º.- PRESTACION DE SERVICIOS DE CERTIFICACION POR LA ADMINISTRACION PUBLICA.

La Directiva comunitaria se limita a indicar en su Considerando 12 que los servicios de certificación pueden ser prestados tanto por entidades públicas como por personas físicas o jurídicas cuando así se establezca de acuerdo con el derecho nacional. De ahí que se defina el proveedor de servicios de certificación como "la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica" (art.2.11).

La principal preocupación en esta materia del Real Decreto-Ley español es que no se distorsione el régimen de libre competencia. Por ello, el artículo 4, titulado precisamente "Régimen de libre competencia", después de sentar el principio general conforme al cual la prestación de servicios de certificación no está sujeta a autorización previa y se realiza en régimen de libre competencia, sin que queda establecer restricciones para los servicios de certificación que procedan de alguno de los Estados miembros de la Unión Europea, admite la intervención de las Administraciones Públicas en un segundo apartado que dice así:

"La prestación de los servicios de certificación por las Administraciones o los organismos o sociedades de ellas dependientes se realizará con la debida separación de cuentas y con arreglo a los principios de objetividad, transparencia y no discriminación"

Nada impide, por tanto, que una Administración Pública decida constituirse ella misma, o destinar a ello una entidad pública de ella dependiente, en autoridad certificadora y llevar a cabo la identificación de los solicitantes de certificado por sí misma o con el auxilio de otras Administraciones Públicas. P.e. una Comunidad Autónoma puede crear un organismo autónomo que actúe como autoridad certificadora y constituir en entidades de registro a sus propias oficinas junto con las de las entidades locales ubicadas en su territorio.

Si esta actividad se lleva a cabo con una clara ausencia de intencionalidad mercantil, es decir, sin intervenir un precio (que no

parece un elemento esencial de la contratación de un certificado de firma electrónica a pesar del tenor del artículo 11,d del Real Decreto-Ley), su admisibilidad debería estar fuera de toda duda, independientemente del uso que, en función del nivel de confianza que genere, tenga el certificado en relaciones jurídicas entre particulares.

El problema se presenta si la actuación administrativa se hace mediando un precio, en cuyo caso habría que extremar el celo para no competir deslealmente con los certificados de las entidades certificadoras privadas[29]. Así sucedería si una Administración Pública sólo admitiera sus propios certificados que vende por un precio a los ciudadanos.

Hasta donde conocemos el único proyecto avanzado de Administración Pública como Entidad Certificadora es el de la Fábrica Nacional de la Moneda y Timbre-Real Casa de la Moneda, liderando el denominado proyecto CERES (Certificación Española)[30]. El artículo 81 de la Ley 66/1997, con el añadido operado recientemente por la Ley 55/1999, autoriza a la mencionada entidad para que preste los servicios técnicos, administrativos y de seguridad en relación con las comunicaciones electrónicas, informáticas y telemáticas entre las Administraciones Públicas y los ciudadanos, así como entre los órganos jurisdiccionales y las partes del proceso.

Asimismo procede de la Administración Pública corporativa el proyecto CAMERFIRMA, impulsado por las Cámaras de Comercio, Industria y Navegación, que actúan como Autoridades Locales de Registros, representantes del Consejo Superior de Cámaras de España, quien

[29] Por tanto, la prestación de servicios de certificación por parte de las entidades públicas no debería contravenir en modo alguno el principio de libre competencia en perjuicio de las entidades de certificación privada. Y ello nos plantea cuestiones como la de si los certificados emitidos por una entidad pública pueden ser utilizados no sólo con fines de comunicación con la Administración Pública sino también para otros fines distintos (p.ej. usos comerciales), en cuyo caso competirían, y no en igualdad de condiciones, con los certificados de las entidades certificadoras privadas y comerciales. MARTINEZ NADAL, Apol.lónia, op.cit.p·g.160.

[30] En líneas generales consiste en establecer una Entidad Pública de Certificación, que permita autentificar y garantizar la confidencialidad de las comunicaciones entre ciudadanos, empresas u otras instituciones y Administraciones Públicas a través de redes abiertas de comunicación. Mayor información en http://www.cert.fnmt.es/que_es_ceres.htm

actúa como Autoridad de Certificación y como interlocutor a nivel internacional (red de confianza Chambersign)[31].

4º.- ESPECIALIDADES TRIBUTARIAS.

Finalmente, el artículo 5 del Real Decreto-Ley autoriza al Ministro de Economía y Hacienda para que, respetando las condiciones previstas en este Real Decreto-Ley, pueda establecer un régimen normativo destinado a garantizar el cumplimiento de las obligaciones tributarias, determinando, respecto de la gestión de los tributos, la posibilidad de que el signatario sea una persona física o una persona jurídica.

Esta norma no cuenta con un precedente inmediato en la Directiva comunitaria, por lo que, en ausencia de debate parlamentario, resulta difícil comprender su exacto sentido, con excepción de su inciso final. En efecto, salvo la posibilidad de que el signatario de una firma electrónica sea una persona jurídica nada más se dice. La clave de la cuestión estriba en la interpretación que deba darse a la expresión "respetando las condiciones previstas en este Real Decreto-Ley", pues no existe ningún epígrafe ni título en la norma que establezca precisamente cuáles son esas condiciones[32]. En todo caso es claro que ha de respetarse el contenido propio de la Directiva comunitaria, por virtud de la primacía del derecho comunitario.

El reto que actualmente se le plantea a la Administración tributaria es adaptar el sistema de firma electrónica que lleva ya implantado un año (establecido en las Ordenes de 13 de abril y 30 de septiembre de 1999) a las condiciones previstas en el Real Decreto-Ley y al pleno respecto al derecho comunitario.

VI.- POSIBILIDAD DE QUE LAS PERSONAS JURIDICAS SEAN SIGNATARIAS.

[31] El objetivo es definir y ofrecer a las empresas un certificado digital de alta calidad, deseado específicamente para las necesidades de las empresas y con reconocimiento internacional basado en la garantía que supone su emisión por una Cámara de Comercio. Mayor información en: http://www.camerfirma.com

[32] Ya hemos visto que el uso de la firma electrónica en las Administraciones Públicas puede supeditarse si las condiciones adicionales que se consideren necesarias, para salvaguardar las garantías de cada procedimiento. Pero condiciones adicionales a cuáles? a las condiciones previstas en este Real Decreto-Ley a que alude el inciso relativo a las obligaciones tributarias?

Se entiende por signataria la persona que signa o firma electrónicamente el documento electrónico.

La única especialidad explicitada en el Real Decreto-Ley 14/1999 respecto del uso de firma electrónica para el cumplimiento de las obligaciones tributarias consiste en la posibilidad de que el signatario sea una persona jurídica. Es una excepción a la definición de signatario contenida en el artículo 2.c 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".

Parece, prima facie, que el legislador español ha escogido entre las diversas opciones que ofrece la definición más neutra de "Firmante" contenida en el artículo 2.3 de la Directiva ("la persona que está en posesión de un dispositivo de creación de firma y actúa en su propio nombre o en el de la entidad o persona física o jurídica a la que representa"). Sin embargo la Directiva comunitaria sí se pronuncia de modo implícito en el Anexo I. Al referir los requisitos de los certificados reconocidos la letra c) dice así: "el nombre y los apellidos del firmante o un seudónimo que conste como tal".

Podría, en consecuencia, concluirse que la Directiva no contempla tampoco la posible firma electrónica de una persona jurídica, por lo que la especialidad tributaria contenida en la norma española no sólo merece una clara explicación sino que podría llegar a contravenir el marco normativo comunitario.

Sin embargo un análisis más reposado de ambas normativas delata que tanto una como otra admiten claramente que las personas jurídicas, o al menos algunas de ellas, pueden ser signatarias de una firma electrónica. En efecto, el mencionado Anexo I de la Directiva incluye entre los requisitos de los certificados reconocidos "la firma electrónica avanzada del proveedor de servicios de certificación que expide el certificado", proveedor que, como es sabido, puede ser una persona física o jurídica. No se habla de la firma electrónica del representante del proveedor de servicios de certificación sino del

propio proveedor. Idéntico tenor literal se observa en el artículo 8.d del Real Decreto-Ley 14/1999.

1º.- POR QUÉ DE LA ESPECIALIDAD TRIBUTARIA.

Es lógico que nos preguntemos por qué el artículo 5 contiene tan singular especialidad en materia tributaria.

La explicación puede hallarse en el extraño proceso de implantación de la firma electrónica en los procedimientos administrativos españoles, que se detalló anteriomente. Ya la Orden de 13 de abril de 1999, primera que aplica la firma digital de clave asimétrica en la presentación de declaraciones tributarias prevé que los titulares de certificados sean personas jurídicas (entidades), en tanto en cuanto autorizadas para presentar declaraciones del Impuesto sobre la Renta de las Personas Físicas en representación de terceras personas. La Orden de 30 de septiembre de 1999, por su parte, contempla la presentación telemática de declaraciones de retenciones practicadas por empresarios admitiéndose que las personas jurídicas contribuyentes sean titulares de certificados.

Cuando se tramitó el actual Real Decreto-Ley ya habían sido expedidos miles de certificados a personas jurídicas, por lo que se consideró adecuado mantener una posibilidad que era ya una realidad que funcionaba perfectamente, faltando valentía para generalizar esta posibilidad.

2º.- POSIBLE CONDICION DE SIGNATARIA DE LA PERSONA JURIDICA.

La posibilidad de que una persona jurídica firme electrónicamente un documento resulta no sólo de la experiencia tributaria sino del reconocimiento implícito contenido en la Directiva comunitaria y en el Real Decreto-Ley 14/1999.

Para abordar el problema hemos de remitirnos de nuevo a MARTINEZ NADAL quien ha estudiado las formas teóricamente posibles de vinculación electrónica de una persona jurídica, distinguiendo tres

supuestos: (a) el titular del certificado sea la persona física con poder de representación de la persona jurídica; (b) la persona jurídica es la titular del certificado; (c) el certificado se emite para una persona jurídica pero haciendo constar en uno de los campos opcionales del certificado la persona autorizada para firmar digitalmente en nombre de la sociedad titular del certificado. La autora citada se pronuncia a favor de un régimen general de representación (incluso sin necesidad de que el certificado contuviera como atributo el poder de representación de la persona jurídica, siendo suficiente su mención en el documento, con lo que se evitaría posible discordancia entre la apariencia registral y la derivada del sistema de certificados respecto de un determinado poder de representación) junto con la admisión en algunos supuestos de firma de la persona jurídica para pequeñas transacciones en las que tradicionalmente no se identifica al vendedor ni se examinan los poderes de representación[33].

La mayoría de los estudios al respecto (y de las legislaciones que conocemos) parten de la necesaria presencia de una persona física que vincule a la persona jurídica, pues éstas sólo pueden actuar a través de la única persona que puede firmar, esto es, de la persona natural o física. Sin embargo, la utilización del término "firma" e incluso la homologación o equivalencia funcional entre la firma manuscrita y la firma electrónica que establece la Ley en ciertos supuestos no debe ocultar una realidad. La firma electrónica no es una firma manuscrita sino un criptograma que, merced a ciertos principios y requisitos técnicos, vincula un documento a una autoría determinada y acredita su integridad. Parece guardar mayor proximidad con el tradicional "sello lacrado" que con la genuina firma manuscrita. De hecho la legislación alemana emplea el término sello para definir qué sea la firma electrónica (aunque, ciertamente, sólo parece reconocer como signatarias a las personas físicas). Esta peculiaridad permite que una misma persona sea titular de varios certificados de usos variados, o que se puedan emplear pseudónimos. Alguna doctrina empieza a calificar a la firma digital como "sigillum informaticus" (SILVIA

[33] Martínez Nadal, Apollónia. El Comercio Electrónico, Firma Digital y Autoridades de Certificación î. Civitas, 1998. P·g.138 y ss.

MICCOLI, GAETE GONZALEZ) que desempeña una doble función, identificativa y declarativa de voluntad.

Aunque se afirme, como hace el art.3 del Real Decreto-Ley 14/1999 la regla de equivalencia funcional entre las firmas manuscrita y electrónica, existe una importante diferencia en el tráfico jurídico. Mientras que la firma manuscrita suele acompañarse de algún mecanismo de identificación de quien la hace valer (p.e. identificación mediante D.N.I. de quien presenta un documento en un registro público), la firma electrónica queda dispensada de tal requisito, precisamente porque vincula per se al signatario en virtud de un certificado cuya expedición viene precedida precisamente de la identificación.

Si consideramos la firma electrónica como un sello electrónico que vincula a su titular ningún obstáculo existe para que tal vinculación se establezca no sólo con personas naturales sino también jurídicas. Será responsabilidad de su titular la custodia y buen uso del "sello", tal como acontece hoy en día en el tráfico jurídico. ¿Acaso los sellos de registro de las Administraciones Públicas recogen el nombre del funcionario que sella el documento que se presenta en la oficina pública? Si el procedimiento de solicitud y entrega del certificado se hace con plenas garantías la titularidad del mismo puede corresponder a una persona jurídica. En puridad, no se trataría más de llevar a un estadio superior la propia ficción de la personalidad jurídica, ficción imposible en las relaciones jurídicas en soporte papel pero que puede dejar de serlo cuando la relaciones dejan de ser físicas para pasar a ser lógica y simplemente "jurídicas".

La solicitud del certificado de la persona jurídica sólo puede proceder del administrador, que tiene capacidad general para gestionar el objeto social, o de apoderado con poder al efecto. En caso de cese o cambio de la persona física que utiliza el certificado ésta deberá "devolverlo" -de modo análogo a como se hace con las llaves de la oficina-; y en función de la confianza entre empresa y empleado o según las circunstancias siempre se podrá revocar el certificado y solicitar uno nuevo –de igual manera que se pueden cambiar las cerraduras-.

Hay que reconocer que se trata de una cuestión muy sugestiva pero que requiere una reflexión más profunda y sosegada. Habrá que profundizar en su estudio y comprobar los efectos prácticos, positivos y negativos, de esta posibilidad.

VII.- HACIA EL PROCEDIMIENTO ADMINISTRATIVO ELECTRONICO: ALGUNAS CUESTIONES.

La informatización de las Administraciones Públicas y la seguridad proporcionada por la firma digital permite avanzar hacia el diseño y funcionamiento de los procedimientos administrativos electrónicos tramitados por la Administración Pública Electrónica. Una Administración para la que desaparecen en gran medida las limitaciones derivadas del tiempo y del espacio, pudiendo lograr sus objetivos con una reducción considerable de costes (y aumento correlativo de la eficiencia) y un incremento espectacular de la celeridad de las relaciones jurídicas sin merma de la seguridad.

Esta nueva Administración Pública deberá implantarse gradualmente, de forma progresiva, en función de los medios técnicos de las distintas Administraciones Públicas. Debe ser neutral respecto de la Administración Pública tradicional, evitando mayores formalismos y cargas de los ciudadanos que los derivados de la tramitación en soporte papel. Asimismo el marco legal actual sólo permite que se plantee como alternativa a los ciudadanos, los cuales podrán escoger entre un medio u otro de tramitación de los procedimientos[34]

Algunas cuestiones que deberán abordarse respecto de los procedimientos administrativos electrónicos y que dejamos sólo apuntadas y pendientes de estudio:

a) Deslocalización de la Administración Pública: las actuaciones administrativas se pueden producir desde lugares

[34] Sin perjuicio de las excepciones que puedan darse. Así sucede con la presentación de ciertas declaraciones ante la Agencia Tributaria que las grandes empresas están obligadas a presentar por medios telemáticos, por razones gestoras de eficacia y con fundamento legal en la Disposición Final 5™ de la Ley 66/1997.

distantes de la ubicación del administrado, que pueden incluso ser ignorados, lo que proporciona una gran flexibilidad para ubicar físicamente los órganos administrativos con competencias electrónicas. Cualquier Administración Pública puede estar próxima al ciudadano, poniendo en crisis conceptos como el de "Administración única".

b) Simplificación y automatización de los procedimientos: para lograr una adecuada eficiencia técnica deberán reducirse al mínimo posible la pluralidad de procedimientos administrativos, tratando de optimizar el uso de las aplicaciones informáticas. Sin caer en la "cibercracia" o dictadura de la aplicación informática que puede llegar a imponerse a la norma escrita, podrán diseñarse, más allá del registro, procedimientos administrativos automatizados (p.e. obtención de licencias o certificaciones en tiempo real)[35] .

c) Registro y archivo electrónicos: Como es sabido los registros administrativos deben estar informatizados. Sin embargo, el procedimiento electrónico exige un registro de tal carácter que tiene algunos rasgos propios, como son la deslocalización (puede recibir escritos desde cualquier lugar del mundo) o la tramitación automatizada (posible expedición de recibos de presentación con la firma digital de la Administración Pública, en cualquier día y hora). Se trataría de un órgano administrativo peculiar al frente del cual hay un responsable que no interviene en cada actuación sino que vigila y controla el buen funcionamiento. En cuanto al archivo electrónico, exige garantizar el derecho a la obtención de copias de documentos presentados por los ciudadanos (art.35.c Ley 30/1992).

d) Personalización de procedimientos administrativos: Los ciudadanos pueden escoger actualmente el lugar y medio de

[35] El artículo 13 de la Ley Modelo UNCITRAL ya citada entiende que un mensaje electrónico proviene del remitente si ha sido enviado *por un sistema de información programado por el remitente o en su nombre para que opere automáticamente*.

notificación con ocasión de un procedimiento determinado. El procedimiento electrónico permitirá personalizar de modo extraordinario la tramitación (admisión de comparecencias electrónicas y videoconferencias), tanto respecto del formato como del contenido de los documentos (p.e. presentación de un recurso en entorno multimedia).

e) Notificaciones electrónicas: auténtico desafío del procedimiento electrónico. La Ley deja la puerta abierta a esta posibilidad al recoger como contenido de las solicitudes (art.70 LPAC) o de la interposición de recursos (art.110.1.c LPAC) "la identificación del medio preferente o del lugar que se señale a efectos de notificaciones". No obstante se plantea el problema del posible repudio en destino de las comunicaciones electrónicas.

f) Cómputo de plazos del procedimiento: reconsideración de los días hábiles; introducción de las horas.

g) Posible aplicación de técnicas de traducción automática: En nuestro país existen Comunidades Autónomas con varias lenguas oficiales, todas las cuales pueden emplearse en la tramitación de los procedimientos administrativos. El procedimiento electrónico permitirá traducir automáticamente aquellos documentos que deban surtir sus efectos en otros territorios donde no sea oficial la lengua en que se aquél se encuentra redactado.

h) Presunción de la representación a través del colaborador administrativo.

La firma electrónica actúa como palanca que remueve el principal obstáculo existente para el pleno desarrollo de la Administración Pública Electrónica, verdadera Nueva Administración, al garantizar la autenticidad e integridad de las comunicaciones electrónicas. No obstante, se trata de una condición necesaria pero no suficiente para el total logro del procedimiento administrativo electrónico que requiere

soluciones en materia de confidencialidad, no repudio y registro y almacenamiento.