

Dictamen jurídico sobre Firma Electrónica DOYFE

Destinatario	Flag Solutions, S.L.		
Páginas	22		
Versión	Fecha	Autor	Descripción
1	24/06/2015	MRC	Redacción del Dictamen
2	02/06/2015	JRA	Revisión del Dictamen
3	10/09/2015	MRC	Versión final

INDICE

1.	ALCANCE DEL INFORME.....	3
2.	ANÁLISIS DE LA LEGISLACIÓN VIGENTE.....	4
	i. Legislación vigente sobre firma electrónica.....	4
	ii. Legislación vigente sobre prueba en juicio.....	4
	iii. Legislación vigente en materia de protección de datos de carácter personal.....	5
3.	RESPUESTA A LA CONSULTA.....	6
3.1.	VALIDEZ JURÍDICA DE LOS SISTEMAS DE FIRMA ACTUALES.....	6
	i. Los certificados de firma electrónica avanzada.....	6
	ii. Los certificados de firma electrónica reconocida.....	6
3.2.	COMPATIBILIDAD DEL SISTEMA DE FIRMA ELECTRÓNICA DE DOYFE CON EL OBJETIVO DE PRECONSTITUIR PRUEBA.....	7
	i. Características del sistema de certificación de correos electrónicos de DOYFE.....	8
	ii. Idoneidad de la preconstitución de prueba mediante documentos electrónicos con firma electrónica.....	11
	iii. Uso indebido de la plataforma por el usuario.....	12
3.3.	VALIDEZ JURÍDICA DE DOCUMENTOS FIRMADOS ELECTRÓNICAMENTE COMO PRUEBA EN JUICIO.....	14
3.4.	PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.....	15
	i. Usuarios del servicio.....	16
	ii. Posibles terceros.....	16
4.	CONCLUSIONES FINALES.....	21

1. ALCANCE DEL INFORME

El presente informe da respuesta a la consulta realizada por FLAG SOLUTIONS, S.L., empresa responsable del servicio bajo la marca DOYFE (en adelante DOYFE) respecto a la validez de los distintos servicios de certificación ofrecidos en la página web www.doyfe.es, que se resumen en los siguientes:

- Certificación de correos electrónicos.
- Certificación de contenidos en páginas web.
- Certificación de fotografías.
- Emisión de actas de certificación.

DOYFE está interesada en obtener una opinión legal acerca de la validez como prueba en juicio de los documentos creados y certificados mediante los servicios web de DOYFE, así como en su caso, las implicaciones legales que pudiera tener en materia de protección de datos de carácter personal.

DOYFE aboga por la preconstitución de prueba en formato electrónico, eliminando, entre otros, trámites ante notario, con el consiguiente riesgo de pérdida de la prueba (por ejemplo, en contenidos disponibles en páginas web que pueden desaparecer en cualquier momento), a la vez que proporciona un documento electrónico que garantiza plenamente la autenticación, integridad, y no repudio de la prueba.

Es por tanto básico para la ejecución de los servicios ofrecidos por DOYFE conocer los mínimos legales exigidos por la normativa para la sustitución del papel por medios informáticos cuyos archivos tengan un valor jurídico equiparable a los actuales documentos en papel o actas notariales.

Para la redacción del presente informe nos hemos basado en el siguiente marco legal:

- Ley 59/2003, de 19 de diciembre, de firma electrónica (LFE).
- Ley 1/2000, de 7 de enero, de enjuiciamiento civil (LEC).
- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal (RLOPD).

La realización del presente informe se ha llevado a cabo mediante la información proporcionada por los interlocutores de DOYFE con la finalidad de realizar una valoración jurídica respecto a la validez de los distintos servicios de certificación.

Este documento analiza la validez jurídica del sistema tal y como se nos ha descrito, y en ningún caso forma parte del alcance del mismo analizar, comprobar o validar los procedimientos técnicos seguidos por DOYFE en la prestación de los servicios.

2. ANÁLISIS DE LA LEGISLACIÓN VIGENTE.

i. Legislación vigente sobre firma electrónica.

La Ley 59/2003, de 19 de diciembre, de firma electrónica, establece expresamente en su primer artículo que las disposiciones contenidas en la misma no alteran las normas relativas a la celebración, formalización, validez y eficacia de los contratos y cualesquiera otros actos jurídicos ni las relativas a los documentos en que unos y otros consten.

Asimismo, la Ley define en su artículo 3 la firma electrónica como aquel conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

La referida normativa define asimismo los conceptos firma electrónica avanzada, como *“la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control”* y firma electrónica reconocida, definida como *“aquella firma electrónica avanzadas basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida, señala la Ley, tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel”*.

Todo ello sin perjuicio de que la Ley de Firma Electrónica asimismo señala en su Artículo 3.9 que *“no se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica”*.

ii. Legislación vigente sobre prueba en juicio.

Para entrar a valorar el valor probatorio de un documento electrónico en juicio, es necesario remitirse a la Ley 1/2000, de 5 de enero, de enjuiciamiento civil, normativa que regula los procedimientos sometidos a conocimiento de jueces y tribunales.

Esta normativa regula, entre muchos otros aspectos, los medios de prueba aceptables en juicio. Así, establece su artículo 299 que se podrá hacer uso en juicio de interrogatorios, documentos públicos o privados, dictámenes de peritos o reconocimientos judiciales.

Asimismo, indica el mismo artículo que se aceptará “ [...] cualquier otro medio no expresamente previsto [...] por el que pudiera obtenerse certeza sobre hechos relevantes”.

Por otro lado, en cuanto a los documentos privados, establece el artículo 326 que harán prueba plena con los mismos efectos que los documentos públicos, siempre que no sean impugnados. Este artículo, a diferencia del indicado anteriormente, sí hace expresa referencia al documento electrónico, estableciéndose que cuando se impugne la autenticidad de este tipo de documentos, se procederá de acuerdo a lo establecido en la LFE.

iii. Legislación vigente en materia de protección de datos de carácter personal

Otro aspecto a tener en cuenta es la protección de los datos de carácter personal del usuario. No sólo ya los datos identificativos, firmas en documentos, otros datos personales como imágenes, etc., que puedan incorporarse en el propio uso de los servicios de DOYFE.

El uso personal de este servicio podría no estar sujeto a la aplicación de la normativa vigente en materia de protección de datos de carácter personal, en tanto que sería un tratamiento de datos realizado en el ámbito estrictamente personal o doméstico. En este sentido por tanto, estos tratamientos entrarían en la excepción del artículo 2 de la LOPD que limita el ámbito de aplicación de la misma.

Sin perjuicio de lo anterior, ciertos usos del servicio, como se indicará más adelante, sí pueden verse afectados por la LOPD, como por ejemplo la custodia de documentos o el uso del servicio con finalidades que excedan del ámbito personal descrito en el párrafo anterior.

3. RESPUESTA A LA CONSULTA.

3.1. VALIDEZ JURÍDICA DE LOS SISTEMAS DE FIRMA ACTUALES

i. Los certificados de firma electrónica avanzada.

De acuerdo a lo dispuesto en el artículo 3 de la Ley 59/2003, se define la **firma electrónica avanzada** como *“aquella que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control”*.

Debe tenerse en cuenta que esta firma tiene validez jurídica, aunque no es equiparable a la firma manuscrita. En caso de ponerse en duda la autenticidad de este tipo de firma, se deberá proceder a comprobar, por parte del prestador de servicios de certificación que hubiese expedido los certificados, que se cumplen los requisitos establecidos en la ley en cuanto a la garantía de los servicios que presta en la comprobación de la eficacia de la firma electrónica. En caso de que se impugne la validez de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, deberá respetarse lo establecido en el artículo 326.2. de la Ley de Enjuiciamiento Civil, es decir, que se procederá al cotejo pericial de letras o se propondrá cualquier otro medio de prueba que resulte útil y pertinente al efecto.

Adicionalmente, debe recordarse que la normativa vigente en materia de firma electrónica establece que cuando se utilice una firma electrónica conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas. **Por ello, si las partes deciden darle plena validez jurídica a los actos jurídicos celebrados entre sí mediante firma electrónica avanzada, aunque no ofrezca las garantías establecidas para la firma electrónica reconocida, debe respetarse tal decisión.**

ii. Los certificados de firma electrónica reconocida.

En virtud de lo establecido en la normativa de firma electrónica citada en el apartado anterior, el sistema electrónico necesario para la sustitución de documentación en papel de forma que se garantice la autenticidad plena de la firma del documento sustituido requiere de la expedición de certificados reconocidos por parte de las dos partes intervinientes, que deberán cumplir las siguientes obligaciones, tal y como establece el artículo 12 de la Ley 59/2003:

- a) Comprobar la identidad y circunstancias personales de los solicitantes de certificado.

- b) Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.
- c) Garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación.

La utilización de certificados reconocidos en la práctica puede plantear dificultades, tanto desde el punto de vista de la necesidad de unificar los distintos estándares utilizados por los operadores, como desde la perspectiva de la necesidad de que el usuario disponga de un certificado de estas características, algo que no es viable exigir a día de hoy.

3.2. COMPATIBILIDAD DEL SISTEMA DE FIRMA ELECTRÓNICA DE DOYFE CON EL OBJETIVO DE PRECONSTITUIR PRUEBA.

El objetivo de los servicios ofrecidos por DOYFE es ofrecer al usuario la posibilidad de preconstituir prueba de todo aquello que pudiera ser del interés de éste. En este sentido, se ofrece (i) la certificación de correos electrónicos, (ii) la certificación de contenidos de páginas web y, (iii) la certificación de fotografías.

Mediante la prestación de estos servicios, el usuario puede obtener un documento electrónico, firmado electrónicamente y con las garantías que estos documentos ofrecen, que le permita acreditar el contenido de un mensaje, la existencia de un contenido ilícito o dañino en una página web concreta o la existencia de un determinado hecho mediante la captación gráfica del hecho (por ejemplo, la fotografía de un siniestro entre vehículos y los resultados del mismo). Con dichos documentos, el usuario obtiene un documento electrónico con suficientes garantías técnicas para emprender aquellas reclamaciones, judiciales o no.

DOYFE genera, para todos los servicios, documentos resumen de la operación, con firma electrónica y sellado de tiempo.

Como ya se ha comentado anteriormente, la firma electrónica permite obtener tres características esenciales:

- *Autenticación*: La firma electrónica permite autenticar que la persona que ha sellado el documento es quien dice ser. En este caso, la firma electrónica identificaría a DOYFE. Sin embargo, el uso del servicio requiere del registro del usuario en la plataforma, por lo que, aunque no quede garantizado el usuario al no comprobarse la identidad del mismo físicamente, esto no resta validez jurídica a la firma del documento.
- *Integridad*: Asimismo, mediante el uso de algoritmos matemáticos, un documento firmado electrónicamente permite garantizar que su contenido no ha sido modificado

desde el momento de la firma, lo que garantiza que es un documento auténtico tal y como el usuario lo envió a DOYFE.

- *No repudio*: Tal y como sucede con la autenticación, el no repudio corresponde en este caso a DOYFE, y no al usuario. De esta forma, DOYFE no podrá negar que certificó un documento concreto, mientras que el usuario deberá demostrar que efectivamente fue él el usuario del servicio.

Asimismo, el sellado de tiempo permite garantizar el momento exacto (esto es, fecha y hora) en la que se generó el documento.

i. Características del sistema de certificación de correos electrónicos de DOYFE.

A continuación, se exponen las características técnicas de los sistemas ideados por DOYFE para cada servicio ofrecido, a fin de describir correctamente todo el procedimiento que se sigue desde la generación del documento hasta la ulterior custodia, puesto que es este procedimiento el que garantiza la veracidad, integridad y validez del documento final.

a) Certificación de correos electrónicos: El sistema desarrollado por DOYFE consiste en un servidor de correo titularidad de Flag Solutions, S.L. con capacidad de recibir correos de cualesquiera remitentes, descargar su contenido, y certificar su envío y contenido mediante firma electrónica y sellado de tiempo.

Así pues, el usuario, una vez registrado en la plataforma, puede hacer uso del servicio mediante el envío de los correos electrónicos a la dirección copia-certificada@doyfe.es o copia@doyfe.es, según se quiera informar al destinatario del uso del servicio o no, que recibirán el correo y certificarán el envío del mismo y su contenido.

El sistema puede usarse como certificación de un envío, incluyendo la dirección electrónica anterior como destinatario, en copia, o en copia oculta (en este caso, se incluiría la segunda dirección únicamente). De este modo, el servidor de correo electrónico de DOYFE recibirá el correo, en el que figurará la dirección de correo electrónico del remitente y, más importante, del destinatario. Aunque como se indicará más adelante el sistema no permite garantizar la recepción del correo por el destinatario, sí permite probar que un correo electrónico se envió y, por tanto, corresponderá a la otra parte demostrar que no fue así.

Los usos de este servicio son diversos, como por ejemplo la negociación de contratos, plasmar la preexistencia de una obra en casos de plagio sirviendo como *registro* privado de la Propiedad Intelectual e Industrial (creación gráfica o literaria, fotografía, etc.), envío de presupuestos, facturas, averías, quejas y reclamaciones, y un largo etcétera.

b) Certificación de contenidos en páginas web: Los servicios ofrecidos mediante la página web www.doyfe.es permiten la certificación de páginas web. Mediante la introducción, por parte de los usuarios registrados, de direcciones web, puede obtenerse una copia fidedigna de lo que ésta contiene.

El servicio de DOYFE realiza dos acciones, por un lado captura la pantalla tal y como el usuario la está viendo, y por otro, captura los datos técnicos de esa página, desde toda la información de la transmisión que se ha llevado a cabo como el código fuente que genera la página web.

De esta forma, queda totalmente acreditado que la página web contenía los contenidos que se muestran en los documentos generados, ya que el usuario no tiene ninguna capacidad de alteración de los mismos desde el momento en que son los equipos de DOYFE quienes acceden a la página web y la certifican y no el usuario quien hace las capturas para luego enviarlo a DOYFE.

Este servicio está principalmente orientado a certificar información relevante contenida en páginas web, comentarios o contenidos ofensivos o ilícitos, demostración de vulneraciones de la propiedad intelectual, derechos de autor, etc.

A diferencia del servicio anterior, no existe aquí ningún problema en cuanto a las características esenciales de la firma electrónica, puesto que la autenticación, integridad y no repudio del documento pueden ir perfectamente vinculadas a DOYFE como sociedad o servicio que ha accedido a la página web (bajo las instrucciones del usuario) y certificado sus contenidos.

En este sentido, no solo no se aprecia diferencia entre el servicio ofrecido por DOYFE en relación a lo que realizaría un notario, sino que además realiza comprobaciones que, por norma general, los notarios no están capacitados para realizar, como es conseguir una trazabilidad de todas las comunicaciones realizadas por la página web certificada, así como el código fuente.

Eso sí, el documento del notario tendría fuerza de documento público, mientras que el documento de DOYFE será un documento privado, sin perjuicio de que pueda elevarse a público mediante testimonio notarial, por ejemplo.

c) Certificación de fotografías: El servicio de fotografía certificada requiere de la instalación en un Smartphone de la aplicación móvil de DOYFE. Dicha aplicación, en el momento de realizar una fotografía con ella, realiza las siguientes acciones:

- *Fotografiar con la cámara trasera:* Se captura lo que el usuario quiere certificar.
- *Fotografiar con la cámara delantera:* Para identificar, en su caso, a la persona que realiza la fotografía.
- Obtención de datos técnicos de la fotografía, que podrían compararse en un momento posterior con los datos de la fotografía original.
- Captura de la posición en la que se realizó la fotografía mediante la geolocalización del propio Smartphone.

Las finalidades de este servicio son variadas, en tanto que sirve para dejar constancia gráfica de la existencia de un hecho, como pueden ser averías o estados de objetos, accidentes de tráfico, demostrar la pre-existencia de diseños titularidad del autor, etc.

En este sentido, aplicar la firma electrónica y el sellado de tiempo a una fotografía realizada mediante la aplicación móvil de DOYFE garantiza todas las características básicas de un documento firmado electrónicamente, en tanto que existe autenticación de la persona que ha realizado la fotografía, mediante la captura realizada con la cámara frontal, integridad en tanto que al realizarse todo el procedimiento desde la propia Aplicación (APP) no existe posibilidad de alterar la fotografía, y no repudio, desde el momento en que el procedimiento automatizado de DOYFE firma electrónicamente la imagen en el momento de su captura por parte del usuario, por lo que no puede negarse su realización.

En cuanto a las medidas de seguridad establecidas por la Ley de Protección de Datos de Carácter Personal, el sistema de DOYFE garantiza el cumplimiento de todas ellas, en cuanto al tratamiento del consentimiento informado (no es objeto del presente dictamen el análisis del cumplimiento de la LOPD de toda la plataforma), ya que, entre otras:

- no es posible el tratamiento de información mediante soportes no controlados por el sistema o DOYFE.
- la existencia de un servidor externo, como es el caso, podría funcionar como sistema de copias de seguridad de estos documentos, si bien es cierto que no es su principal finalidad.
- los documentos son generados automáticamente por el sistema, en formato PDF, con el consecutivo encapsulamiento de los contenidos mediante las firmas electrónicas y

el sellado de tiempo final, por lo que se garantiza la no modificación de los documentos a posteriori. Aún así, es importante destacar que, por un lado, tanto el sistema propio de DOYFE como el de custodia en el servidor externo cuentan con sus respectivos sistemas de generación de LOGS firmados electrónicamente de forma diaria con el fin de que quede absolutamente garantizada su integridad, y que, además, conservan la información exigida por la LOPD, lo que en el servidor externo supone un añadido a la certificación como documento original y no manipulado.

- Las comunicaciones, tanto con el servidor externo como los emails enviados al usuario, se realizan previo cifrado de los datos, siendo por tanto comunicaciones seguras que no permitan su acceso por terceros.

ii. Idoneidad de la preconstitución de prueba mediante documentos electrónicos con firma electrónica.

Históricamente los documentos aportados en juicio eran documentos manuscritos o documentos en papel originales, que gozaban de por sí de validez formal para ser presentados como prueba.

Por el contrario, el documento electrónico posee unas características intrínsecas que conllevan ciertos inconvenientes para garantizar su capacidad de probar, como por ejemplo:

- Son de fácil alteración.
- Carecen de certeza en cuanto a autoría y datación.
- No puede distinguirse un original de una copia.

La firma electrónica se desarrolló como concepto jurídico precisamente para evitar la inseguridad jurídica que se creaba al trabajar con documentos electrónicos. Así como era difícil negar la firma de un contrato, en especial cuando se trataba de originales firmados manuscritamente por las partes, es relativamente fácil desacreditar la aceptación de unas condiciones de contratación que se remitieron en formato electrónico por correo electrónico.

Como se ha venido indicando, los documentos firmados electrónicamente poseen unas características propias que permiten salvar esta inseguridad jurídica, dotando a los documentos de mayores garantías, mediante la aplicación de técnicas criptográficas y algoritmos matemáticos que permiten la ejecución de procedimientos técnicos que, a su vez, garantizan que el firmante es quien dice ser, que el contenido no se ha manipulado desde su firma, y que la firma es válida y no puede ser negada.

Los sistemas de preconstitución de prueba ofrecidos por DOYFE permiten por tanto ofrecer la garantía a sus usuarios de que dicho documento o prueba existía como tal en el día en que se firmó. Así, si lo que se quiere garantizar es el cumplimiento de la obligación legal de remitir a un comprador las condiciones generales de compra en una operación por internet (de acuerdo a lo exigido por la Ley de Defensa de los Consumidores), la certificación de un correo electrónico junto las condiciones generales de contratación adjuntadas al mismo, permitirían que el vendedor pudiera acreditar en cualquier momento que efectivamente las mismas se enviaron a una dirección de correo determinada por el comprador, el contenido del correo y sus adjuntos, así como el día y hora exactos en que fueron enviadas.

Otro ejemplo sería el de la certificación de los daños causados, por ejemplo, en un accidente de tráfico. Si el usuario pretende dejar constancia de los daños en ambos vehículos para evitar un fraude a la compañía aseguradora, el uso de los servicios de DOYFE permitirían demostrar que el accidente tuvo lugar en la fecha y hora en que se tomó la fotografía.

Teniendo lo anterior en cuenta, los servicios de DOYFE son totalmente válidos como preconstitución de prueba desde el momento en que permite superar los inconvenientes típicos de los documentos electrónicos garantizando la integridad del documento y la fecha y hora exacta del mismo, así como garantizar en gran medida la identidad de la persona que lo genera.

iii. Uso indebido de la plataforma por el usuario.

Durante la revisión de la plataforma DOYFE se han detectado algunos aspectos que, por un lado, pueden desvirtuar algunos de los aspectos característicos de la firma electrónica, y en otros en un momento dado pueden poner en duda la validez de la solución.

El aspecto que puede desvirtuar las características de la firma electrónica es el hecho que la firma del documento la realiza un tercero, y no el usuario en sí. Actualmente, para obtener un certificado electrónico, el interesado debe personarse ante la entidad certificadora para que ésta verifique que, efectivamente el solicitante es a quien se le hace entrega del certificado.

En los sistemas de DOYFE, esta identificación fehaciente como tal no existe. Es decir, el usuario se registra en el sistema, pero no se realiza en ningún momento una verificación de que dicho usuario es efectivamente quien dice ser. Esto puede afectar, en algunos casos, a la autenticación en el documento firmado electrónicamente.

Sin perjuicio de lo anterior, cabe tener en cuenta que los sistemas de DOYFE son totalmente compatibles con firmas electrónicas propias que los usuarios pudieran tener instalados o incluso a elementos de firma electrónica reconocida (como por ejemplo el DNle). De esta forma, se garantizaría la autenticidad y el contenido incluso antes de que los contenidos firmados abandonaran el propio ordenador del usuario, superponiéndose las firmas del usuario y la de DOYFE como prestador del servicio, añadiendo y certificando además toda la información técnica relativa al envío, aspectos que el usuario por sí no podría garantizar.

Por otro lado, puede haber supuestos en los que incurra mala fe del usuario como por ejemplo:

- **Correo electrónico:** puede ser redactado conteniendo afirmaciones falsas. La veracidad de los contenidos del correo electrónico no pueden ser garantizadas por DOYFE, al actuar el usuario en un momento previo a la intervención de DOYFE y siendo un procedimiento manual que dependerá siempre de la intención con la que el usuario utilice el servicio.
- **Página web:** en el supuesto de que un tercero alterase maliciosamente una página Web (ciberdelincuencia), DOYFE certificará el contenido alterado existente en el momento de la certificación, constituyendo prueba de la misma. En el supuesto que el usuario del servicio sea utilizado por el atacante de la página web sea la persona que ha alterado la página web, o un tercero que ha encontrado la misma alterada, efectivamente dispondrá de una prueba de que la página web mostraba un determinado contenido en un determinado momento, del mismo modo que si dicho atacante o tercero hiciera capturas de pantalla y acudiera al notario (o solicitara que éste hiciera dichas capturas) para protocolizar la existencia de dichos contenidos. Por tanto, se trata de una acción ajena al control de DOYFE y dependiente de un acto ilícito previo.
- **Fotografía:** cuando se falsea intencionadamente la escena antes de ser fotografiada, DOYFE garantizará fehacientemente la fecha, hora, lugar y demás datos técnicos de la fotografía, independientemente de que el contenido de la escena pueda ser impugnado. Cabe destacar en cualquier caso que el acto de manipulación es previo a la intervención de los procedimientos de DOYFE, ya que una vez realizada la fotografía, ésta no puede ser modificada.

Sin perjuicio de los usos indebidos que pueden ser llevados a cabo por el usuario indicados anteriormente, no cabe pensar que el servicio en sí es incorrecto, o que no permite ofrecer lo que desde DOYFE se pretende. Al contrario, el sistema en sí es suficientemente robusto desde el momento en que la mayoría de operaciones las realiza DOYFE en sus propias máquinas y de forma automática, por lo que la intervención humana en el proceso de certificación es totalmente inexistente. En este sentido, DOYFE certifica lo que el usuario desea certificar,

siendo que si lo certificado no se corresponde a la realidad, se debe necesariamente a una manipulación del sistema por parte del usuario, como en los ejemplos descritos anteriormente.

3.3. VALIDEZ JURÍDICA DE DOCUMENTOS FIRMADOS ELECTRÓNICAMENTE COMO PRUEBA EN JUICIO.

Como ya se ha comentado anteriormente, tanto la **LFE** como la Ley de Enjuiciamiento Civil reconocen la plena validez de los documentos firmados electrónicamente.

En este sentido, es importante tener en cuenta que un documento electrónico tiene, por sí mismo, la misma calificación que un documento en formato papel. En el caso que nos ocupa, es importante tener en cuenta el artículo 3.6 de la **LFE**, cuyo apartado c) indica que *el documento electrónico será soporte de documentos privados*, añadiendo el punto 7 de dicho artículo que *los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable*.

Por tanto, sabiendo que un documento electrónico es considerado un documento privado, cabe acudir a la LEC para comprobar que, efectivamente, el artículo 299 establece que el documento privado es efectivamente un medio de prueba del que se puede hacer uso en juicio.

Por otro lado, el artículo 268 de la mencionada LEC indica que *[...] los documentos privados que hayan de aportarse se presentarán en original, añadiendo en su punto segundo que si la parte sólo posee copia simple del documento privado, podrá presentar ésta, ya sea en soporte papel [...] que surtirá los mismos efectos que el original"* .

El documento electrónico reviste de una particularidad frente al documento convencional, y es que es difícil calificar a un determinado documento electrónico como original, ya que por el hecho de copiar un documento electrónico en otro soporte (por ejemplo, del ordenador a un pendrive), este documento no ha perdido su originalidad, como sí sucedería al realizar una fotocopia de un documento manuscrito. En cualquier caso es importante lo indicado en el artículo anterior, en tanto que una copia simple puede surtir los mismos efectos que el documento original. Es lógico pensar que el artículo va orientado a documentos físicos y no electrónicos, pero nada dice al respecto, por lo que la afirmación del punto segundo sirve por lo menos para no tener que demostrar que el documento electrónico aportado es el archivo original, el primero que se creó.

En cualquier caso, volviendo a los documentos firmados electrónicamente, el artículo 3.8 de la LFE añade, respecto lo visto hasta el momento, que “[...]el soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio[...]”.

Por tanto, no cabe duda, vista la regulación de ambos cuerpos normativos, que (i) el documento electrónico es válido como prueba en juicio en tanto que es documento privado, y (ii) cualquier soporte en el que existan datos que esté firmado electrónicamente será, directamente y sin necesidad de hacer mayores análisis, admisible como prueba documental en juicio.

Hay que tener en cuenta, sin perjuicio de todo lo indicado anteriormente, que la prueba electrónica es una prueba generalmente impugnada, por la fragilidad que, por las propias características de cualquier documento electrónico, muestran éstos para garantizar ninguna autenticidad. Los correos electrónicos, documentos de Word, incluso imágenes o documentos PDF son fácilmente manipulables sin que exista trazo alguno de dicha manipulación.

En este sentido, es muy importante para la validez de la prueba en juicio la forma de funcionar de los servicios de DOYFE. Al configurarse como tercero independiente, garantiza, en todos sus servicios, que el contenido no se ha manipulado desde que se envió dicho correo, se solicitó la certificación del contenido de una determinada página web o se tomó una fotografía concreta. Sencillamente el usuario del servicio no tiene esa posibilidad de manipular el documento electrónico, puesto que recibe dicho documento ya firmado electrónicamente.

Por tanto, el propio sistema de DOYFE descarta, a priori, la posibilidad de impugnación de la prueba por parte de un contrario, puesto que no puede existir duda sobre la veracidad del contenido del documento electrónico, tal y como se ha firmado.

La adición de la firma electrónica avanzada de DOYFE sirve, por tanto, como medio de garantía adicional para probar que los documentos electrónicos aportados como prueba no han sufrido modificaciones desde que se crearon. La firma aplicada por DOYFE es una firma electrónica avanzada, lo que garantiza con suficiente fortaleza las características esenciales de la firma electrónica que, como hemos visto anteriormente, se basan en la autenticación, integridad y no repudio.

3.4. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El servicio de DOYFE supone el tratamiento, por parte de la Compañía, de datos de carácter personal, por un lado del propio usuario que utiliza el servicio, y por otro, en determinadas

ocasiones, es probable que también de terceros como destinatarios de un correo electrónico, o en el cuerpo de éste, o en un comentario de una página web, o incluso la imagen de un tercero en una fotografía.

Cabe sin embargo plantearse hasta que punto aplica realmente la normativa de protección de datos a estos distintos supuestos.

i. Usuarios del servicio.

Todo usuario debe registrarse en la plataforma de DOYFE con carácter previo al uso de sus servicios. Esto evidentemente supone la creación de un fichero de usuarios (o clientes) y el tratamiento de los datos solicitados en el formulario de registro.

Se ha comprobado la existencia de un fichero declarado al Registro General de Protección de Datos, así como que en el formulario de registro, el usuario debe aceptar obligatoriamente las “*condiciones legales*”, que incluyen una cláusula que recoge debidamente lo exigido por la LOPD.

ii. Posibles terceros.

Como indicábamos anteriormente, puede darse el caso que cuando un usuario registrado desee certificar el envío de un correo electrónico, incluya una dirección de correo electrónico personal (si fuera profesional, podría aplicar, según el contenido del correo, la excepción del artículo 2.2 del RLOPD), considerada dato de carácter personal por la normativa de protección de datos.

En este sentido, DOYFE podría ser considerado Encargado del Tratamiento de acuerdo al artículo 12 de la LOPD y 20 y siguientes del RLOPD, debiendo por tanto formalizar un contrato por escrito con el usuario que solicita el servicio, así como obligarse a eliminar los datos una vez finalizada la relación contractual, aplicar determinadas medidas de seguridad, etc.

En cualquier caso, para determinar correctamente la postura a adoptar por parte de DOYFE, hay que tener en cuenta las diferentes esferas de los usuarios en las que pueden prestarse los servicios prestado por DOYFE:

- a) Usuario persona física con finalidades puramente personales.

La LOPD aplica únicamente en aquellos casos en los que existe un fichero organizado de datos personales objeto de tratamiento por parte de su Responsable. Sin embargo, el artículo

2.2 de la LOPD excluye del ámbito de aplicación de la normativa los ficheros y tratamientos con finalidad limitada al ámbito doméstico de dichas personas físicas.

Así, el mantenimiento de un listín telefónico de contactos, o de una agenda con correos electrónicos, siempre que sea con una finalidad puramente personal de la persona física y sin salir de este ámbito doméstico, no se vería afectado por la previsiones de la LOPD. En este sentido se han pronunciado en diversas ocasiones tanto la Agencia Española de Protección de Datos (AEPD) como la Audiencia Nacional. Es destacable la sentencia de este órgano de 15 de junio de 2006, que recuerda la fundamentación jurídica de esta excepción, indicando:

“Lo relevante para la sujeción al régimen de protección de datos no será por tanto que haya existido tratamiento, sino si dicho tratamiento se ha desarrollado en un ámbito o finalidad que no sea exclusivamente personal o doméstico. Qué ha de entenderse por “personal” o “doméstico” no resulta tarea fácil. En algunos casos porque lo personal y lo profesional aparece entremezclado. En este sentido el adverbio “exclusivamente” utilizado en el art. 2.2.a) apunta a que los ficheros mixtos, en los que se comparten datos personales y profesionales, quedarían incluidos en el ámbito de aplicación de la ley al no tener como finalidad exclusiva el uso personal. Tampoco hay que entender que el tratamiento se desarrolla en un ámbito exclusivamente personal cuando es realizado por un único individuo. Por ejercicio de una actividad personal no debe entenderse ejercicio de una actividad individual. No deja de ser personal aquella actividad de tratamiento de datos que aun siendo desarrollada por varias personas físicas su finalidad no trasciende de su esfera más íntima o familiar, como la elaboración de un fichero por varios miembros de una familia a los efectos de poder cursar invitaciones de boda. Y un tratamiento de datos personales realizado por un solo individuo con finalidad profesional, mercantil o industrial estará claramente incluido en el ámbito de aplicación de la ley 15/1999. Será personal cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos”.

Asimismo, en el informe de la AEPD 615/2008, sobre la actuación de unos padres que comparten fotografías de sus hijos, mediante páginas web, de las actividades extraescolares, se incide en que *“Para que nos hallemos ante la exclusión prevista en el artículo 2 LOPD, lo relevante es que se trate de una actividad propia de una relación personal o familiar, equiparable a la que podría realizarse sin la utilización de Internet, por lo que no lo serán aquellos supuestos en que la publicación se efectúe en una página de libre acceso para cualquier persona o cuando el alto número de personas invitadas a contactar con dicha página resulte indicativo de que dicha actividad se extiende más allá de lo que es propio de dicho ámbito”.*

Los textos anteriores dejan abierta la posibilidad de que los servicios de DOYFE no queden excluidos de la aplicación de la LOPD, puesto que concretamente del informe de la AEPD mencionado podría concluirse que, si la página web a la que se hace referencia tuviera su acceso restringido a terceros, quedaría dentro del ámbito doméstico de los usuarios de la misma. En este sentido, siempre que el usuario mantuviera cualquier documento certificado por DOYFE en su esfera más íntima y personal, el servicio de DOYFE no se habría visto afectado por las disposiciones de la LOPD, pudiendo no ser así en la mayoría de supuestos.

b) Usuario persona física con finalidades que exceden el ámbito doméstico.

Sin perjuicio de lo anterior, cabe tener en cuenta que DOYFE no puede controlar la finalidad para la cual se van a utilizar sus servicios, pudiendo perfectamente exceder de ese ámbito más íntimo, por ejemplo al utilizarlo para cursar, por ejemplo, reclamaciones a comercios o profesionales que le hayan prestado algún servicio.

Aunque realmente la aplicación de la LOPD en estos casos no es clara, puesto que la propia AEPD o la Audiencia Nacional no han logrado, en todos estos años, conseguir delimitar de forma pacífica lo que es el ámbito doméstico, es correcta la opción adoptada por DOYFE de regular, en sus condiciones de contratación, la figura del Encargado del Tratamiento.

En este sentido, se da cobertura a las obligaciones de los artículos 12 de la LOPD y 20 y siguientes del RLOPD, siendo que si efectivamente el uso que el usuario pueda hacer de los servicios excede de su ámbito personal la relación estaría cubierta correctamente, mientras que en caso contrario, en nada afectaría la cláusula incluida sobre el encargo del tratamiento.

La cláusula incluida en las condiciones del servicio de DOYFE es legalmente válida, por lo que los servicios de DOYFE son totalmente compatibles con las disposiciones de la normativa vigente en materia de protección de datos.

c) Usuario persona jurídica.

En última instancia, analizaremos el usuario persona jurídica, ya que los servicios de DOYFE van orientados tanto a personas físicas como personas jurídicas. A éstas últimas les es de aplicación la LOPD en toda su extensión, ya que es obvio que no puede aplicar en ningún caso la excepción del ámbito doméstico, en tanto que las personas jurídicas, aún en su funcionamiento interno, carecen de esfera personal.

En este sentido, DOYFE deberá constituirse como Encargado del Tratamiento de dichas personas jurídicas, lo que como ya hemos comentado anteriormente, se encuentra debidamente regulado en las Condiciones Generales de Contratación.

Cobra especial importancia, en los servicios prestados a personas jurídicas y sin perjuicio de que también pudiera aplicarse a los prestados a personas físicas, el nivel de medidas de seguridad que deberá adoptar DOYFE durante la prestación de los servicios. La cláusula actual prevé la adopción de las medidas de seguridad de nivel Básico. Esta aproximación nos parece adecuada, ya que DOYFE no puede conocer, por el mero uso de los servicios por parte de los usuarios, las medidas de seguridad a adoptar.

Existirían aquí dos posibilidades. La primera, más garantista, sería aplicar las medidas de seguridad de nivel alto en todo momento, garantizando que sea cual sea el uso dado a los servicios, se cumpliría plenamente con la normativa. La segunda, opción escogida por DOYFE, no ofrece tantas garantías, en tanto que es el usuario quien, voluntariamente, debe comunicar el nivel de seguridad aplicable a DOYFE mediante la dirección de correo electrónico doyfe@doyfe.es.

Esta segunda opción, aunque consideremos que es menos garantista en tanto que se deja al arbitrio del usuario el comunicar las medidas de seguridad a aplicar, no debe considerarse en ningún caso inválida. Es de hecho la forma habitual de configurar la relación con el encargado del tratamiento incluso cuando la contratación se realiza mediante contrato negociado y firmado por el Responsable y el Encargado, sin recurrir a Condiciones Generales habitualmente de adhesión, puesto que no es responsabilidad del Encargado del Tratamiento determinar las medidas de seguridad, salvo que conozca exactamente la tipología de datos a tratar.

Es importante resaltar que la normativa dispone como obligación del responsable de tratamiento comunicar al encargado del mismo las medidas de seguridad que deberá aplicar al tratamiento encomendado. Si el Cliente no le comunicase las medidas de seguridad a aplicar y éste ha aceptado las medidas de seguridad ofrecidas por DOYFE en las Condiciones Generales de Contratación, DOYFE podría presumir que las mismas son suficientes para proteger los datos objeto del encargo.

Por tanto, dejar al arbitrio del usuario del servicio la determinación, y por tanto comunicación a DOYFE, de las medidas de seguridad a aplicar, no solo es totalmente válido, sino que es el procedimiento habitual en la determinación de los servicios.

De acuerdo con todo lo anterior, cabe indicar pues que, sea como fuera que se prestaran los servicios (ámbito personal, a persona física excediendo la esfera privada, o a persona jurídica),

DOYFE cumple, y se encuentra en posición de cumplir en cualquier momento, la normativa vigente en materia de protección de datos, en lo que a la prestación de su servicio se refiere.

Obviamente, igual que sucedía con la veracidad de lo certificado, se dependerá siempre del cumplimiento de la normativa por parte de los usuarios, lo que en cualquier caso sería un incumplimiento de la normativa por parte de éstos y no de DOYFE.

d) Medidas de seguridad.

DOYFE manifiesta que toda la solución se ha diseñado partiendo de las bases del Privacy by Design (Privacidad desde el diseño), aplicando por defecto las medidas de seguridad de nivel medio independientemente del tipo de usuario que contrate los servicios.

Por tanto, no hay duda que, salvo en casos especiales, la plataforma DOYFE garantiza unos estándares de seguridad superiores a los que serían necesarios en la mayoría de los casos.

4. CONCLUSIONES FINALES

Una vez analizados los distintos aspectos de la solución desarrollada por DOYFE, no cabe otra opción que determinar la validez de la misma para **los documentos firmados electrónicamente por DOYFE**, creados mediante procedimientos que garantizan la no manipulación durante la fase de firmado de los contenidos proporcionados por los usuarios, **son totalmente válidos como prueba en juicio.**

Asimismo, **tampoco existe riesgo de incumplimiento de la normativa de protección de datos**, en tanto que las condiciones de contratación de los servicios de DOYFE cumplen con lo exigido por la mencionada normativa, y DOYFE aplica las medidas de seguridad de nivel básico, encontrándose además en condición de aplicar también las de nivel medio y/o alto si el usuario así lo indica.

Aunque no era objeto del presente informe, DOYFE también preguntó por la validez internacional de la firma electrónica aplicada mediante los servicios prestados por ésta. No es una cuestión clara la validez de la firma electrónica, sin embargo, no hay que olvidar que ésta se basa en procedimientos informáticos y matemáticos que deben cumplir unas características determinadas para garantizar la validez de la firma y, por ende, del documento y la identificación del firmante.

Cabe además tener en cuenta que la normativa de firma electrónica española es una de las más exigentes, al derivar de la ya exigente Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco común para la firma electrónica ya que en síntesis la misma establece los criterios para el reconocimiento jurídico de la firma digital, centrándose en los servicios de certificación.

Dichos criterios son:

- obligaciones comunes de los proveedores de servicios de certificación, para garantizar el reconocimiento transfronterizo de las firmas certificadas en la Comunidad Europea;
- normas comunes en materia de responsabilidad para fomentar la confianza, tanto entre los consumidores que utilizan los certificados como entre los proveedores de servicios;
- mecanismos de cooperación para facilitar el reconocimiento transfronterizo de las firmas y certificados en las relaciones con terceros países.

A la vista de lo anterior, sería correcto deducir que una firma electrónica que cumpla con la normativa española debería ser válida en cualquier otra jurisdicción, o por lo menos en aquellas en las que exista una normativa equivalente que regule la firma electrónica.

En definitiva, los servicios prestados por DOYFE cumplen con los objetivos marcados por la Compañía.

Dictamen realizado por Ribas y Asociados para Flag Solutions, S.L.

Marc Rius Calaveras
Abogado

A handwritten signature in blue ink, consisting of stylized initials and a surname, enclosed within a circular scribble.