Identificación y autenticación en la Ley de Administración electrónica

José Félix Muñoz Soro
Investigador de la Agencia Aragonesa para la Investigación y el Desarrollo (ARAID)

SUMARIO. 1. Introducción. 2. La identidad electrónica. 3. La autenticación de los documentos. 4. Los certificados electrónicos. 5. La firma electrónica y la Administración electrónica. 6. Los medios de identificación y autenticación de los administrados. 7. La identificación y autenticación de las Administraciones Públicas. 8. La identificación y autenticación de los empleados de las Administraciones Públicas. 9. Algunos retos. 10. Conclusión.

Resumen

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, regula los distintos medios admitidos para la identificación de los ciudadanos, de las Administraciones Públicas y de sus empleados, así como para la autenticación de los documentos emitidos por todos ellos. La firma electrónica avanzada, regulada en la Ley 59/2003, de 19 de diciembre, de firma electrónica, es el mecanismo básico a utilizar, pero la LAE, con un marcado sentido práctico, admite también otros medios basados en la firma electrónica no avanzada. El conjunto de todos ellos crea un completo marco de herramientas con el que se facilita el desarrollo de las operatorias de Administración electrónica por parte de las Administraciones Públicas españolas.

1. Introducción

Después de un período, que comenzó en 1992, en el que la Administración electrónica ha evolucionado en base a normas dispersas, la publicación de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos constituye un hito, ya que por primera vez hay una norma que reúne y sistematiza todas las cuestiones relacionadas con la Administración electrónica. Precisamente por este carácter de regulación integral, parte de la doctrina ha optado por referirse a

Serie Claves del Gobierno Local, 12
ISBN: 978-84-614-0970-9
Fundación Democracia y Gobierno Local

ella como Ley de Administración electrónica (LAE), opción que seguiremos en este artículo.[1]

Entre las cuestiones que trata la LAE ocupa un lugar destacado la utilización de la firma electrónica, elemento imprescindible para la realización de trámites utilizando medios electrónicos, y que está regulada por la Ley 59/2003, de 19 de diciembre, de firma electrónica (LFE)[2] y la Directiva 1999/93, de 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica. La importancia de la firma electrónica deriva de la obligación que la LAE establece para las Administraciones Públicas de que garanticen la seguridad de sus operatorias de Administración electrónica. Esta seguridad exige tanto identificar a las personas, físicas o jurídicas, que actúan en un determinado momento, como garantizar la autenticidad e integridad de los documentos electrónicos generados por las mismas.

Uno de los aspectos en los que cabe esperar que la LAE suponga una aportación importante es el de la terminología con la que nos referimos a los diferentes elementos y funciones asociados con la Administración electrónica. No es éste, ni mucho menos, un aspecto secundario, porque la imprecisión a la hora de denominar los conceptos añade una notable dificultad a la adecuada comprensión de cuestiones que, por su propia naturaleza, ya resultan bastante difíciles para los juristas. En este sentido, la Ley diferencia claramente dos funciones: la identificación, que se refiere a las personas, y la autenticación, que se aplica a los documentos. En ambos casos el objetivo es similar, se trata de conocer con seguridad el origen, en el primer caso, de una acción y, en el segundo caso, de un documento. Para la realización de estas dos funciones utilizamos los certificados electrónicos.

Por otra parte, la firma electrónica no es algo que tenga que ver únicamente con la Administración electrónica, sino que es un elemento importante en el conjunto de la sociedad de la información. Por ello, antes de entrar a estudiar la regulación de la LAE nos detendremos, en primer lugar, en establecer el marco global en el que se desarrollan los sistemas de identificación y autenticación, y en segundo lugar, en explicar brevemente los fundamentos técnicos en que se basa la firma electrónica. Una vez vistos estos puntos entraremos a detallar los diferentes mecanismos que para la identificación de los diversos agentes y la autenticación de los documentos prevé

1. Es el caso de E. Gamero, J. Valero (eds.), *La Ley de Administración Electrónica*, Thompson-Aranzadi, Cizur Menor, 2008, p. 61. Por otra parte, la Ley ha sido desarrollada parcialmente para la Administración General del Estado por el Real Decreto 1671/2009, de 6 de noviembre.

2. La Ley derogó la primera norma promulgada en nuestro país sobre la materia, el Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica.

Serie Claves del Gobierno Local, 12 Fundación Democracia y Gobierno Local
ISBN: 978-84-614-0970-9

la LAE. Finalmente, haremos alguna consideración sobre las dificultades que aún plantean ambas cuestiones y las perspectivas para su desarrollo.

2. La identidad electrónica

Ya en los primeros sistemas informáticos apareció la necesidad de poder identificar a la persona que realizaba las acciones en un ordenador, mucho más en cuanto los primeros equipos eran multiusuario y un gran número de personas compartían su uso. Se estableció entonces un método de identificación que sigue siendo, con gran diferencia, el más utilizado: la combinación de un nombre de usuario y una contraseña.

Este método está en el primero de los tres niveles que suelen distinguirse, en el ámbito informático de las medidas de seguridad, a la hora de clasificar los medios para la identificación de una persona. El primer nivel (algo que se sabe) se basa en la revelación a quien identifica de algo que únicamente la persona identificada sabe, como es el caso de una contraseña o un PIN;[3] el segundo (algo que se tiene) consiste en probar la posesión de un objeto que únicamente debe tener la persona identificada, como, por ejemplo, una tarjeta de crédito; finalmente, el tercer nivel (algo que se es) consiste en la verificación de rasgos físicos que son característicos de cada persona, como es el caso de la huella dactilar.[4]

Desde un punto de vista conceptual, los métodos de identificación basados en claves criptográficas pertenecen al primer nivel, ya que las claves que se utilizan no son sino números. Lo que ocurre es que se trata de cifras de gran longitud, imposibles de memorizar por una persona normal y, por tanto, en la práctica la identificación mediante claves criptográficas equivale a comprobar que la persona posee el soporte en el que se ha almacenado la clave.[5] Como medida adicional de seguridad, el acceso al soporte donde se almacena la clave exige introducir una contraseña o PIN, de forma que, al igual

3. Siglas de *Personal Identification Number* o número de identificación personal.

4. En el ámbito técnico se denominan medidas biométricas. Actualmente ya está muy extendido el uso de la huella dactilar. Otro rasgo característico que se utiliza es la coloración del iris del ojo, que se examina mediante un rayo láser. También están ya en avanzado grado de desarrollo los sistemas de reconocimiento facial, capaces de identificar a una persona mediante la imagen de su rostro. Estos últimos plantean el problema de que pueden ser utilizados para reconocer a las personas de forma automatizada sin su conocimiento, por ejemplo, mediante imágenes tomadas por cámaras situadas en la vía pública.

5. Las claves comúnmente utilizadas tienen 1024 bits, lo que equivale a un número decimal de 309 dígitos. En algunos de los sistemas más utilizados las claves se guardan en el propio ordenador, aunque cada vez se extiende más la utilización de *tokens* criptográficos, como la tarjeta del DNI electrónico, en cuyo interior se guardan las claves con grandes medidas de seguridad.

Serie Claves del Gobierno Local, 12
ISBN: 978-84-614-0970-9
Fundación Democracia y Gobierno Local

que ocurre con las tarjetas de crédito, se combinan dos de los niveles de identificación: algo que se tiene (la tarjeta) y algo que se sabe (el PIN que la protege).[6]

Pero la identidad digital no es únicamente una cuestión técnica. Conforme aumenta la completitud y complejidad de las redes y, por tanto, la cantidad y diversidad de acciones que podemos realizar en las mismas, más importante se vuelve la cuestión de qué identidad o identidades podemos utilizar ante cada una de las entidades o personas con las que interactuamos. Una gran parte de los expertos opina que obligar a las personas a actuar siempre bajo una única identidad es incompatible con el derecho a la intimidad[7] y que, por tanto, es preciso crear un marco más flexible para la identidad electrónica, que permita utilizar en el mundo virtual recursos como el anonimato o los apodos.

Partiendo del hecho de que, al menos en un futuro próximo, el medio de identificación más utilizado serán los certificados electrónicos, aparecen distintos tipos, cuyo conjunto integra el esquema global que nos permite gestionar nuestra identidad electrónica. En primer lugar, según su función, distinguimos tres clases de certificados. Los que denominamos "personales" identifican a la persona física y se basan en medios muy seguros de comprobación de la identidad, normalmente fundados en documentos públicos como la partida de nacimiento. Suelen ser emitidos por el Estado o agencias delegadas del mismo y, dado su alto nivel de seguridad, pueden servir de base para la generación de otros medios de identificación.[8] La segunda clase son los certificados "corporativos", que establecen la vinculación con una organización y pueden ser de distintos tipos como, por ejemplo, de cargo o representante de una entidad privada, de cargo electo, de funcionario o empleado de una Administración Pública, o de miembro de un colegio profesional. Finalmente, la tercera categoría, a la que denominamos certificados "de cliente", se utiliza cuando existe una relación de negocio, normalmente para identificar a los clientes de una determinada empresa. Estos últimos son, hoy por hoy, los medios de identificación más utilizados.

Una segunda clasificación distingue también tres clases de medios de identificación, según quien es el emisor. La primera categoría son los certificados "de tercera

6. Hay prototipos de *tokens* criptográficos que comprueban una medida biométrica, normalmente la huella dactilar, para permitir el acceso a las claves. Se trata de métodos que combinan algo que se tiene con algo que se es y tienen la gran ventaja de no poder ser cedidos a otras personas.

7. La aceptación de un identificador único, el número del DNI, está profundamente arraigada en nuestro país, pero no ocurre así en otros lugares, como los países anglosajones o Portugal, país cuya Constitución, de 2 de abril de 1976, dice en su artículo 35, 3.º, que "se prohíbe atribuir un numero nacional único a los ciudadanos".

8. Es el caso, por ejemplo, de la apertura de una cuenta corriente en un banco en Internet utilizando el DNI electrónico. Este puede servir al banco de base para la emisión de medios de identificación "de cliente", como el PIN que nos permitirá acceder a su web.

Serie Claves del Gobierno Local, 12 Fundación Democracia y Gobierno Local
ISBN: 978-84-614-0970-9

parte", que se emiten para su uso en relaciones con entidades ajenas al emisor. Es el caso de los certificados expedidos por Prestadores de Servicios de Certificación, como la Fábrica Nacional de Moneda y Timbre (FNMT). Una segunda categoría son los medios de identificación "de segunda parte", que una entidad nos proporciona para las relaciones que mantenemos con la misma. Ejemplos típicos son las tarjetas de empleado o el PIN que nos proporciona una entidad bancaria para el acceso a su banca electrónica. Finalmente hay mecanismos de identificación que podemos generar nosotros mismos sin necesidad de que nadie nos los dé, son los medios "de primera parte". Aunque en principio pueda parecer un concepto extraño, su uso es bastante frecuente entre los internautas. Así, por ejemplo, cuando alguien se da de alta en las redes sociales o en sitios web como *SecondLife*, crea libremente una identidad y unos medios de identificación asociados a la misma, sin que nadie verifique la veracidad de los datos aportados.[9] La existencia de esta última clase de medios de identificación, cuyo control queda únicamente en manos del titular, es importante para garantizar el libre desenvolvimiento de las personas en Internet.

3. La autenticación de los documentos

En el ámbito jurídico, las acciones de las personas y, en particular, las decisiones que éstas adoptan, individualmente o como miembros de una organización, quedan plasmadas en documentos. Y, por ello, desde hace unos 5.000 años la actividad de las burocracias se basa en los documentos en papel, en torno a los cuales se ha construido toda la arquitectura del tráfico jurídico, tanto en el Derecho privado como en el público.[10] De hecho, podemos decir que la circunstancia más característica del actual momento en la evolución de los sistemas de información en las organizaciones es precisamente la sustitución de los documentos en papel por sus equivalentes electrónicos.[11] Éste no es un mero cambio instrumental, sino que afecta de manera profunda a la forma en la que los procedimientos se sustancian y, con ello, a la forma en la que se desenvuelven las organizaciones y la sociedad en los aspectos jurídicamente ordenados.[12]

---

9. I. Alamillo, "Identidad en la red", *Investigación y Ciencia*, 386, noviembre 2008, p. 54-61.

10. "La burocracia funda su poder sobre la cosa escrita y sobre la acumulación de las cosas escritas", H. Lefebvre, *La vie quotidienne dans le monde moderne*, Gallimard, París, 1968.

11. Bing divide la evolución de los sistemas de información en las organizaciones en tres generaciones: la primera utiliza sistemas orientados a los datos; la segunda, orientados a los documentos, y la tercera (aún por llegar), orientados al conocimiento (J. Bing, "Three generations of computerized systems for public administration and some implications for legal decision-making", *Ratio Iuris* 3/2, 1990, p. 225). El autor desarrolla ampliamente esta propuesta en J. F. Muñoz, *Decisión jurídica y sistemas de información*, Colegio de Registradores, Madrid, 2003, p. 77 y ss.

12. La LFE, según la redacción dada por la Ley 56/2007, de 28 diciembre, de Medidas de Impulso de la Sociedad de la Información, define el documento electrónico en el apartado 5 del artículo 3, como "la información de cualquier naturaleza en forma electrónica, archivada en un

Serie Claves del Gobierno Local, 12
ISBN: 978-84-614-0970-9
Fundación Democracia y Gobierno Local

Pero, para que los documentos electrónicos puedan sustituir a sus homólogos en soporte papel en las funciones relacionadas con la prueba documental, es preciso garantizar que cumplen con dos requerimientos básicos: la autenticidad de origen y la garantía de integridad. El primero significa que debemos ser capaces de conocer con seguridad cuál o cuáles son la persona o las personas que crearon un determinado documento. El segundo consiste en que, una vez creado el documento, su contenido no pueda ser modificado sin que lo detectemos. La LAE se refiere con el término autenticación al método que permite a los documentos electrónicos satisfacer estos dos requisitos.

La firma electrónica es el mecanismo técnico-jurídico que utilizamos para autenticar los documentos. Desde el punto de vista técnico, el problema consiste en que, a diferencia de los documentos en papel, que son objetos del mundo físico y por tanto únicos, los documentos electrónicos se materializan mediante codificaciones informáticas que no son sino larguísimos números, representados en una base binaria formada por ceros y unos. Por tanto, la existencia de los documentos electrónicos es abstracta y carecen de identidad única. ¿Cómo es posible, entonces, conocer con exactitud cuál es el origen de un documento?

El problema se resuelve mediante la denominada criptografía moderna, en la que se utiliza una pareja de claves, tales que lo que se cifra con una de ellas sólo puede descifrarse con la otra. En su uso práctico, hay una que denominamos "clave privada", ya que sólo debe poseerla el firmante, y otra que denominamos "clave pública", porque se da a conocer de forma pública.[13] Para garantizar la autenticidad de origen del documento, el emisor añade a éste una firma cifrada con su clave privada. Luego, el destinatario utilizará la clave pública del emisor para verificar la firma. En consecuencia, utilizando la terminología de la LFE, decimos que la clave privada es el "mecanismo de creación de firma" y la clave pública el "mecanismo de reconocimiento de firma".

---

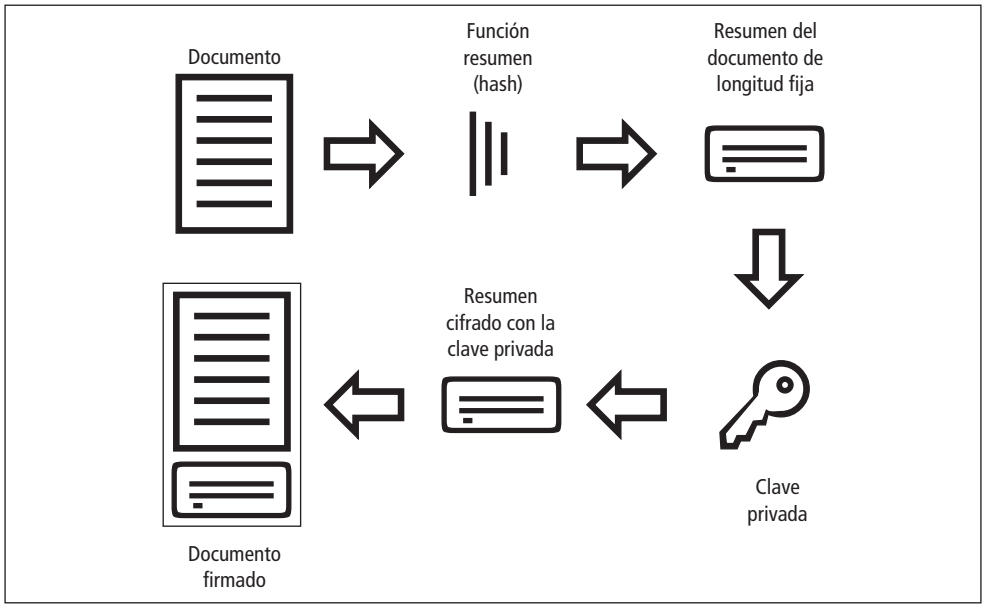
soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado". Por su parte, la LAE, en su Título II, Capítulo IV, define los documentos administrativos electrónicos como los documentos administrativos definidos por la LRJPAC cuando se crean en formato electrónico. Antes el legislador ya había creado otros tipos de documentos electrónicos, como el documento público electrónico, introducido por la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, que modifica la Ley de 28 de mayo de 1862, del Notariado, o el documento único electrónico (DUE), caso particular de documento electrónico introducido por la Ley 7/2003, de 1 abril, de la Sociedad Limitada de la Nueva Empresa. Sobre el documento público electrónico puede verse J. Micó, *La firma electrónica de notarios y registradores y el documento público electrónico*, Tirant lo Blanch, Valencia, 2007.

13. Por ello la criptografía moderna se denomina también de "claves asimétricas" o "criptografía de clave pública". Su origen teórico es el célebre artículo: W. Diffie, M. E. Hellman, *New Directions in Cryptography*, IEEE Trans. Inform. Theory, IT-22, 6, 1976, p. 644-654. En 1978, R, Rivest, A. Shamir y L. Adleman desarrollaron los algoritmos RSA, en los que se basa la utilización práctica de este método criptográfico.

Serie Claves del Gobierno Local, 12 Fundación Democracia y Gobierno Local
ISBN: 978-84-614-0970-9

Pero, ¿cuál es el elemento que el firmante cifra con su clave privada para crear una firma electrónica? Se trata de un "resumen" del documento que se crea utilizando unas funciones denominadas *hash*, las cuales permiten obtener de un conjunto de datos de cualquier longitud –el documento– un número de longitud fija, que es un resumen único del documento. Este resumen, o *hash*, tiene la propiedad de que su valor varía ante la más mínima modificación del conjunto de datos inicial, propiedad que permite utilizarlo para garantizar la integridad del documento. Existe, por tanto, una relación totalmente unívoca entre cada documento y su resumen. En consecuencia, la firma electrónica se define como el resumen de un documento cifrado con la clave privada del firmante.

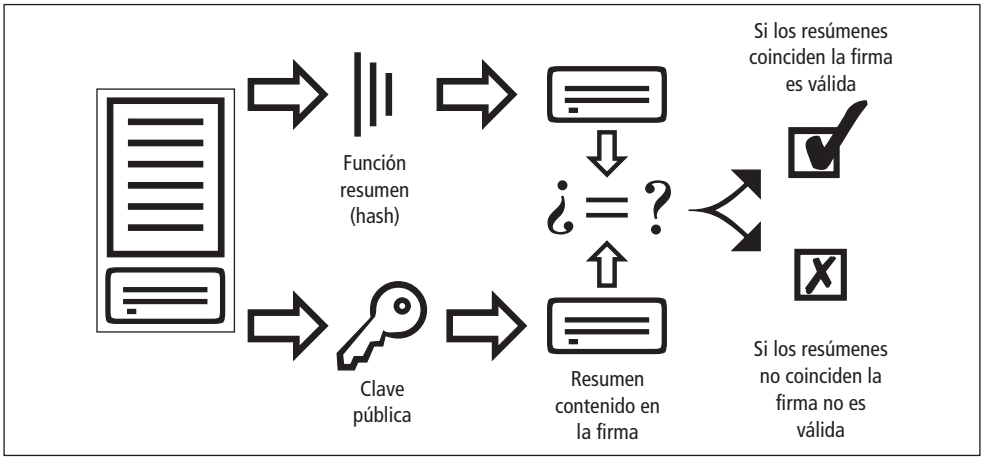
Figura 1. Firma de un documento



Para comprobar la validez de la firma se realizan dos operaciones. Por una parte se calcula de nuevo el resumen del documento con la misma función que se empleó al firmarlo, por otra se descifra la firma utilizando la clave pública del firmante, de forma que extraemos el resumen contenido en la firma. Ésta será correcta si el valor de ambos resúmenes coincide, ya que así sabremos con seguridad que el resumen de la firma fue cifrado con la clave privada del firmante (autenticidad de origen), así como que el documento no ha sido modificado (garantía de integridad).

Serie Claves del Gobierno Local, 12
ISBN: 978-84-614-0970-9
Fundación Democracia y Gobierno Local

Figura 2. Comprobación de la firma



Para terminar esta introducción a la firma electrónica es preciso introducir un nuevo concepto. Tanto la LFE como la Directiva distinguen dos clases de firma: la no avanzada y la firma electrónica avanzada, que es la que hemos explicado hasta ahora. La primera, la no avanzada, se define como "el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge" y se corresponde con las contraseñas y mecanismos equivalentes. Por ejemplo, en una banca electrónica la primera clave que se nos pide es una clave de identificación, pero luego cuando realizamos una operación, como puede ser ordenar una transferencia, se nos solicita una segunda clave y ésta es una firma electrónica no avanzada. En la práctica suelen utilizarse claves de ocho posiciones de las que se solicitan cuatro cada vez o tarjetas de coordenadas.

La práctica totalidad de los sistemas de banca y comercio electrónico existentes en la actualidad se basan en la firma no avanzada, y la experiencia ha demostrado que ofrece un nivel de seguridad suficiente para estas aplicaciones. Las grandes ventajas que presenta son su bajo coste y su facilidad de implementación y uso. Sin embargo tiene dos inconvenientes muy graves: el primero es que los datos de creación de la firma nos los da la otra parte (por ejemplo, el banco) y, por tanto, es inevitable que los conozca; el segundo es que la firma no está vinculada de forma indisociable con los datos firmados, sino que sólo existe lo que la LFE denomina "una asociación funcional". Esto quiere decir que son los programas los que se encargan de vincular el momento en el que introducimos la clave de firma con la operación que estamos autorizando, y que no queda constancia permanente de qué fue lo que firmamos. Por tanto, la firma electrónica no avanzada sólo puede utilizarse en contextos donde

Serie Claves del Gobierno Local, 12 Fundación Democracia y Gobierno Local
ISBN: 978-84-614-0970-9

la confianza en la otra parte sea muy elevada. Pero, como hemos visto, la firma electrónica avanzada supera estas dos limitaciones, ya que se genera con medios que están bajo el exclusivo control del firmante y es única para cada documento, existiendo entre firma y documento una relación totalmente unívoca.

4. Los certificados electrónicos

La clave pública es el mecanismo de comprobación de las firmas electrónicas, pero ¿cómo podemos saber con seguridad que una clave pública pertenece a una persona dada?. En grupos pequeños puede ser suficiente con que las personas intercambien sus claves públicas de forma presencial pero, cuando el ámbito es mayor, se hace preciso el concurso de unas nuevas entidades a las que denominamos "servicios de certificación".[14] Estos servicios emiten certificados electrónicos, que no son sino unos documentos electrónicos firmados por la entidad de certificación, en los que se vincula a una persona con una clave pública. De esta forma podemos distribuir con seguridad las claves públicas, ya que las recibimos en un pequeño documento en el que se acredita quién es su titular.[15]

Antes de emitir un certificado hay que realizar alguna comprobación sobre la identidad del poseedor de la clave, y éste debe manifestar de forma fehaciente que tiene la clave privada y su compromiso con las firmas que sean generadas en el futuro mediante la misma, a fin de que quede vinculado por éstas. La seguridad con que se realiza dicho trámite, que se denomina de inscripción o registro, es uno de los factores principales a la hora de distinguir el nivel de confianza de los certificados. El mínimo exigido por la LFE para los certificados reconocidos es la firma presencial del compromiso ante un representante del servicio de certificación.[16] Otro requisito importante que deben cumplir los servicios de certificación es mantener un directorio, accesible por Internet, en el que pueda consultarse qué certificados han sido revocados. Antes de dar por válida una firma se verifica en el directorio que el certificado está vigente. Esta medida permite que, en caso de pérdida o compromiso de la clave

14. El término que emplea la LFE es el de Prestadores de Servicios de Certificación. En el ámbito técnico suelen ser conocidas por sus siglas inglesas CA (*Certification Authorities*) o como autoridades de certificación.

15. Para comprobar la autenticidad de un certificado necesitamos conocer la clave pública del servicio de certificación que lo ha emitido. Estas claves se incorporan en los certificados que denominamos "autofirmados" o "certificados raíz". Los fabricantes de sistemas operativos, como Microsoft, incluyen en el sistema los certificados raíz de los servicios de certificación más importantes, lo que permite la comprobación de la validez de los certificados emitidos por los mismos de forma "transparente para el usuario".

16. LFE, artículo 13. El concepto de certificado reconocido se ve más adelante, en la p. 179.

Serie Claves del Gobierno Local, 12
ISBN: 978-84-614-0970-9
Fundación Democracia y Gobierno Local

privada, los titulares de los certificados puedan invalidarlos y, con ello, las firmas posteriores al momento de la revocación.[17]

Una cuestión que añade bastante complejidad al uso de la firma electrónica es que estas firmas, según el certificado por el que están respaldadas, tienen un valor muy diferente. Así, por ejemplo, hay servicios de certificación que emiten certificados de prueba, sin ningún valor legal, de forma que las firmas electrónicas basadas en los mismos carecen de cualquier carácter vinculante. En el otro extremo, las firmas respaldadas por un Certificado Notarial Personal[18] tienen pleno valor legal, sin limitación respecto a la naturaleza o cuantía del negocio jurídico en el que se utilicen.

Por ello, desde la óptica jurídica, un elemento básico de los servicios de certificación son los documentos en los que se establece, entre otras cuestiones, el valor que podemos otorgar a una firma respaldada por una determinada clase de certificados. El primero de estos documentos es único para cada servicio de certificación y se denomina "declaración de prácticas de certificación".[19] Este documento es obligatorio, y en él se establece el modo en el que el servicio gestiona las claves y certificados, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados, las medidas de seguridad técnicas y organizativas, y los mecanismos de información sobre la vigencia de los certificados. Pero, para poder valorar las firmas, lo más importante es que enumera las distintas clases de certificados que emite el servicio de certificación con sus características básicas, el procedimiento para la emisión de los certificados de esa clase, su contenido, los usos posibles, y el alcance y limitaciones de las firmas respaldadas por los mismos.[20]

Aunque la LFE no obliga a ello, es práctica frecuente disponer también de unos documentos breves, denominados Políticas de Certificación, que establecen estos últimos extremos para cada clase de certificados. Tanto la declaración de prácticas de certificación como las políticas deben estar disponibles al público de manera fácilmente accesible, al menos por vía electrónica, y de forma gratuita. También, de

17. El primer estándar definido para la publicación de revocaciones se basa en listas que contienen todos los certificados revocados, son las denominadas CRL (*Certificate Revocation List*). Conforme la emisión de certificados aumenta, también lo hace el número de revocaciones y, en consecuencia, el tamaño de las CRL. Por ello se está generalizando el uso de un nuevo estándar que permite consultar directamente el estado de un certificado concreto y que se llama OCSP (*On-line Certificate Status Protocol*).

18. Son certificados emitidos por la Autoridad Notarial de Certificación (ANCERT), en los que el acto de registro se realiza ante un notario.

19. La denominación de este documento, bastante ajena a nuestra tradición jurídica, es traducción directa del término inglés *Certification Practice Statement* (CPS), al igual que la expresión Políticas de Certificación, que proviene de *Certificate Policy* (CP).

20. LFE, artículo 19.

Serie Claves del Gobierno Local, 12 Fundación Democracia y Gobierno Local
ISBN: 978-84-614-0970-9

acuerdo con los estándares técnicos,[21] los certificados indican en uno de sus campos la dirección de Internet donde pueden verse estos documentos.

Tanto la LFE como la Directiva establecen el principio de libre creación de servicios de certificación, de forma que cualquier entidad pública o privada puede constituirse como organismo emisor de certificados, sin que sea necesaria ninguna autorización previa.[22] Pero en la práctica son pocas las entidades que han constituido servicios de certificación. En nuestro país las principales son la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM), la Autoridad Notarial de Certificación (ANCERT), el Servicio de Certificación de los Registradores (SCR) y Camerfirma, constituido por las Cámaras de Comercio, además de alguna empresa.

La LFE también crea un mecanismo que permite alcanzar un nivel reforzado de seguridad en los servicios prestados: los certificados reconocidos. Los servicios de certificación que expidan estos certificados, así como los propios certificados, deben cumplir un conjunto de requisitos establecidos por la LFE.[23] Por imperativo legal, la firma electrónica avanzada basada en un certificado reconocido tiene un valor equivalente al de la firma manuscrita.[24]

Pero, pese a esta afirmación de la Ley, es preciso tener en cuenta que, dada su distinta naturaleza, la firma electrónica no es directamente asimilable a la manual, ya que esta última es una acción consciente con un resultado que es característico de cada individuo. Si decíamos antes que en materia de medidas de seguridad se distinguen tres niveles –algo que se sabe, algo que se tiene y algo que se es–, podríamos afirmar que la firma manuscrita corresponde a un cuarto nivel: algo que se hace. Además, otra diferencia muy importante entre ambas es que la firma manual y las reglas para su utilización están profundamente arraigadas en nuestra cultura. Por el contrario, la firma electrónica se genera mediante un dispositivo, y sólo la correcta conservación y utilización del mismo garantiza que tengamos el control de todas las firmas de las que somos titulares. Y la cultura para la gestión de los mecanismos de creación de firma y, en general, para el uso de la firma electrónica, está aún por desarrollarse.

---

21. Los principales estándares técnicos sobre firma electrónica son el X-509 v.3, definido por la Unión Internacional de Telecomunicaciones (UIT), que establece el formato de los certificados, los RFC 2459 y 3739 y algunas normas del ETSI (*European Telecommunications Standards Institute*) y del CWA (*Comité Europeo de Normalización*). Los *Request for Comments* (RFC) son los estándares de Internet y se denominan así porque, una vez aprobados inicialmente por el IETF (*Internet Engineering Task Force*), se someten a los comentarios de la comunidad científica, hasta que finalmente son aprobados.
22. LFE, artículo 5.
23. LFE, artículos 11 a 14.
24. LFE, artículo 3.4.

Serie Claves del Gobierno Local, 12
ISBN: 978-84-614-0970-9
Fundación Democracia y Gobierno Local

Finalmente, destacamos de nuevo la necesidad de distinguir el uso de las claves privadas y de los certificados para la identificación de personas y para la firma de documentos (autenticación). En el primer caso, únicamente utilizamos la clave privada para resolver lo que en criptografía se denomina un reto, que permite a quien lo plantea comprobar que poseemos la clave privada sin que le demos ninguna información sobre la misma. Podríamos decir que esta forma de operar equivale a que nos entreguen una tarjeta en blanco para firmar en ella, y viendo nuestra firma poder comprobar nuestra identidad. Una vez realizada esta operación la tarjeta se desecha. Por el contrario, cuando generamos una firma electrónica para autenticar un documento, nuestra intención es que la firma se incorpore a éste como garantía del origen e integridad del mismo. En este caso, la firma que generamos tiene ánimo de permanencia y de servir como prueba del compromiso del firmante con el contenido del documento.[25] Prueba de esta diferencia es que, por motivos de seguridad, se considera conveniente utilizar distintas claves para la identificación y la autenticación. Así se hace, por ejemplo, en el DNI electrónico, que contiene dos claves privadas con sus correspondientes certificados, una para identificación y otra para firma (autenticación).[26]

5. La firma electrónica y la Administración electrónica

La prestación de servicios de certificación para firma electrónica comenzó en España en el año 1997.[27] La experiencia de los años transcurridos desde entonces ha demostrado que la adopción de la firma electrónica avanzada resulta mucho más lenta y difícil de lo esperado. De hecho, vemos que el comercio electrónico, incluida la banca, ha alcanzado un alto nivel de penetración basándose en la firma electrónica no avanzada, mientras que la Administración electrónica pone, al exigir la utilización de firma electrónica avanzada, una barrera que la mayoría de ciudadanos no supera.

Al comenzar los primeros desarrollos de Administración electrónica, se consideró que la firma electrónica no avanzada no era garantía suficiente para la realización

25. También se insiste en la importancia de esta distinción en E. Gamero, J. Valero (eds.), *op. cit.*, p. 322 y ss.

26. Así lo establece el RD 1553/2005, de 23 de diciembre, por el que se regula la expedición del DNI y sus certificados de firma electrónica. El artículo 11.4 dice que el DNI contendrá "Certificados reconocidos de autenticación y de firma, y certificado electrónico de la autoridad emisora,...". Como puede verse, la norma utiliza el término autenticación en sentido distinto al de la LAE (por identificación), y se refiere a lo que la LAE denomina autenticación como firma. Este uso de la terminología es el habitual en el ámbito técnico y es previsible que dé lugar a confusión hasta que se consolide la terminología introducida por la LAE.

27. Los pioneros fueron la FNMT, con el proyecto CERES, y la Fundación para el Estudio de la Seguridad de las Telecomunicaciones (FESTE), formada, entre otros, por los Consejos Generales del Notariado y de la Abogacía, y la Universidad de Zaragoza.

Serie Claves del Gobierno Local, 12 Fundación Democracia y Gobierno Local
ISBN: 978-84-614-0970-9

de trámites administrativos, ya que no quedaba una prueba fehaciente que acreditara su momento y contenido. Pero, como la lentitud en la introducción de la firma electrónica avanzada se ha convertido en un freno para la evolución del gobierno electrónico, algunos estudios sobre esta materia consideran que el exigir el uso de la firma electrónica avanzada fue un requisito demasiado exigente, y que debe replantearse si es necesario utilizarla en todas las operatorias de Administración electrónica.

Como ejemplo de lo anterior puede servir la operatoria paradigmática de la Administración electrónica en nuestro país: la presentación del Impuesto de la Renta de las Personas Físicas (IRPF) a través de Internet. En las primeras campañas del IRPF en las que se incorporó esta posibilidad, el procedimiento exigía que el contribuyente obtuviera un certificado de la FNMT con el que podía presentar su declaración, y el número de declaraciones entregadas por Internet era muy pequeño, del orden de 20.000. Ante la baja utilización de este canal, la Agencia Tributaria (AEAT) creó una figura, que denominó "colaboración social", en base a la cual se emiten unos certificados específicos para despachos profesionales, como gestorías y abogados, y para los bancos. Estos certificados permiten presentar la declaración de cualquier contribuyente. A partir de este momento, el número de declaraciones presentadas por Internet aumentó hasta llegar a ser de varios millones, pero el sistema ha sacrificado buena parte de su seguridad, ya que la Agencia no tiene ninguna constancia de que el contribuyente ha autorizado al presentante a que presente su declaración.

Hoy, la LAE establece un marco flexible para garantizar la identidad de las personas y la autenticidad de los documentos. A nuestro juicio, la forma en la que la Ley regula esta cuestión refleja su clara visión práctica, derivada de la experiencia anterior en el desarrollo de sistemas de Administración electrónica y de las dificultades observadas. Como acabamos de ver, entre estas dificultades, una de las más destacadas ha sido la exigencia a los sistemas informáticos de niveles de seguridad muy superiores a los existentes previamente, y que no resultan necesarios en muchos de los casos. Frente a esta tendencia, la LAE hace suyo un principio básico de la seguridad informática: el de proporcionalidad, y dispone que "sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones", estableciendo también un límite inferior, ya que se exigirá, como mínimo, un nivel de seguridad equivalente al de las operatorias no electrónicas.[28]

La evolución de la operatoria para la presentación de la declaración del IRPF puede seguir sirviéndonos como ejemplo de la conveniencia de esta actitud abierta de la

28. LAE, artículo 4. f) y g).

Serie Claves del Gobierno Local, 12
ISBN: 978-84-614-0970-9
Fundación Democracia y Gobierno Local

LAE. En las últimas campañas, se da a los contribuyentes que han recibido el borrador de la declaración la posibilidad de presentar su declaración simplemente aceptando el borrador con el envío de un mensaje (SMS) mediante el teléfono móvil, con un código alfanumérico que se incluye en el borrador. Recibido éste, la AEAT envía otro SMS con un código de verificación que sirve al contribuyente como acuse de recibo. Se trata, en nuestra opinión, de una operatoria ejemplar por su sencillez y por la comodidad que supone para el presentante. Es preciso, por tanto, permitir la utilización de medios de garantía de la identidad y autenticidad que no impidan ni obstaculicen el desarrollo de operatorias como la mencionada.

6. Los medios de identificación y autenticación de los administrados

La LAE comienza por los ciudadanos, al establecer los medios de identificación y autenticación que podrán utilizarse en la Administración electrónica,[29] siendo los certificados contenidos en el DNI electrónico el mecanismo que deberá ser universalmente aceptado por las Administraciones Públicas. Sin embargo, hay dos razones que impiden la existencia de un único medio de identificación.

La primera tiene que ver con el principio de libre prestación de los servicios de la sociedad de la información, que inspira toda la normativa europea sobre la materia, y que introduce en nuestro ordenamiento la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).[30] En materia de firma electrónica, este principio se traduce en el principio de libre creación de prestadores de servicios de certificación, que mencionamos anteriormente. Pero no tendría sentido permitir la existencia de múltiples servicios de certificación si luego sus certificados no van a ser aceptados en un sector tan importante como son las Administraciones Públicas. Por ello, cada Administración deberá establecer una "política de firma" en la que detalle los certificados que acepta en sus operatorias de Administración electrónica, haciéndola pública por medios electrónicos.[31]

Hay un segundo motivo, de tipo práctico, que impide que el único medio de identificación y autenticación sea el DNI electrónico, y es que los titulares del mismo

29. LAE, artículo 13.2 y artículos 14 a 16.
30. LSSI, artículo 7.
31. LAE, artículo 15.2. Aunque la Ley no lo especifica, ha de suponerse que esta publicación debe hacerse en la sede electrónica de la entidad. Algunas observaciones sobre la vigencia práctica de este principio pueden verse en Valero, J., *El régimen jurídico de la e-Administración. El uso de medios informáticos y telemáticos en el procedimiento administrativo común*, Comares, Granada, 2.ª edición, 2007, p. 60-62.

Serie Claves del Gobierno Local, 12 Fundación Democracia y Gobierno Local
ISBN: 978-84-614-0970-9

son únicamente las personas físicas y, sin embargo, las Administraciones necesitan en muchos casos relacionarse con personas jurídicas. Es ésta una cuestión, la firma de las personas jurídicas, que ha tardado en aclararse dentro del ámbito de la firma electrónica. La confusión comenzó con la primera norma española sobre firma electrónica, el derogado Real Decreto-Ley 14/1999, que en su artículo 2, establecía que los signatarios únicamente podían ser personas físicas, pese a que la experiencia de la única Administración que en aquellos momentos había desarrollado operatorias de Administración electrónica, la AEAT, ya le había llevado a utilizar certificados de persona jurídica. Por ello, el Real Decreto tuvo que añadir una excepción, en virtud de la cual el Ministro de Economía y Hacienda podría determinar "respecto de la gestión de los tributos, la posibilidad de que el signatario sea una persona física o una persona jurídica". Finalmente, la LFE introdujo los certificados de persona jurídica para su uso en cualquier ámbito.[32]

Previsiblemente, la modalidad de certificado más utilizado para la actuación de las personas jurídicas será el de "cargo o representación". Éstos son certificados cuyo titular es una persona física, pero que pertenecen a un tipo de certificados denominados "de atributos", que son aquéllos en los que, además de la identidad del titular, se hace constar alguna información sobre el mismo como, por ejemplo, su condición de profesional en ejercicio o, en el caso que nos ocupa, el hecho de que ocupa un cargo en una organización o de que es representante de la misma.[33]

Es así porque de muchas de las actuaciones de las personas jurídicas, tanto públicas como privadas, pueden derivarse responsabilidades de las personas físicas que actúan con agentes de las mismas y, por tanto, en estos actos la firma electrónica deberá aportarnos una doble información: la de la persona física que suscribe el documento y la de su carácter de representante de una determinada organización. En este sentido, otra posibilidad que cabe plantearse es utilizar en las Administraciones Públicas una doble firma: la de la persona que suscribe el documento y un sello de la entidad que, como veremos, es la firma de la persona jurídica. A falta de certificados de atributos se trataría de una solución aceptable.

De hecho, según la Exposición de Motivos de la LFE, la única incorporación de una firma de persona jurídica, sin que quede constancia de la persona física que

32. LFE, artículo 7.

33. La definición que se da de los certificados de atributos es la comúnmente utilizada, sobre todo en el ámbito jurídico. Sin embargo, desde el punto de vista técnico, el concepto se refiere a certificados vinculados a un certificado principal, que es el que contiene la clave pública, y que permitirían crear alrededor del mismo una estructura variable de atributos. Estos certificados serían emitidos por "autoridades de atributos" como, por ejemplo, un colegio profesional, que acreditaría la condición de profesional en ejercicio.

Serie Claves del Gobierno Local, 12
ISBN: 978-84-614-0970-9
Fundación Democracia y Gobierno Local

incorporó la firma al documento, puede dar lugar "a la aparición de obligaciones incontrolables frente a terceros".[34] En la práctica, puede ser útil recurrir al criterio de que la firma de la persona jurídica equivale al tradicional sello en tinta y que, por tanto, podrá utilizarse en los mismos casos que éste. Desde la óptica de las nuevas formas de proceder asociadas a los sistemas de información, la firma de las personas jurídicas estaría asociada a los procesos automatizados, que conllevan la emisión de determinados documentos de forma masiva, sin la intervención directa ni la supervisión individualizada del contenido por una persona física. Son ejemplos de lo anterior la emisión de las facturas electrónicas, en el caso de las empresas, o de los acuses de recibo en los registros de entrada, en el caso de las Administraciones Públicas.[35]

Pese a existir estas diversas opciones, la LAE no menciona la firma de las personas jurídicas cuando regula la identificación y autenticación de los ciudadanos.[36] Tenemos que ir al Anexo para saber que, según la LAE, ciudadanos son "cualesquiera personas físicas, personas jurídicas y entes sin personalidad que se relacionen, o sean susceptibles de relacionarse, con las Administraciones Públicas". Por tanto, hemos de entender que toda la regulación de este apartado se extiende a las personas jurídicas, y que serán las Administraciones las que en su "política de firma" establecerán cuándo admiten certificados de persona jurídica y cuándo de cargo o representación.[37] Isaac Martín va más allá y considera que esta asimilación entre los certificados de persona física y jurídica significa que los segundos han de ser aceptados por las Administraciones de forma tan general como los primeros, por lo que su uso deja de ser excepcional y se genera un derecho de las personas jurídicas a obtener sistemas de firma y hacer uso de los mismos.

Por otra parte, también admite la LAE la utilización de sistemas de firma electrónica no avanzada tales "como claves concertadas en un registro previo, aportación de información conocida por ambas partes u otros sistemas no criptográficos". Esta utilización deberá hacerse de forma justificada y, seguramente pensando en supuestos como el anteriormente mencionado de presentación de la declaración del IRPF a través del envío de un SMS, añade la Ley que "en aquellos supuestos en los que se utilicen estos sistemas para confirmar información, propuestas o borradores remitidos

34. Sobre esta cuestión puede verse A. Martinez, *Comentarios a la Ley 58/2003 de firma electrónica*, Thompson-Civitas, Madrid, 2004, p. 124 y ss.

35. Esta interpretación estaría respaldada por la inclusión, por parte de la LAE, de los sellos electrónicos entre los sistemas de firma electrónica para la actuación administrativa automatizada, como veremos más adelante.

36. La LAE sí que menciona expresamente la admisibilidad de los certificados emitidos para entidades sin personalidad jurídica (artículo 15.3). Este tipo de certificados se admitía desde hace tiempo por la Administración tributaria, por ejemplo, para el caso de las herencias yacentes.

37. E. Gamero, J. Valero (eds.), *op. cit.*, p. 345.

Serie Claves del Gobierno Local, 12 Fundación Democracia y Gobierno Local
ISBN: 978-84-614-0970-9

o exhibidos por una Administración Pública, ésta deberá garantizar la integridad y el no repudio por ambas partes de los documentos electrónicos concernidos."[38]

Finalmente, la LAE contempla el supuesto de aquellos ciudadanos que carecen de los medios electrónicos de identificación necesarios para una determinada operación.[39] En estos casos habrá funcionarios, expresamente habilitados para ello, que podrán sustituir con sus propios medios de identificación y autenticación al ciudadano. Para ello, este último deberá identificarse y dar su consentimiento expreso, del que deberá quedar constancia. Se trata de una disposición de claro sentido práctico, útil para evitar que quienes no disponen de medios de identificación electrónicos se vean imposibilitados para acceder a algunos servicios, pero, sobre todo, para evitar que la carencia, por parte de los ciudadanos, de medios de identificación y autenticación electrónicos haga inútiles los esfuerzos de las Administraciones para la puesta en marcha de las operatorias de Administración electrónica.[40]

7. La identificación y autenticación de las Administraciones Públicas

Los medios de identificación y autenticación que utiliza la propia Administración son, de acuerdo con lo visto anteriormente, certificados de persona jurídica. La LAE menciona en primer lugar el dispositivo utilizado para la identificación de las sedes electrónicas, concepto este último con el que la LAE da carta de naturaleza a los sitios web de las Administraciones Públicas, y que es una de las novedades más importantes introducidas por la Ley.

Uno de los requisitos que exige la LAE es que las sedes electrónicas dispongan de sistemas que permitan el establecimiento de comunicaciones seguras.[41] Desde el punto de vista técnico se utilizan para ello los "certificados de servidor", que tienen una doble función: por una parte acreditan que un servidor pertenece a una organización o persona y, por otra, garantizan la confidencialidad de la información que se intercambia entre el servidor y el ordenador del usuario (cliente).[42] Su activación se

38. LAE, artículo 16.

39. Dado el carácter voluntario del uso de los medios electrónicos, cabe suponer que el precepto también se aplicará a quien, disponiendo de los medios de identificación, no desee utilizarlos.

40. E. Gamero, J. Valero (eds.), *op. cit.*, p. 361 y 362.

41. LAE, artículo 10.4.

42. Los certificados de servidor utilizan el protocolo SSL (*Secure Socket Layer*), que permite identificar de forma segura al sitio web y activa el cifrado de confidencialidad entre servidor y cliente durante toda la sesión. Para ello, cuando el cliente inicia una conexión con el servidor éste

Serie Claves del Gobierno Local, 12
ISBN: 978-84-614-0970-9
Fundación Democracia y Gobierno Local

indica al usuario mediante la aparición de la imagen de un candado cerrado en el navegador web.

La definición que da la LAE de la sede electrónica es muy amplia, ya que "es aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública,...". Una vez promulgada la norma, muchas Administraciones Públicas han emprendido la tarea de delimitar, dentro de su sitio web, qué zonas son sede electrónica y qué zonas no. Esta delimitación está sobre todo condicionada por la responsabilidad que la misma Ley establece sobre los contenidos de la sede, la cual hace que las entidades no quieran asumir ese nivel de compromiso sobre la totalidad de los contenidos actuales de su sitio web.[43]

Para realizar esta delimitación, ateniéndonos estrictamente a la definición legal, sería preciso que únicamente los contenidos de la sede estén bajo la dirección de la entidad, teniendo que crearse para los demás contenidos otras direcciones. Pero lo que cualquier entidad, privada o pública, pretende en el mundo de Internet es posicionar lo mejor posible su dirección (dominio), para que éste sea conocido por el mayor número posible de ciudadanos, que lo utilizarán para acceder a sus servicios. Por ello, multiplicar los dominios sería una estrategia perjudicial.

En este sentido, el certificado de servidor puede servir como medio de delimitación de la zona del sitio web que tiene el carácter de sede electrónica, de modo similar a como suele ocurrir en los sitios web de los bancos electrónicos, en los cuales hay una zona con información comercial que no está dentro del servidor seguro, y otra zona, donde los clientes realizan sus operaciones, que sí que está dentro del servidor seguro.[44]

Una segunda clase de medios de identificación y autenticación que, según la LAE, pueden utilizar las Administraciones Públicas, son los que denomina "sistemas de

---

le envía su certificado con la clave pública. A continuación el cliente envía al servidor una clave de sesión para cifrado simétrico cifrada con la clave pública del servidor. Este último al descifrar la clave de sesión demuestra que posee la clave privada correspondiente al certificado y prueba, por tanto, su identidad. A partir de ese momento la clave de sesión se utiliza para cifrar todos los datos que se intercambien entre ambos ordenadores, con lo que se consigue también la confidencialidad de la comunicación.

43. Por ejemplo, hay Administraciones Públicas que permiten que los contenidos de determinadas zonas de su sitio web sean administrados por colectivos que colaboran con las mismas en cuestiones determinadas, pero que orgánicamente son ajenos a la entidad.

44. Con ello no quiere decirse que la sede electrónica deba hacerse coincidir con la zona del sitio web que suele denominarse "oficina virtual", y que es donde se ubica la realización de trámites. En nuestra opinión el concepto de sede electrónica es mucho más amplio.

Serie Claves del Gobierno Local, 12 Fundación Democracia y Gobierno Local
ISBN: 978-84-614-0970-9

firma electrónica para la actuación administrativa automatizada". Antes de entrar a estudiarlos, cabe hacer una precisión de tipo técnico, y es que los certificados de servidor que acabamos de ver son únicamente un medio de identificación, ya que su función es garantizar la identidad de un sitio web, y, por el contrario, los sistemas de firma electrónica para la actuación administrativa automatizada son únicamente medios de autenticación de documentos, ya que no se emplean para identificar al órgano administrativo, sino para que éste pueda autenticar documentos que genera de forma automatizada, como puede ser el ejemplo antes mencionado de los acuses de recibo de un registro electrónico, o los certificados emitidos en base a información obrante en las bases de datos de la Administración correspondiente, como es el caso del certificado de vida laboral, que emite la Tesorería General de la Seguridad Social (TGSS).

Entre los sistemas de firma electrónica para la actuación administrativa automatizada la LAE incluye dos mecanismos: uno basado en la firma electrónica avanzada, que son los sellos electrónicos, y otro basado en firma electrónica no avanzada, los códigos de verificación.

Respecto a los primeros, dice la Ley que cada Administración publicará en su sede la relación de los sellos electrónicos que utilice, con sus características y los prestadores de servicios de certificación que los emiten. Una cuestión a resolver es si los sellos electrónicos, como certificados de persona jurídica que son, deben contener necesariamente los datos de la persona física que los ha solicitado, tal y como establece la LFE en su artículo 7.2. Pero, según el párrafo 6 del mismo artículo, los certificados electrónicos de persona jurídica emitidos para Administraciones Públicas están sujetos a su normativa específica, por lo que debemos atender a lo dispuesto por la LAE. Y ésta, en su artículo 18.2, dispone que los sellos electrónicos deben contener necesariamente el número de identificación fiscal y la denominación del órgano para el que se emiten, siendo potestativo incluir el nombre del titular del órgano.

Estamos ante una nueva manifestación del carácter pragmático de la LAE. En efecto, si incluimos en el certificado el nombre de una persona física en virtud del cargo que ostenta, cuando esta persona abandone el cargo deberíamos revocar el certificado, lo que no tiene mucho sentido, ya que es un certificado de persona jurídica. Otra opción sería una interpretación, según la cual la persona que suceda en el cargo a aquélla que consta en el certificado, se subrogaría automáticamente en las obligaciones de custodia y buen uso del mecanismo de creación de firma asociado al certificado. Pero, en la primera aproximación práctica a esta cuestión, que es la Política de Certificación de la FNMT referente a sus "certificados para la actuación administrativa automatizada", se establece que éstos serán revocados cuando la persona física, a la que denomina "firmante/custodio" del certificado, deje de corres-

Serie Claves del Gobierno Local, 12
ISBN: 978-84-614-0970-9
Fundación Democracia y Gobierno Local

ponderse con el titular del órgano administrativo para el que se ha emitido el certificado.[45]

Por ello, la LAE permite la posibilidad, más sencilla, de emitir certificados que únicamente mencionen al órgano administrativo. En caso de que sea necesario delimitar las responsabilidades, por fallos en la custodia o la incorrecta utilización de las claves, se recurriría a las normas administrativas de carácter general que establezcan las responsabilidades y obligaciones de los componentes del organismo y del titular del mismo.

En cuanto al segundo mecanismo, los códigos de verificación son cadenas alfanuméricas que se incluyen en los documentos, electrónicos o en soporte papel. Estos códigos nos permiten generar "copias verificables", es decir, documentos que tienen plena identidad visual con un documento electrónico auténtico, circunstancia que podemos comprobar accediendo a este documento, que la Administración que lo emitió conserva en su archivo, introduciendo el correspondiente código de verificación en una operatoria, que debe estar disponible en la sede electrónica de la entidad, y a la que denominamos "punto de verificación".[46]

Teniendo en cuenta las dificultades que supone para los usuarios el disponer de los medios informáticos necesarios para validar las firmas electrónicas de los documentos recibidos de las Administraciones Públicas, los códigos seguros de verificación presentan la ventaja de no exigirles ningún requisito ni esfuerzo adicional. Además, cuando el objetivo es generar copias en papel que puedan ser aportadas en cualquier lugar y procedimiento, son, hoy por hoy, el único mecanismo utilizable. En general, la utilización de "copias verificables", cuya funcionalidad es la misma tanto en formato electrónico como en soporte papel, simplifica una cuestión clave desde un punto de vista práctico, que es el paso del soporte papel al formato electrónico y viceversa. Y, por otra parte, el mecanismo de cotejo en la sede las convierte en un medio robusto de autenticación de documentos, sin que pierdan nada de su sencillez.

45. La política de certificación de la AC AP puede verse en www.cert.fnmt.es.

46. Un ejemplo puede verse en la sede electrónica de la AEAT: https://www5.aeat.es/es13/S/E2CAE2CAVI0S?ORIGEN=C (14/3/2010). La AEAT denomina a la opción: "cotejo de documentos".

Serie Claves del Gobierno Local, 12 Fundación Democracia y Gobierno Local
ISBN: 978-84-614-0970-9

Figura 3. Ejemplo de código seguro de verificación

8. La identificación y autenticación de los empleados de las Administraciones Públicas

La LAE establece, en primer lugar, que el modo común de actuación de las Administraciones Públicas será a través de la firma electrónica de sus empleados, de forma que los medios vistos en el apartado anterior se utilizarán únicamente en los supuestos específicos para los que se han previsto. Como dijimos anteriormente, es una opción lógica, ya que la mayor parte de las decisiones de las organizaciones han de venir respaldadas por una persona física que, en virtud de su función o cargo, pueda responder de las mismas.

Una vez establecido lo anterior, la Ley deja abiertas dos posibilidades: el uso por parte de los empleados de su DNI electrónico, o la utilización de certificados específicamente emitidos para el ejercicio de las funciones desarrolladas como empleados públicos, y que serán proporcionados por la Administración a la que éstos pertenezcan. Se trata en este caso de certificados de empleado, que son certificados de persona física, pero que también identifican a la organización y pueden contener el puesto o cargo que el titular ocupa dentro de la misma. Son un supuesto típico de los certificados de atributos, a los que nos referimos anteriormente. La Ley no se pronuncia expresamente, pero parece preferir esta segunda opción, aunque sólo sea por el orden en que las menciona.

Hay varias razones para preferir la utilización de certificados específicos, frente a la del DNI electrónico. Desde el punto de vista de los empleados públicos, se manifiesta con frecuencia la reticencia a tener que utilizar en el ejercicio de sus funciones administrativas los mismos mecanismos de creación de firma que en sus actividades privadas. Aunque suele objetarse que es lo mismo que ocurre actualmente con la firma manual, lo cierto es que, dada la gran diferencia entre la naturaleza de ambas clases de firma, la percepción de las personas sobre las mismas es muy distinta y la firma electrónica se ve, con acierto, como un mecanismo técnico que debería proporcionar la organización cuando va a utilizarse exclusivamente en funciones relacionadas con la misma.

Serie Claves del Gobierno Local, 12
ISBN: 978-84-614-0970-9
Fundación Democracia y Gobierno Local

Por otra parte, desde el punto de vista de la Administración, los certificados de atributos son un medio muy potente para el control de los permisos dentro de sus sistemas de información. Explicándolo de forma sencilla, existen dos paradigmas técnicos para la gestión de los permisos que un empleado tiene dentro de los sistemas de su organización. El primero y más utilizado actualmente, consiste en identificar al empleado –normalmente mediante su nombre de usuario y su contraseña– y posteriormente consultar una base de datos donde se contienen los permisos que tiene respecto a cada operatoria. El segundo paradigma, es la gestión de los permisos a través de certificados, de forma que al identificarse el empleado mediante un certificado ya no sólo sabemos quién es, sino que también sabemos con certeza cuál es su puesto en la organización, tanto a nivel jerárquico como funcional, y, en virtud de ello, podemos autorizarle a acceder o no a una determinada operatoria del sistema. Esta segunda solución facilita lo que técnicamente se denomina una gestión de permisos "distribuida".[47]

Además, en las grandes organizaciones los certificados de empleado suelen incorporarse a tarjetas que ya vienen utilizándose para la identificación en los accesos físicos a la sede, para el control de horarios, y en algunos casos también para el acceso a los sistemas informáticos, en sustitución del nombre de usuario y la contraseña. En este supuesto, parece natural la evolución en el sentido de sustituir las tarjetas por tarjetas criptográficas, e incorporar en las mismas los certificados de identificación y firma.

Por último, desde el punto de vista del ciudadano, el uso de certificados de empleado público es el que en mayor medida garantiza sus derechos, ya que, cuando recibe un documento firmado por una Administración Pública, tiene información completa y fehaciente sobre el órgano del que proviene el documento, la persona o personas físicas que lo emitieron y el puesto que éstas ocupan en la Administración, en virtud del cual han suscrito el documento recibido.

En cuanto a la disponibilidad de estos certificados, la FNMT, que es el prestador de servicios de certificación para la Administración General del Estado,[48] ha

47. Aunque la gestión de permisos se ve como una cuestión muy técnica, está directamente relacionada con aspectos sociales y políticos de la sociedad de la información, como, por ejemplo, el aprovechamiento de las posibilidades que la Administración electrónica ofrece para potenciar la transparencia de la actuación administrativa, y el acceso a la información de las Administraciones Públicas por parte de los ciudadanos. En efecto, actualmente la mayoría de las aplicaciones de Administración electrónica –como otras muchas– se diseñan para residir en un servidor web y ser utilizadas a través del navegador. Se dice que son aplicaciones "listas para el web" (*web-enabled*). Pues bien, una vez que una aplicación se ha desarrollado de este modo, tan fácil es dar acceso a los funcionarios como a cualquier ciudadano, ya que sólo se trata de establecer una adecuada política de permisos.

48. Según el artículo 81 de la Ley 66/1997, de 30 de diciembre, de acompañamiento a los presupuestos para 1998, desarrollado por el RD 1317/2001, de 30 noviembre. También puede

Serie Claves del Gobierno Local, 12 Fundación Democracia y Gobierno Local
ISBN: 978-84-614-0970-9

creado en 2009 una autoridad de certificación destinada a las Administraciones Públicas. La nueva autoridad de certificación se denomina AC APE y emite tres clases de certificados: de personal al servicio de las Administraciones Públicas, de sede electrónica y para la actuación administrativa automatizada (sello electrónico). En la práctica se echan de menos certificados específicos para los cargos electos, como alcaldes y concejales, que se encuentran entre los primeros usuarios de la firma electrónica,[49] ya que no parece adecuado asimilarlos a los empleados de la Administración, única opción actualmente existente. También emiten certificados para los empleados públicos ANCERT,[50] bajo la denominación de "certificados para corporaciones de Derecho público", y el Servicio de Certificación de los Registradores (SCR), bajo la denominación de "certificado de cargo administrativo".

El último mecanismo de identificación y autenticación que contempla la LAE, demuestra de nuevo su sentido práctico, al establecer que los documentos intercambiados en entornos cerrados de comunicación serán considerados válidos, a efectos de autenticación e identificación de los emisores y receptores. El término que utiliza la Ley –entorno cerrado de comunicación– se corresponde con lo que habitualmente conocemos como intranet, recurso técnico que cada vez es más utilizado en todas las organizaciones, tanto del sector público como del privado. En cuanto a su naturaleza, podemos considerar que es un medio de identificación y autenticación de la Administración Pública como tal, es decir, como persona jurídica.

Estas redes de acceso restringido están llamadas a ocupar un lugar central en el desarrollo de la cooperación interadministrativa, uno de los objetivos básicos de la LAE. Así, dentro de los mecanismos instrumentales que han de servir de base al desarrollo de la Administración electrónica en nuestro país, uno de los principales es la Red de comunicaciones de las Administraciones.[51] Esta Red, que está siendo desarrollada actualmente, se conoce como Red SARA (Sistema de Aplicaciones y Redes para las Administraciones) y, a su vez, está interconectada con una Red paneuropea denominada Red TESTA. Se prevé que a través de la Red SARA sea posible acceder a múltiples servicios, siendo los primeros en estar disponibles la verificación de los

---

prestar estos servicios a otras Administraciones Públicas, como es el caso, por ejemplo, de la Diputación General de Aragón y numerosas entidades locales de esta Comunidad Autónoma. Otras comunidades han creado sus propios servicios de certificación, como, por ejemplo, el CatCert de Cataluña.

49. Así ocurre, por ejemplo, en las operatorias para la remisión de actas y acuerdos municipales a las Administraciones autonómicas.

50. Siglas de "Autoridad Notarial de Certificación".

51. LAE, artículo 43.

Serie Claves del Gobierno Local, 12
ISBN: 978-84-614-0970-9
Fundación Democracia y Gobierno Local

datos de identidad y residencia, y la plataforma de validación de firma electrónica (@Firma).[52]

9. Algunos retos

Son numerosos los retos, tanto técnicos como jurídicos, que plantea la Administración electrónica. La LAE, como la mayor parte de los expertos, es consciente de que uno de los más importantes y difíciles, y del que depende que la Administración electrónica suponga un aumento importante en la eficiencia de las Administraciones Públicas, es conseguir la interoperabilidad de los sistemas de información utilizados por todas ellas. Por tanto, en su artículo 42 ordena la elaboración de un "Esquema Nacional de Interoperabilidad". Esta previsión legal ha sido desarrollada en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica,[53] el cual dedica su capítulo IX a la firma electrónica. Previamente, en el año 2008, había sido aprobado por el Consejo Superior de Administración Electrónica el "Esquema de identificación y firma electrónica de las Administraciones Públicas", que define la "infraestructura de clave pública"[54] que van a utilizar, al menos en un futuro cercano, las Administraciones españolas.[55]

Otro reto, es el archivo a largo plazo de los documentos. Es sabido que la durabilidad de los documentos electrónicos preocupa a los especialistas, ya que de ella dependerá la historia de nuestra época. Desde un punto de vista técnico está relacionada tanto con la persistencia de los soportes físicos que almacenan los documentos, como con la disponibilidad de los programas necesarios para acceder a su contenido. Pero, además, desde la óptica jurídica, la cuestión no es sólo la conservación

52. Con esta plataforma de validación se cumple con lo dispuesto en el artículo 21. 3 de la LAE, según el cual "la Administración General del Estado dispondrá, al menos, de una plataforma de verificación del estado de revocación de todos los certificados admitidos en el ámbito de las Administraciones Públicas que será de libre acceso por parte de todos los Departamentos y Administraciones."

53. El artículo 42 también ordena la elaboración de un Esquema Nacional de Seguridad, regulado por el Real Decreto 3/2010, de 8 de enero.

54. Suele conocerse también como PKI, por las siglas de *Public Key Infrastructure*, y se refiere al conjunto de los elementos precisos para la utilización de la firma electrónica en un entorno amplio. Aunque se encuentra todavía en fases iniciales de su desarrollo, esta infraestructura tiende a tener, al igual que ocurrió con los nombres de dominio, alcance global. Hay que observar, sin embargo, que mientras el sistema de nombres de dominio se construyó de arriba hacia abajo, partiendo de un órgano único que fue delegando en diferentes órganos nacionales, la PKI global se construirá de abajo hacia arriba mediante acuerdos de confianza entre PKIs formadas en ámbitos locales.

55. El *Esquema de identificación y firma electrónica de las Administraciones Públicas* puede verse en la dirección de Internet: www.ctt.map.es/web/certica

Serie Claves del Gobierno Local, 12 Fundación Democracia y Gobierno Local
ISBN: 978-84-614-0970-9

de los documentos, sino la necesidad de poder validar las firmas en cualquier momento futuro. Este requisito encuentra dos serios obstáculos. Uno la caducidad de los certificados de firma, otro la técnica utilizada para la conservación de documentos a largo plazo, consistente en unificar los distintos formatos de los documentos en un estándar especialmente diseñado para ello, ya que esta transformación invalida las firmas que acompañan a los documentos. La solución del problema es complicada, y una adecuada aplicación del principio de proporcionalidad al establecer los requisitos formales será, probablemente, necesaria.[56]

Pero hay otros problemas relacionados con la interoperabilidad que tienen que ver con la propia naturaleza de los documentos electrónicos porque, aunque en el mundo del soporte papel no hay problema para formar expedientes, integrados por documentos individuales que podían desgajarse de los mismos y cumplir su función en lugares y casos muy diferentes, dicha virtualidad no surge por sí misma en el caso de los documentos electrónicos, sino muy al contrario, ya que éstos no son, a diferencia del documento tradicional, un ente con existencia autónoma, sino un elemento más de un complejo sistema de información.

Cabe prever que esta diferencia entre los documentos electrónicos y los documentos en papel tenderá a acentuarse, ya que la Administración electrónica forma parte de un proceso general de automatización de las tareas de las burocracias. Si la Revolución Industrial se caracterizó por la sustitución del trabajo manual por el realizado por máquinas, sobre todo en las tareas más repetitivas y pesadas, actualmente asistimos también a un proceso de automatización, pero en esta ocasión referido a tareas que consisten en el manejo e intercambio de información. Para ello se estructura el contenido de los documentos electrónicos, de forma que su potencialidad va mucho más allá de la mera transmisión de información entre personas, ya que el objetivo que se persigue es que, en la medida de lo posible, los ordenadores puedan manejar su contenido y realizar algunas operaciones con los mismos.

Actualmente, el XML (*eXtensible Markup Language*)[57] es el estándar más empleado para estructurar el contenido de los documentos de forma que los programas de ordenador puedan manejar la información que contienen. El XML define un metalenguaje para crear dialectos destinados a aplicaciones específicas como, por ejemplo, la contabilidad o los historiales médicos. Hay organismos de ámbito mundial dedica-

56. La Unión Europea ha establecido un "Modelo de Requisitos para la Gestión de Documentos Electrónicos de Archivo", conocido como "MoReq". En nuestro país, el servicio de certificación de la Generalidad de Cataluña ha creado un servicio de archivo a largo plazo para las Administraciones Públicas de su ámbito, denominado iArxiu (www.aoc.cat/index.php/ezwebin_site/INICI/SERVEIS/Serveis-bàsics-d'identitat,-signatura-i-perdurabilitat-electrònica/iArxiu).

57. El XML es un estándar definido por el *World Wide Web Consortium* (W3C).

Serie Claves del Gobierno Local, 12
ISBN: 978-84-614-0970-9
Fundación Democracia y Gobierno Local

dos a esta tarea de estandarización, como la *Organization for the Advancement of Structured Information Standards* (OASIS), una asociación sin ánimo de lucro de la que forman parte las principales multinacionales del sector de la informática. En este marco se están desarrollando dialectos del XML para su uso en el ámbito de los negocios, como el definido por el proyecto ebXML (*Electronic Bussines XML*), pero hace falta que alguien, con suficiente poder prescriptivo, emprenda la elaboración de dialectos dirigidos a las Administraciones Públicas.[58]

Un último aspecto a tener en cuenta es que, en el desarrollo de los sistemas de Administración electrónica, los documentos aparecen generalmente vinculados a una entidad más compleja, como son los actos de comunicación, y que, en cada uno de éstos, es preciso conservar no sólo el documento o documentos que se comunican, con sus respectivas firma o firmas, sino también un sello de tiempo (*time-stamping*), acreditativo del momento en el que se efectuó la comunicación, y las diligencias con el resultado de la verificación hecha en ese momento de la vigencia de cada uno de los certificados que respaldan las firmas.[59] El sellado de tiempo de las firmas es además preciso para poder validarlas en el futuro, comprobando la vigencia de los certificados en el momento en que fueron generadas.

Finalmente, cabe prever que la progresiva automatización de los procedimientos dé lugar al incremento de los actos de comunicación que tendrán lugar directamente entre los sistemas de información. Aunque este hecho, por sí mismo, no tenga por qué suponer un aumento en la complejidad de las operatorias de Administración electrónica, sí que puede suponer una mayor desagregación de los documentos, que cada vez se parecerán menos a los que hoy manejamos para la comunicación entre agentes humanos.

---

58. El siguiente paso es la utilización de la inteligencia artificial, posibilidad que ya contempla la LAE en su artículo 39, al regular la actuación administrativa automatizada, que se caracterizaría por la utilización en la misma de técnicas de inteligencia artificial para la formación de decisiones. Aunque aún es poco frecuente, un ejemplo en nuestro país es la "red neuronal" desarrollada por la Dirección General de Catastro para la valoración de inmuebles. Al respecto puede verse J. Gallego, "La inteligencia artificial aplicada a la valoración de inmuebles. Un ejemplo para valorar Madrid", *Catastro*, abril 2004, p. 51-67. Hay que tener en cuenta que la LAE emplea aquí la misma denominación que para otro tipo de actos automatizados a los que nos hemos referido, por ejemplo, al hablar de los sellos electrónicos, pero éstos son actos cuyo contenido viene unívocamente determinado por una norma, como ocurre en la emisión de un acuse de recibo, o consisten únicamente en aportar al ciudadano información previamente obrante en los sistemas de la Administración, como sería el caso de la emisión de un certificado de vida laboral.

59. Los sellos de tiempo son documentos electrónicos, firmados por una autoridad de sellado de tiempo, que vinculan un momento determinado con un documento a través del resumen (*hash*) del mismo. Se incorporan a los acuses de recibo para garantizar el momento en el que se produjo la recepción de un documento. Por su parte, las diligencias con el resultado de la verificación certifican el resultado obtenido al comprobar que un certificado no ha sido revocado (ver nota 17).

Serie Claves del Gobierno Local, 12 Fundación Democracia y Gobierno Local
ISBN: 978-84-614-0970-9

10. Conclusión

Como hemos visto, la LAE demuestra en diversas ocasiones un claro sentido práctico, seguramente derivado de la experiencia de los años anteriores en el desarrollo de la Administración electrónica. Cabe suponer que, superada la desconfianza inicial de los juristas prácticos hacia los nuevos medios electrónicos, se exijan requisitos y garantías más razonables, con el objetivo de que los aspectos formales no se conviertan en un obstáculo para el desarrollo de la Administración electrónica. Por otra parte, la Ley huye también de entrar en el detalle de cómo deben utilizarse los medios técnicos, y establece un marco general en el que diversas soluciones pueden encontrar cabida. Contribuye a esta actitud no sólo la creciente confianza en las TIC y en las garantías que su utilización ofrece, sino también la convicción de que la constante evolución de la tecnología puede dejar obsoleta, en poco tiempo, cualquier norma cuyo articulado esté excesivamente vinculado a un estado de la técnica.

El desarrollo que a lo largo de estos años ha habido, desde un punto de vista doctrinal, de las cuestiones relacionadas con la Administración electrónica, también ha permitido que la LAE parta de un esquema conceptual más claro que el conjunto de normas que la han precedido, definiendo de forma precisa y denominando de forma clara y unívoca las funciones y elementos que regula. Con ello, la Ley establece una sólida base para el posterior desarrollo teórico y para la didáctica de estas cuestiones. Esta clarificación terminológica comienza con el calificativo que, de forma general, se utiliza para denominar a estos nuevos elementos, y que será el adjetivo "electrónico", descartándose el término "telemático", más utilizado por las nomas anteriores, de forma que, por ejemplo, los registros telemáticos pasan ahora a ser registros electrónicos. En lo referente al tema que aquí nos ocupa, es importante, como se ha visto, la denominación dada a los procesos de identificación de una persona y de autenticación de un documento.

Otro aspecto a destacar de la LAE es la introducción del principio de proporcionalidad, el cual es clave para elaborar operatorias que, siendo seguras tal y como también exige la Ley, no incorporen medidas de seguridad excesivas y que resulten gravosas para los ciudadanos o los empleados públicos que hayan de utilizar los sistemas. Como se acaba de decir, la progresiva familiarización con el uso de los medios informáticos va generando una confianza en los mismos, que favorece esta búsqueda del punto de equilibrio entre seguridad y facilidad de uso.

La disposición adicional segunda de la LAE, dedicada a la formación de los empleados públicos, demuestra que la Ley no olvida, aunque sea simplemente para mencionarlo, este aspecto fundamental del desarrollo de la Administración electrónica. Muchas

Serie Claves del Gobierno Local, 12
ISBN: 978-84-614-0970-9
Fundación Democracia y Gobierno Local

veces se cae en el error de pensar que basta con que una tecnología esté disponible para que comience a utilizarse. Sin embargo el factor humano, es decir, la adopción de la misma por los usuarios, es al final el requisito imprescindible. La firma electrónica avanzada que, desde el punto de vista técnico, está desarrollada desde principios de la década de los 90 del pasado siglo, es una buena prueba de ello, ya que su utilización sigue siendo, pese a todas las facilidades que se dan, muy minoritaria.

En otro orden de cosas, si se actúa de forma adecuada no debe temerse que las nuevas tecnologías supongan un menoscabo de los derechos de los ciudadanos, sino, más bien, todo lo contrario, ya que aparecen nuevas posibilidades de información y participación que abren caminos sumamente prometedores para perfeccionar la democracia.[60] Uno de los elementos que a medio plazo será necesario para aprovechar todas las posibilidades que la sociedad de la información ofrece en este sentido, será el modo como se gestione la identidad electrónica de los ciudadanos. Por tanto, se trata de una cuestión que no sólo está relacionada con el acceso de los ciudadanos a los servicios públicos, sino que tiene un claro carácter político, ya que afecta a derechos fundamentales como la intimidad o la participación en la vida política.

De momento, la LAE ha demostrado una notable amplitud de miras que, unida al tratamiento integral de todos los aspectos relacionados con la Administración electrónica, hace que esta Ley constituya un sólido punto de partida para un período en el que se espera que la tramitación electrónica de los procedimientos deje de ser la excepción y pase a ser la norma en las Administraciones Públicas.

Bibliografía

Bing, J., "Three generations of computerized systems for public administration and some implications for legal decision-making", *Ratio Iuris* 3/2, 1990.

Cruz, D., *Eficacia formal y probatoria de la firma electrónica*, Marcial Pons, Madrid, 2006.

Gamero, E., Valero, J. (eds.), *La Ley de Administración Electrónica*, Thompson-Aranzadi, Cizur Menor, 2008.

Micó, J., *La firma electrónica de notarios y registradores y el documento público electrónico*, Tirant lo Blanch, Valencia, 2007.

60. En esta línea puede verse el documento del Gobierno de los Estados Unidos, "Transparencia y gobierno abierto", publicado en *WhiteHouse.gov.* Un ejemplo de su aplicación es el sitio *Data.gov*, en el que se publicaban 100.000 conjuntos de datos a finales de 2009. Se espera que, mediante el acceso a esta información, la ciudadanía, las ONG y las empresas hagan aportaciones interesantes que se traducirán en mejoras en la forma de gobernar.

Serie Claves del Gobierno Local, 12 Fundación Democracia y Gobierno Local
ISBN: 978-84-614-0970-9

MARTÍNEZ, A., *Comentarios a la Ley 58/2003 de firma electrónica*, Thompson-Civitas, Madrid, 2004.

MUÑOZ, J. F., *Decisión jurídica y sistemas de información*, Colegio de Registradores, Madrid, 2003.

VALERO, J., *El régimen jurídico de la e-Administración. El uso de medios informáticos y telemáticos en el procedimiento administrativo común*, Comares, Granada, 2.ª edición, 2007.

Serie Claves del Gobierno Local, 12
ISBN: 978-84-614-0970-9

Fundación Democracia y Gobierno Local

Serie Claves del Gobierno Local, 12
ISBN: 978-84-614-0970-9
Fundación Democracia y Gobierno Local