Septiembre 2016

COLECCIÓN
DESAFÍOS LEGALES

LA PRUEBA ELECTRÓNICA

VALIDEZ Y EFICACIA PROCESAL

¿ En qué consiste la prueba electrónica?
¿Qué elementos debe reunir para que sea válida y eficaz en el proceso?
¿Se puede manipular?

Prólogo de Ángel Dolado Pérez

Juez Decano de Zaragoza

Coordinadores:
Ricardo Oliva León y Sonsoles Valero Barceló

JURISTAS con FUTURO

eBook

Colección: Desafíos Legales #RetoJCF
Juristas con Futuro

Juristas con Futuro www.juristasconfuturo.com
E-mail: info@juristasconfuturo.com
Tel.: (+34) 69 95 51 887

1º edición - Septiembre de 2016

Diseño y maquetación del eBook:
Sonsoles Valero Barceló

Diseño web:
Óscar Domínguez Merino

Fotografía de la Portada:
Sonsoles Valero Barceló.

ISBN: 978-84-617-4743-6

COLECCIÓN DESAFÍOS LEGALES

LA PRUEBA ELECTRÓNICA

Validez y eficacia procesal

Coordinadores:

Ricardo Oliva León

Sonsoles Valero Barceló

Dedicatoria

A los jueces y magistrados por el esfuerzo que deben hacer para impartir justicia en un mundo cada vez más global y tecnológico.

A los compañeros abogados que se esfuerzan diariamente por realzar el valor de nuestra profesión en la defensa los derechos y libertades fundamentales de los ciudadanos, mientras navegan entre las aguas del Derecho y la tecnología.

A los notarios sinceramente preocupados por servir al ciudadano mientras ejercen su rol de juristas garantes de la fe pública.

A los prestadores de servicio de certificación, terceros de confianza y emprendedores preocupados por proveer soluciones tecnológicas dirigidas a resolver problemas relevantes del sector legal, abriendo con sus iniciativas un camino hacia la innovación jurídica.

A los peritos informáticos que nos ayudan a ver lo que nuestros ojos no pueden percibir en materia de prueba electrónica.

"Algunas personas quieren que algo ocurra, otras sueñan con que pasará y otras hacen que suceda."

Michael Jordan

Listado de palabras clave

Actas notariales

Contratos a distancia

Documento electrónico

Capturas de pantalla

Cotejo pericial de letras

Encriptación de archivo

Fichero electrónico

Fotografía analógica

Fotografía digital

Firma electrónica

Hash

Hecho digital

Metadatos

Notario

Pantallazos

Prestador de servicios de certificación

Prestadores cualificados de servicios de confianza

Prestador de servicios de comunicaciones

Perito informático

Prueba electrónica

Prueba digital

Prueba tecnológica

Prueba pericial informática

Prueba ilícita

Sellos de tiempo

Soporte analógico

Soporte material

Soporte duradero

Soporte electrónico

Técnicas de comunicación a distancia

Teoría del fruto del árbol envenenado

Terceros de confianza

WhatsApp

Tabla de Contenidos

Parte IV: Prestadores de Servicios de Confianza

Epílogo

Infografía

Presentación

Ricardo Oliva León*
Editor y fundador de Juristas con Futuro
@RicardoOlivaON

En los tiempos actuales es cada vez más común que la información que circula por Internet resulte esencial para probar la vulneración de un derecho fundamental (intimidad, honor, imagen, secreto de las comunicaciones), el uso ilegítimo de la propiedad intelectual (fotos, textos, vídeos), la comisión de un delito en la red (amenazas, relevación de secretos, intrusismo informático, estafas, injurias, calumnias), el tratamiento no autorizado de datos personales, el incumplimiento de un contrato (transacciones celebradas a distancia), etc.

De este modo, la Sociedad de la Información nos plantea un gran reto: la oportunidad de conocer herramientas tecnológicas útiles y fiables, y la necesidad de identificar una categoría de profesionales especializados que nos ayuden a demostrar que la información que hemos extraído de la red es fidedigna. Esto implica poder descartar cualquier manipulación en el contenido de dicha información, es decir, estar en aptitud de acreditar la autenticidad de la misma frente a una autoridad, comúnmente, los tribunales de justicia.

* Abogado especialista en Derecho tecnológico y Derecho de sociedades. Letrado colegiado ejerciente en España y Perú. Socio de Lexmotive Law Group, boutique especializada en Derecho tecnológico. Profesor de Derecho Digital en el Centro Universitario Villanueva (Curso de Derecho Digital) y en la Universidad Antonio de Nebrija (Executive Master Business Innovation en Security & Safety y Medical & Health, coordinado por el Grupo GEES Spain). Miembro del equipo ganador del 1º Legal Hackathon de España, realizado en Bilbao en mayo de 2015. Ha estudiado y trabajado en Perú, Portugal, Alemania, Reino Unido, Francia, Italia y los Estados Unidos de América. Fundador y editor de Juristas con Futuro. Autor del blog Des-complicando el Lenguaje Jurídico. Puedes escribirle a ricardo@lexmotive.com. Junto con Sonsoles Valero Barceló ha sido el encargado de coordinar este eBook.

En el argot del Derecho Digital a este nuevo medio probatorio se le conoce como **prueba electrónica** (algunos también lo conocen como prueba digital, prueba informática, prueba tecnológica y ePrueba).

¿Cómo afecta la **prueba electrónica** al trabajo de los juristas? Desde la perspectiva de los **abogados** la **prueba electrónica** nos impone un triple desafío:

1. Resulta indispensable saber cómo recogerla, trasladarla y custodiarla debidamente a fin de garantizar su autenticidad, inalterabilidad e indemnidad y, a la larga, su validez y eficacia procesal.
2. Es necesario saber cómo afrontar la incorporación de la prueba electrónica al proceso judicial, independientemente de si nos encontramos en el orden jurisdiccional civil, penal, contencioso-administrativo o social.
3. Es recomendable saber cómo reaccionar cuando la parte contraria nos opone una prueba electrónica que puede perjudicar los intereses de nuestro cliente.

Desde la perspectiva de los **jueces y magistrados** la **prueba electrónica** exige conocer las diversas formas en qué se manifiestan los medios probatorios de carácter electrónico y especialmente comprender cómo funcionan los mecanismos que permiten asegurar que los datos recogidos en tales medios probatorios no han sido modificados indebidamente por las partes con el fin de alterar la realidad para obtener una sentencia favorable a sus intereses.

La ciencia nos provee hoy en día herramientas tecnológicas destinadas a garantizar el origen y la integridad de los datos incorporados en un documento electrónico -la prueba electrónica por excelencia- como sucede con los sellos de tiempo electrónico.

El ordenamiento jurídico, por su parte, reconoce la labor de diversos profesionales especializados dedicados a dotar de las máximas garantías a las pruebas que acreditan lo que ha sucedido en el mundo digital. Me estoy refiriendo a los notarios, peritos informáticos, prestadores cualificados de servicios de confianza y prestadores de servicios de certificación. La labor de estos agentes no es para nada excluyente. Muchas veces su trabajo es complementario e, incluso, necesario, si pretendemos dotar de validez y eficacia procesal a la **prueba electrónica** al interior de un proceso judicial.

Parafraseando la frase de Antoine de Saint-Exupéry, en El Principito, puedo decir que **en materia de prueba electrónica lo esencial es invisible para nuestros ojos**.

El equipo de **Juristas con Futuro**, consciente de esta realidad, promovió un debate público a través de Twitter (desde la cuenta @JuristasFuturo y con el hashtag #Reto2JCF) dirigido a analizar, precisamente, todo y cuanto concierne a la **prueba electrónica**. Dicha convocatoria pública fue lanzada el 11 de marzo de 2016 y se enmarca dentro de lo que hemos bautizado como los **Desafíos Legales de Juristas con Futuro**.

El segundo desafío (el primero versó sobre la viabilidad legal del testamento digital y el tratamiento jurídico post-mortem del patrimonio digital, y originó al **1º eBook de Juristas con Futuro, descargable gratuitamente desde nuestra web**), cuyas reglas se **publicaron oportunamente**, constituye el germen del 2º eBook que ahora tengo el gran placer de presentar.

El objetivo perseguido con los desafíos legales de Juristas con Futuro es fomentar un debate colectivo abierto, especializado e inclusivo donde todos los participantes puedan analizar una relevante cuestión legal concreta relacionada con el mundo de las nuevas tecnologías. Los desafíos legales de Juristas con Futuro son una especie de ciberpalestra donde abogados, jueces, magistrados, fiscales, notarios, profesores de Derecho, investigadores jurídicos, peritos, policías junto con emprendedores del sector legal discurren e intercambian reflexiones en torno al reto legal planteado.

El libro digital que ahora tienes frente a ti es una obra colectiva en la que como autores participamos 20 profesionales, entre abogados, notarios, un juez, peritos informáticos, un desarrollador web, prestadores cualificados de servicios de confianza, prestadores de servicios de certificación y terceros de confianza. Prologa esta obra colectiva el jurista don Ángel Dolado Pérez, Juez Decano de Zaragoza, lo cual constituye un auténtico honor para nosotros.

No puedo terminar esta presentación sin antes decir que es para mí un orgullo compartir la autoría de este libro electrónico junto con excelentes profesionales y compañeros que gozan de todo mi respeto y aprecio personales.

Espero fervientemente que disfrutes este eBook.

Zaragoza, 29 de junio de 2016.

Prólogo

Ángel Dolado Pérez*
Juez Decano de Zaragoza

Que la realidad supera al Derecho Positivo, incluso a pesar de la vorágine legislativa de 2015 es un hecho incuestionable y apelamos al argot para mencionar al Derecho digital y a la prueba electrónica.

La primera idea que me sugiere esta nueva realidad jurídica es que debemos reformular el Derecho Procesal, en sus diferentes ramas civil, penal, social y contencioso-administrativa, ya que las pruebas son imprescindibles para la obtención de una resolución favorable.

En ocasiones, de poco o nada sirve que tengamos la razón con hechos y derecho, si no los probamos o si la prueba se aporta mal a la causa o se ha obtenido ilícitamente.

---

* Ángel Dolado Pérez (Soria, 1962), estudió Derecho en Zaragoza donde aprobó las oposiciones a juez, secretario judicial y fiscal, decidiéndose finalmente por la carrera judicial. Ha trabajado en Balaguer, Reus, Lérida y Zaragoza. Tras ejercer como juez de Primera Instancia durante 10 años en la capital maña, fue elegido decano. Con una intensa actividad judicial a sus espaldas, además es experto en Derecho Foral Aragonés. Ha dado clases de Derecho Procesal como Profesor Asociado de la Facultad de Derecho de Zaragoza e impartido numerosas conferencias y cursos sobre temas de derecho foral aragonés, procesal civil y derecho de consumo, así como de mediación y arbitraje. Expresidente del Foro Judicial Independiente que agrupa a 350 magistrados, ha recibido numerosos reconocimientos de diferentes instituciones de la esfera social entre las que destacamos las siguientes: la medalla al Mérito Social Penitenciario del Ministerio del Interior, la medalla al Mérito de la Policía Local de Zaragoza, Procurador de Honor del Colegio de Zaragoza y la medalla al Mérito en el Servicio de la Abogacía otorgada por el Consejo General de la Abogacía Española (CGAE) siendo el primer magistrado que la recibe en la historia de esta distinción. Ha participado en numerosas publicaciones siendo la más reciente: *La corrupción en España. Ámbitos, causas y remedios jurídicos* en la editorial Atelier.

Actualmente, en las tertulias jurídicas de jueces y magistrados lo que predomina es la duda en estos temas, no estamos seguros de casi nada. Los viejos cimientos del derecho clásico se están moviendo. Y junto a ello, está la desconfianza ante el concepto de ciberseguridad, sobre si es un mito o una realidad. Parece ser que todo es manipulable, y nos preguntamos si tendremos medios de auxilio técnico suficientes para detectar lo que es dubitable e indubitable, lícito o contaminado.

Estamos en pleno apogeo del "expediente judicial electrónico" y de la mediática frase "papel cero" en la administración de justicia, y nos preocupa que la implantación sea correcta y segura.

Los jueces debemos identificar las ventajas, riesgos e inconvenientes de las nuevas tecnologías de la información.

Estas nuevas herramientas no deben cercenar los derechos procesales de las partes y debemos velar por la protección de los derechos de los intervinientes. No queremos que la informática sea una nueva fuente del derecho por la vía de las novedades tecnológicas y que llegue a afectar a la independencia e imparcialidad judicial.

Los jueces debemos implicarnos en la evaluación de su impacto en el proceso, especialmente cuando se puede exigir que la prueba documental se tramite por medios electrónicos.

Las dificultades de funcionamiento de las TI no deben impedir el funcionamiento del sistema judicial y en caso de averías, se deben prever alternativas adecuadas para un mantenimiento integral, con el fin de evitar repercusiones negativas en el ya lento funcionamiento de la justicia.

Un principio de prudencia aconseja que las nuevas leyes que incorporan novedades electrónicas tengan periodos de vacatio legis que aseguren y certifiquen la operatividad de los sistemas informáticos para el cumplimiento de las nuevas exigencias procesales.

Especialmente relevante en esta materia son las reformas de los procesos civil y penal:

- La doctrina procesalista civil se plantea si la enumeración de LEC y CC es numerus clausus de medios de prueba o simplemente indicativa no limitativa.

Nada excluye que en los procedimientos se puedan utilizar cualquier otro medio o instrumento probatorio capaz de ofrecer al juez la percepción del objeto de la prueba, bien por intuición bien por transmisión. El tratamiento procesal en unos casos será el de la prueba documental, en otros el reconocimiento judicial y la única limitación es que no vulnere los derechos fundamentales reconocidos en la CE como se recoge en la lejana STC 114/84, de 28 de noviembre, a partir de la cual es común que no surtirán efecto las pruebas obtenidas directa o indirectamente, violentando los derechos o libertades fundamentales (art. 11.1 LOPJ)

- La reforma procesal penal de L.O. 13/2015 de 5 de octubre para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica es la que de forma sectorial regula la "prueba informática" en la instrucción penal.

El art. 588 bis contempla las disposiciones comunes y los principios rectores de la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, y la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

La premisa básica es la autorización judicial y los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida. No me cabe duda que estos preceptos y su interpretación empezarán a ser analizados por la jurisprudencia.

La era digital va avanzando en Justicia, pero para alcanzar la verdad material, en último término y en casos extraordinarios, el juez debería tener la facultad de ordenar la comparecencia de las partes, la presentación de pruebas en su formato original y la declaración de testigos en audiencia pública. Los imperativos de seguridad no deben ser un obstáculo para dichas facultades, sobre todo en procesos donde prime el principio de actuación de oficio, por los intereses públicos en juego. Lo procesal, aún en formato digital debe ser instrumental para la resolución sustantiva o de fondo.

Otra gran preocupación de jueces, fiscales, letrados de la administración de justicia y funcionarios es el derecho y también el deber de exigir y obtener una

formación inicial y continuada en materia de nuevas tecnologías para que puedan utilizarse plena y adecuadamente las ventajas de las mismas.

Los jueces mostramos nuestro apoyo en la modernización tecnológica del Derecho procesal y de la Administración de Justicia; modernización que debe conjugarse con el carácter individualizado que debe caracterizar el ejercicio de la potestad jurisdiccional (alejados de la emanación de "actos masa" propios de otros ámbito de gestión pública), en función de la dignidad que merece todo justiciable.

Por eso, se aplauden iniciativas como las de **Juristas con Futuro** porque estamos convencidos que la transformación digital requiere capital humano, jurídico, económico, informático…siendo necesario un cambio de la relación de los usuarios de Justicia con la tecnología y, cómo esto genera una transformación en el entorno corporativo, institucional, interacción entre los operadores jurídicos y los demandantes de justicia.

La gestión y procesamiento del BIG DATA, así como la protección de datos y la seguridad del sistema es el gran reto de este fenómeno imparable, sin merma de los principios esenciales de separación de poderes e independencia judicial.

Zaragoza, 15 de junio de 2016.

PARTE I:
Notarios

1

Prueba electrónica y notariado

José Carmelo Llopis Benlloch [*]

@josecarmelollb

Tras el éxito del **primer #RetoJCF** sobre testamento digital, desde **Juristas con Futuro** se plantea un segundo y apasionante tema relativo a las denominadas **evidencias digitales**. Como no podía ser de otra manera, voy a realizar mi aportación en este post, pues es una materia sobre la que ya he tratado anteriormente y que me preocupa por la relación entre el Notario y esas evidencias digitales.

Por cierto, aprovecho para apuntar que a mí nunca me ha gustado el concepto anglosajón de "evidencia" para referirnos a las pruebas que se aportan y practican en juicio, como tampoco me gustan los conceptos de "securizar", "empoderar" o "notarizar". Manías que tiene uno… Por eso, con el permiso de los organizadores, me referiré a la prueba digital.

Recapitulando (o resumiendo) antes de comenzar.

Como he dicho, ya he tratado en varias ocasiones en este blog este tema. Por ejemplo, **en este post** llegaba a la conclusión de que el hecho de crear una prueba digital es una finalidad en sí misma con independencia de que ésta haya

[*] Notario desde el año 2008, actualmente cuenta con despacho en Ayora (Valencia), perteneciente al Colegio Notarial de Valencia. Compatibiliza su actividad con el ejercicio de la mediación en el seno de la Fundación Solutio Litis del Colegio Notarial de Valencia. Publica semanalmente sobre derecho, notarios y nuevas tecnologías en su blog http://www.notariallopis.es/blog/

sido falseada, pues tanto lo analógico como lo digital es falseable, y eso no evita o frena la práctica de pruebas sobre otros soportes no digitales. Vamos, que puede falsearse una carta manuscrita y un correo electrónico, y no por eso nos cuestionamos que las cartas manuscritas sean admisibles en juicio.

También apuntaba que no se puede decidir si la práctica de una prueba digital es o no conveniente en función exclusivamente de que se vaya a presentar en juicio, puesto que no siempre todas las disputas acaban en los Tribunales, sobre todo actualmente con instituciones como la mediación. De hecho, muchas de las actas sobre temas digitales que he autorizado precisamente han evitado que las partes acudan a juicio: una precisamente, al ver el remitente de unos sms (sí, he dicho bien… sms) que el receptor los tenía protocolizados, suavizó su posición en la disputa con el receptor y todo finalizó en un acuerdo amistoso. El sujeto parecía creer que al borrarlos de su móvil, los borraba también el móvil del receptor.

Eso significa que tanto si se admiten o no en juicio como el valor que le dé el Juez pueden ser motivaciones secundarias para los requirentes, por lo que la prueba digital no debería estudiarse únicamente desde un punto de vista procesal, pues ese estudio constriñe sobremanera la actuación de los profesionales, sean o no Notarios, en el mundo digital.

Pero incluso si nos centramos en el punto de vista procesal, este **otro post** defendía que para percibir datos electrónicos, tanto los Notarios como el resto de profesionales técnicos, incluidos por ejemplo los peritos informáticos, deben confiar en aplicaciones y programas, e interpretar los datos que de ellos reciben para con ellos crear una prueba electrónica, que constituye la prueba técnica de aquello que se quiere constatar.

Planteaba por eso la conveniencia de dotarnos los Notarios de un sistema seguro para obtener la prueba electrónica, utilizando nuestra conexión reconocidamente segura, de modo que el acceso a la información se haga directamente por el Notario (y no por el usuario), y desde un equipo del Notario (y no del usuario), con el fin de eliminar suspicacias de alteración de la prueba electrónica si es el propio interesado quien la obtiene. Dicho de otro modo: que no se pueda poner en duda bajo ningún concepto que el afectado ha podido incidir en el resultado de la prueba electrónica.

De ese modo, podríamos aportar una prueba técnica revestida de fe pública. Dicha prueba, como ocurre con los documentos privados, sería alternativa y

concurrente con la pública, de modo que cualquier persona pudiera optar por la que más se adecue a sus necesidades.

Incluso si dentro del punto de vista procesal nos centramos en la valoración judicial de una prueba, el Juez probablemente vaya a valorarla en función de la confianza en el sujeto que la obtiene, en la seguridad del sistema empleado para obtenerla y en que no se altere la cadena de custodia. Y si algo genera el Notario, es confianza, pues cualquier Juez o abogado que recibe un documento notarial suele confiar en él.

¿De qué hablamos cuando hablamos de prueba electrónica?

Al hablar de prueba electrónica, en mi opinión hablamos de dos conceptos diferenciados, que suelen entremezclarse. Por una parte, la aportación de documentos públicos electrónicos como prueba en juicio y por otra parte la constatación de hechos digitales.

En relación a lo primero, simplemente apuntaré que no creo que estemos hablando de prueba digital en sentido estricto, pues comprendería todos los casos en que se aporta un documento público (expedido o intervenido por Notario u otro funcionario público), pero en vez de en formato físico, en formato electrónico. Debemos partir de la idea de que un documento electrónico con firma electrónica tiene ciertas características intrínsecas probatorias, y si esa firma electrónica pertenece a un funcionario público, su valor y eficacia probatoria será la que el ordenamiento jurídico atribuye al documento público.

Es en la segunda parte en la que me quiero detener, en la constatación documental de hechos digitales, partiendo de la idea de que cuando nos referimos a la constatación de hechos digitales, estamos refiriéndonos a todos aquellos medios de prueba en formato electrónico, de hechos, actos o situaciones que no pueden ser amparados bajo el concepto de documento electrónico con firma electrónica reconocida, pero que pueden ser opuestos a otras personas o presentados en juicio.

Nos movemos entonces en un entorno que está a caballo entre el documento privado y la prueba pericial informática, lo cual es muy importante porque el Tribunal Supremo parece exigir pruebas electrónicas periciales para aceptar como prueba las comunicaciones electrónicas. Ahora bien, en mi opinión cuando el Tribunal Supremo habla de pruebas periciales electrónicas no está

afirmando que exclusivamente puedan ser válidas en juicio las pruebas digitales que hayan sido verificadas por un perito informático, sino que intenta decir que no cualquier captura de imagen o impresión de un correo electrónico es válida en juicio si es contradicha.

Dicho de otro modo: el Tribunal, en mi opinión, está queriendo fijar para las pruebas electrónicas un mínimo de seriedad en orden a verificar el origen de la comunicación y, en su caso, la imputación del mismo a una persona. Y eso puede hacerse de muchas maneras, y no sólo con intervención de peritos.

Pero… ¿qué es la prueba pericial?

Aun así, debemos plantearnos qué es prueba pericial en materia informática. Prueba pericial es la practicada por un perito, que es aquel que, debido a sus conocimientos especializados en una materia, está en una posición adecuada para aportar conocimientos técnicos que el Juez no posee, y emitir un dictamen sobre unos hechos que permiten a éste valorar adecuadamente el objeto de la pericia.

En materia informática, parece que únicamente quienes acrediten oficialmente ser peritos informáticos deberían ser considerados como tales, pues la Ley de Enjuiciamiento Civil dice que los peritos deberán poseer el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de éste.

Entiendo que el perito debe ser una persona física con conocimientos suficientes y acreditados oficialmente, por lo que no podemos hablar de pruebas periciales fuera de las practicadas por estos. Queda claro, por esto, que el Juez no puede ni debe llamar como perito informático a quien no cumpla dichos requisitos. Los Notarios, de momento, no los cumplimos, pero tampoco creo que los cumplan las empresas que se dedican a certificar pruebas digitales por Internet.

Ahora bien, también es cierto que es pacífico el hecho de que se exige esa titulación oficial para los peritos que nombra el Juez (peritos judiciales), pero no es tan pacífico que se exija para los peritos presentados de parte, para los que dicha titulación no sería un requisito esencial, y sería el Juez el que debería valorar su seriedad, confianza y conocimientos acreditados.

Dicho de otro modo, no es lo mismo que el Juez pida un perito informático para que se le aclare que una prueba electrónica no ha sido alterada (perito judicial, que por tanto debe tener titulación oficial), que las partes decidan

apoyar sus hechos en pruebas periciales (perito de parte). En este segundo caso, podrán estar tomadas por cualquier persona que a ellos le genere confianza y que sea entendido en la materia, siendo después el Juez el que valorará la prueba electrónica aportada y, de no estar convencido, pedirá la pericial judicial.

Por tanto, todos aquellos documentos, informes, dictámenes o conclusiones sobre hechos electrónicos que no hayan sido aportados a un proceso por peritos informáticos a solicitud del Juez, deben tener la misma consideración, incluyendo tanto las pruebas digitales obtenidas por empresas dedicadas a ello como las obtenidas por ejemplo por Notario, si es que unas y otras llegan a considerarse como pruebas periciales y no como mera prueba documental.

La prueba electrónica pericial y documental.

Digo esto porque no es lo mismo la prueba pericial que la prueba documental. En la primera, no sólo se exige constatación de hechos (por ejemplo, el remitente de un correo electrónico), sino una valoración del perito o experto sobre ellos (por ejemplo sobre el haber sido alterado o no el contenido del correo electrónico después de haberlo enviado).

En la segunda, el documento recoge un hecho, sin que sea absolutamente necesaria su valoración. Y es ahí donde encontramos el hábitat natural de las actas notariales en materia electrónica, pues éstas tienen por objeto aquello que el Notario ve, oye o percibe por los sentidos. El hecho de que el Notario incorpore datos objetivos de carácter técnico obtenidos mediante el uso de aplicaciones o programas informáticos no desvirtúa, a mi entender, su naturaleza.

Debemos tener en cuenta que el artículo 199 del Reglamento Notarial, entre otras cosas, dice que el Notario redactará el concepto general en uno o varios actos, según lo que presencie o perciba por sus propios sentidos, en los detalles que interesen al requirente, si bien no podrá extenderse a hechos cuya constancia requieran conocimientos periciales.

A mi entender, este artículo lo que está negando no es la posibilidad de que el Notario constate hechos informáticos, sino a que el Notario extraiga de esos hechos informáticos conclusiones sobre materias técnicas reservadas a peritos.

Por ejemplo: El Notario puede dar fe del hecho de que en determinada URL está publicada una página web que se percibe de una determinada forma en el

navegador, con cierto código que se incorpora, que dentro de la misma hay un enlace que lleva a la visualización de un determinado archivo, que una vez descargado al ordenador del Notario resulta que tiene ciertos datos o metadatos.

Lo que en principio no puede el Notario es llegar a conclusiones más allá, si éstas requieren conocimientos periciales. Por ejemplo, el Notario no puede entrar en si esa página web ha sido alterada justo antes de la realización del acta, ni en si el código contiene algún error, si el enlace ha sufrido algún ciberataque o si el archivo descargado ha sido modificado maliciosamente. Pero el hecho de que no pueda valorar los hechos no quiere decir que no pueda constatarlos.

Lo cierto es que queda en el aire preguntarnos: ¿y si el Notario tiene conocimientos periciales en la materia? ¿no resultaría en ese caso absurda la prohibición? Dicho de otro modo: en ese caso, el Notario formalizaría el acta con los hechos y luego podría, como actividad privada extra notarial, emitir un dictamen sobre ellos.

Además del Notario, muchas empresas han visto una importante fuente de negocio en este campo, y han desarrollado aplicaciones para dejar constancia de hechos que ocurren en Internet, intentando acercar la mera prueba electrónica privada a una prueba pericial… pero no como periciales informáticas en sentido estricto.

Por lo dicho, no veo razón alguna para que las obtenidas por empresas informáticas valgan más que las obtenidas por Notario, siempre y cuando ambos sujetos obtengan de manera veraz, segura y seria la prueba electrónica pues, como decimos, en definitiva todos debemos acudir a aplicaciones, programas o instrumentos técnicos para la obtención de pruebas digitales.

De hecho, existe la norma ISO/IEC 27037:2012 que proporciona orientaciones sobre mejores prácticas en la identificación, adquisición y preservación de evidencias digitales potenciales que permitan aprovechar su valor probatorio. Las bases de la norma son las siguientes: La prueba digital debe ser adquirida del modo menos intrusivo posible, tras un proceso que sea trazable y auditable, tratando de preservar la utilidad y originalidad de la prueba. Ese proceso debe ser reproducible, comprensible y verificable, y para ello las herramientas utilizadas deben ser contrastadas. Si se cumple todo lo anterior, tanto un acta notarial como un pdf creado automáticamente por una

web tendrían la misma consideración, que no es otra que ser admisible en juicio.

Pero como en materia de prueba también entra la valoración humana del Juez, hay que plantearse también la confianza que le inspire quien ha obtenido la prueba, sea pericial o documental: obviamente, nunca será lo mismo que la obtenga el propio interesado (con una captura de pantalla, por ejemplo) que un Notario, una empresa web, que haya intervenido un tercero de confianza o un PSC.

Conclusión: Si el Notario emplea medios informáticos seguros, que estén bajo su control y de su confianza, está en una situación equiparable a cualquier otra empresa generadora de pruebas digitales en cuanto a su admisibilidad, al menos como prueba documental siendo al menos discutible que lo pueda ser como pericial. Y luego, si lo que necesita el Juez es confianza en quien obtiene la prueba, es indudable que el Notario la genera. Y mucha.

José Carmelo LLOPIS BENLLOCH

Fuente original:
http://www.notariallopis.es/blog/i/1359/73/prueba-electronica-y-notariado-reto2jcf

2

Validez y eficacia procesal de las evidencias digitales

Francisco Rosales De Salamanca Rodríguez*

@notarioalcala

¿Qué es una evidencia digital?

El tema da para mucho, y la palabra evidencia digital, es una palabra sin sentido jurídico alguno, de la que se aprovechan algunos para hacer un batiburrillo muy peligroso de cosas que nada tienen que ver.

Es muy antigua la distinción entre el hecho, el acto y el negocio jurídico, y cualquiera de ellos puede tener lugar en el mundo analógico o en el mundo digital, más sus consecuencias en un juicio no son las mismas, ni su prueba puede ser igual (o mejor dicho, la prueba es siempre la misma, pues lo que hay que probar es diferente según hablemos de la prueba de un hecho o de un negocio jurídico).

Hay retos pendientes de tratar, como son los **smart contract o la inteligencia artificial**, sin embargo creo que debemos centrar este #Retoblog en las simples evidencias digitales y lanzar nuevos retos para los otros temas.

---

* Notario desde 1997. Actualmente, en la localidad sevillana de Alcalá de Guadaíra. Se confiesa apasionado de su oficio y por las posibilidades que las nuevas tecnologías pueden aportar al mundo del Derecho. Ha sido ponente en varias conferencias y colaborador de algún libro. Ha publicado numerosos artículos, explicaciones y reflexiones, sobre todo en su blog www.notariofranciscorosales.com , donde publica frecuentemente desde octubre de 2013.

¿Cuál es la diferencia entre el hecho jurídico, el acto jurídico y el negocio jurídico?

Creo conveniente que más que hablar de derecho digital, empecemos hablando de la teoría general del derecho y refresquemos algunos conceptos:

· Un hecho, es un suceso o acontecimiento; hay hechos que producen consecuencias jurídicas (muchos más de los que os imagináis) cuando ese acontecimiento produce consecuencias jurídicas, hablamos de un hecho jurídico.

· Cuando una voluntad humana, consciente y exteriorizada, realiza un hecho, hablamos de un acto jurídico; también es acto jurídico todo hecho jurídico que afecte al hombre independientemente de su voluntad (los casos más claros son el nacimiento y la defunción).

El negocio jurídico es la declaración o declaraciones de voluntad privada encaminadas a conseguir un fin práctico jurídico, a las que el ordenamiento jurídico, por sí solas o en unión de otros requisitos, reconoce como base para producir determinados efectos jurídicos.

Deliberadamente he querido seguir esta distinción clásica que ya formuló De Castro, y a ella obedecerá este post; no obstante me cuestiono seriamente si en realidad es el acto un hecho, y el hecho un acto, así como si verdaderamente hay diferencia entre el acto y el negocio (más todas estas reflexiones más que un post requerirían todo un tratado de la teoría general del derecho, y carezco de cualificación para hacerlo).

¿Cabe la prueba digital de hechos jurídicos?

No me cabe duda alguna que en el mundo digital o tecnológico, hay muchísimos hechos, que todos ellos son hechos jurídicos y todos ellos pueden probarse.

Sin embargo la prueba de los hechos jurídicos digitales, es una prueba que tiene peculiaridades frente a la prueba de los que podríamos hablar hechos jurídicos tradicionales (luego hablaremos de la adulteración).

El número de hechos jurídicos digitales es muy superior al número de hechos jurídicos tradicionales y es más difícil de apreciar

La cantidad de operaciones y velocidad con la que computan los ordenadores, es incomparable con la que tiene el ser humano, por lo que en teoría es imposible controlar todos los hechos jurídicos digitales.

Pensad que en el fondo los ordenadores sólo entienden de combinaciones de ceros y de unos, así que calculad ¿cuantos ceros y cuantos unos hay en este post en el que sólo vais letras? prueba de ello es el trabajo que a todos nos supone entender los **conceptos de byte, kilobyte, megabyte etc**.

¿Seguro? ¿No os dais cuenta de vuestro error?

Lo único que sucede es que por primera vez en la historia el hombre tiene control del proceso desde el principio hasta el fin, los ordenadores los creamos nosotros y hacen lo que nosotros decimos; a diferencia de un hecho como la lluvia es algo que ni siquiera entendemos completamente, y que desde luego no funciona con el botón de encendido y apagado como un ordenador.

¿Si reclamáis en juicio los daños de una inundación pediríais que un meteorólogo explique cómo funcionan las bajas presiones?

Nadie discute en juicio por qué llueve, sino simplemente se trata de constatar si ha llovido y posibles consecuencias jurídicas de esa lluvia; de igual manera si accedemos a internet desde una IP basta con localizar dicha IP, y ubicarla (pues aquí hablamos de un hecho jurídico).

El problema que hay, y respecto al que no tengo una respuesta clara, es que los ordenadores no se encienden ni apagan solos, pensaréis en los sistemas de encendido y apagado automático, pero en el fondo son fruto de una programación humana, por lo que se plantea el problema de determinar cuando el acto realizado por un ordenador es acto, y cuando hecho jurídico.

En principio entiendo que sólo hay hecho jurídico digital cuando hay una voluntad humana, consciente y libre, y no en actos automáticos que realizan los ordenadores de modo completamente ajeno incluso al conocimiento de su usuario (por ejemplo la cantidad de conexiones y protocolos que realiza para conectarse a Internet).

Problemas que plantean los hechos jurídicos digitales

1.- La complejidad de la nueva terminología.

Ello obliga a un esfuerzo de estudio por parte de juristas.

Intentar hablar de evidencias digitales en un juicio, y tratar de que jueces, fiscales o abogados hablen de metadatos como quien habla de fútbol es: no solo imposible, sino incluso absurdo, pues un jurista es un jurista y un técnico es un técnico.

No obstante jamás hay un litigio sobre hechos jurídicos, sino sobre actos y negocios jurídicos; y creo que es importante tener en cuenta que los primeros más que demostrarse se aportan a juicio, mientras que los segundos, si son el objeto de un litigio y lo que ha de probarse.

Sólo os dejo una reflexión, y es que tampoco los juristas entienden de medicina, y sin embargo nada impide que haya litigios en los que se hable de medicina (desde responsabilidades médicas, hasta explicar daños sufridos por una persona -por poner el caso de la Talidomida, en juicio lo que se debate no es qué es la talidomida, sino si es dañosa y las responsabilidades que tiene la empresa que la fabricaba, e incluso sus **implicaciones éticas**).

2.- Lo engañoso de los datos.

Es cierto que cada vez más los juristas empiezan a hablar con naturalidad de palabras tecnológicas. Sin embargo no hay nada peor que un "enterao", y basta con acudir a cualquier hospital o farmacia para constatarlo.

Un ejemplo es la IP (que antes pusimos) se trata de una palabra que muchos han sido y pocos entienden, pero que sobre todo y como demuestra **Ruth Sala Ordóñez**, ese dato necesariamente no sirve para localizar un ordenador, y desde luego muchísimo menos para localizar a autor de un hecho.

¿Sirve de algo localizar a un ordenador? ¿La localización del ordenador es objeto de un litigio?, huelga decir que la respuesta es negativa, pues por ahora (…ya veremos con la inteligencia artificial) los ordenadores no son sujetos de derecho.

Hago esta reflexión porque es irrelevante donde está un ordenador, lo verdaderamente importante es quién está usando ese ordenador, y por tanto la IP o cualquier otra evidencia digital (usemos la terminología del #Retoblog) es un mero dato de otros muchos que sirven para convencer al juez.

Es perfectamente posible, y muchísimo más habitual de lo que parece, que a una misma IP se le conecten varios ordenadores (basta con que haya una red sea doméstica o profesional) es también posible que se esté usando una IP ajena (desde el caso de wifi pública, **hasta los que le "chupan" internet al**

vecino) y finalmente se más que posible que tu ordenador sea lo que se conoce como zombi, y esté siendo manipulado por un virus.

Reglas a tener en cuenta en la prueba de evidencias digitales que sean meros hecho jurídicos

1.- La prueba de una evidencia digital concreta, consistente en un hecho jurídico rarísimas veces es importante

Tanto en el mundo analógico como en el digital, **la valoración de la prueba ha de ser general y en su conjunto, y nunca prevalece un medio de prueba frente a otro** (y os lo dice un Notario que autoriza una de las pruebas más solventes del ordenamiento, como es la escritura; más por mucha escritura que haya, y por mucho que se haya confesado el cobro del precio, no es el primer caso de donación simulada bajo la forma de compraventa, que ha sido impugnado ante los tribunales).

2.- La evidencias digitales consistentes en un hecho jurídico se aportan pero no se prueban.

No veo correcto hablar de prueba de la prueba (al menos como norma general) por ello creo que los hechos jurídicos digitales, no se prueban, sino que se aportan al juicio, con el objeto de probar los actos y negocios digitales.

Como bien aclara Ruth Salas Ordóñez, es el Juez el que acepta o no la prueba aportada y la considera o no pertinente; es más (como veremos) quién impugne los hechos aportados, ha de demostrarlo (y pagar las consecuencias si no lo hace -pues las costas están ahí-).

3.- Es importante garantizar la fiabilidad de los hechos digitales aportados como prueba.

Todo hecho que se aporta a juicio puede ser contradicho, y por tanto es necesario garantizar su conservación para que pueda ser contrastado por un tercero (imaginad simplemente las películas, y como se conservan las pruebas de los delitos).

A tal efecto es necesario tener en cuenta la norma **ISO/IEC 27037:2012** que regula el tema a nivel internacional, si bien debemos de tener en cuenta que son meros estándares internacionales de calidad, comúnmente aceptados, pero que ni tienen el valor de tratado internacional ni de norma jurídica,.

Ello supone que estos estándares de calidad, ni tienen que ser conocidos y aplicados por el juez de oficio, ni le vinculan (lo cual no quiere decir que no deban de ser tenidos en cuenta, y que de no respetarse sea más fácil impugnar la veracidad de los hechos aportados al juicio).

4.- De los hechos jurídicos digitales, se derivan actos y negocios jurídicos.

Los hechos jurídicos, unidos a la voluntad humana, es la base de todo acto o negocio jurídico; y son dichos actos y negocios los que hay que probar.

Conforme al **artículo 217 de la LEC**, resulta razonable afirmar que: una vez es aportada la prueba, aquél que la impugne debe de especificar los motivos de su impugnación, y demostrarlo; regla que se refuerza en el **artículo 326.2** (pues normalmente lo que se aportan son documentos privados -por más que muchos se emperren en revestirlos de pseudo oficialidad y los llamen certificados-).

En el mundo digital se reafirma lo que acabo de decir, pues cuando hablamos de firma electrónica, el **artículo 3.8 de la ley de firma electrónica** (Ley 59/2003 de 19 de Diciembre, vigente hasta el 2 de Octubre de 2016, que es cuando entra en vigor el **reglamento eIDAS 910/2014**) admite la validez del documento firmado electrónicamente como prueba, y en caso de impugnación obliga a su cotejo, más de resultar correcto el cotejo, impone las costas y gastos a quien impugnó (eso si, ambas normas sólo entienden que la firma electrónica acredita la identidad del firmante: sin embargo, ni afirman su capacidad, ni la validez legal del documento firmado -en definitiva, para nada valoran el negocio jurídico-).

¿Cabe la manipulación de los actos jurídicos digitales?

Ya hablando en este blog de **Bitcoin** expliqué que absolutamente todo es manipulable y puede falsificarse. Bastaba darse un paseo por cualquier mercadillo para comprobar la barbaridad de "Chemilacó" falsos que hay (por no hablar que todos sabemos lo que es entregar en un supermercado un billete -incluso de 20- y que te lo pasen por la maquinita que detecta billetes falsos).

Basta con buscar en Youtube un poco para descubrir como alterar cualquier dato digital, el hecho es tan evidente que el propio **Tribunal Supremo en sentencia de 19 de Mayo de 2015** expresamente se plantea el tema, más si

leéis el post que os enlazo, la argumentación jurídica digital es más que deficiente cuando afirma:

Y es que la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido

Es evidente que en este caso no hablamos de actos, sino de hechos jurídicos, más el problema de la manipulación viene al caso.

Si nos damos cuenta, lo que verdaderamente critica el Tribunal Supremo es lo que comúnmente se llama "pantallazo", y es lógico, pues a nadie se le ocurriría aportar una prueba tan cutre como esa (de hecho lo absurdo de la sentencia es que no fue aportada dicha prueba, para cuya obtención si hubo garantías, y que además venía corroborada por otras pruebas, sino que simplemente el "pantallazo" se aportó para que pudiera el tribunal visualizar los hechos. Por ello la impugnación de la prueba realizada no puede ser calificada sin faltar seriamente el respeto al letrado que la realizó).

Hay que tener presente que la manipulación de un hecho jurídico digital es una alteración fruto de la voluntad humana, y que dicha alteración es un hecho jurídico, pero que es delito (art 393 del Código Penal) sin embargo también lo es cualquier otra manipulación de una prueba analógica.

En todo caso, creo que puedo afirmar que: cuento por cientos los documentos privados falsos que he visto a lo largo de mi carrera profesional, por no decir que también he visto escrituras falsificadas (de hecho he tenido que levantar actas de cotejo de una copia con el original); pues todo puede falsificarse.

Problemas de la prueba digital del acto jurídico y del negocio jurídico

Si hablar del hecho jurídico digital es fácil, otra cosa son los actos y los negocios jurídicos digitales (que a mi juicio merecen un #Retoblog propio).

En los ordenadores siempre hay una voluntad humana que interviene en mayor o menor medida, por lo que son muchos los actos y negocios jurídicos existen en el mundo digital.

Es aquí cuando se plantea el problema de la teoría general del consentimiento y resolver los problemas que plantea el consentimiento digital, así como sus consecuencias (sería necesario un nuevo #Retoblog para hablar de los actos que pueden realizar de modo automático los ordenadores y robots, y especialmente las responsabilidades derivadas del mal funcionamiento o programación).

¿Quién ha dicho esto?

La **firma electrónica** resuelve en gran medida el problema, y lo cierto es que pocos conocen que absolutamente todo acto digital deja rastro o huella, por lo que siempre es firmado digitalmente.

Otra cosa es que el tipo de firma digital sea más o menos de calidad; de hecho, las firmas digitales que se usan habitualmente son de tan bajo nivel de calidad, que el primer problema que se plantea es probar la autoría del hecho o negocio digital.

He hablado de la identidad digital en diversas ocasiones, pero la realidad actual es tan variopinto que sólo pondré ejemplos muy habituales:

Es posible que tu ordenador haya sido infectado por un virus y esté actuando como robot (**si quieres saber si te ocurre puedes pinchar en este enlace del INCIBE**) en este caso aparentemente es tu ordenador el que actúa y tú el que lo ordenas, sin embargo es obvio que así no sucede.

1. Puedes tener la "feliz" idea de ingresar en una red social con e-mail ad hoc y con nombre de usuario y contraseña ficticio (yo por ejemplo tengo varias cuentas en las que me llamo Rodrigo Díaz de Vivar y con nombres absurdos) sin embargo es obvio que soy yo quien de forma anónima actúo a través de mis dispositivos y que puedo ser localizado.

2. Los hay que ponen su identidad real en Redes Sociales (por ejemplo yo en twitter soy @notarioalcala y en mi perfil pongo mi nombre y dirección) tratar en estos casos de negar mi identidad es absurdo; y sin embargo ¿cuantas cuentas falsas hay suplantando, algunas con una fina ironía una identidad real? os pongo por significativas las cuentas de @norcoreano o de @fijarzebien.

Finalmente merecería otro #Retoblog la personificación de las cosas, y el reto que plantean, entre otras, las notificaciones y comunicaciones digitales, pues la tendencia a entender que por enviar un e mail, un sms, o un WhatsApp a alguien este ha sido notificado da para mucho, pues es más que frecuente que se ofrezcan servicios por llamados **terceros de confianza**, cuando este tercero de confianza, ni acredita la notificación ni tiene el consentimiento legal del notificado que exige el art 25 de la ley 34/2002 (prefiero omitir mi valoración sobre algunos notarios que se ofrecen a facilitar acta de estas notificaciones, creando una auténtica confusión de la que algunos se aprovechan ante el desconocimiento que muchos juristas tienen sobre derecho digital).

¿Puede decirlo?

Llegamos al punto más importante y al reto que plantean los actos y negocios digitales, que es la capacidad del autor de dicho acto o negocio.

Hemos citado la firma electrónica como medio de identificación, y no puede cuestionarse el documento firmado electrónicamente, pero de decir que sabes quién ha dicho o hecho algo, a afirmar que puede decirlo o hacerlo media un universo.

Ladinamente algunos afirman que el mero hecho de usar la firma electrónica implica capacidad, pero nuevamente confunden los conceptos, pues el uso de una firma electrónica supone una habilidad, no una capacidad (por no decir que algunas firmas electrónicas tienen tal grado de sencillez, que hasta la habilidad es cuestionable).

El ejemplo más sencillo lo podemos poner imaginando a alguien mayor de edad, que firma un documento borracho; absolutamente nadie puede negar que ese documento es nulo (creed que no es la primera vez que expulso de mi Notaría a alguien que trata de firmar borracho).

El error, la violencia, la intimidación o el dolo, son vicios del consentimiento que existen y deben de ser tenidos en cuenta, y la tecnología actual no da soluciones a estos problemas (basta recordar temas de actualidad como son: las

participaciones preferentes, o las cláusulas suelo para entender de lo que estoy hablando).

La limitación de un post impide entrar en los cientos de problemas y retos que este tema plantea en el mundo digital, si bien quiero centrarme especialmente en uno, y es fruto del automatismo que el mundo digital plantea en el ser humano.

Hay una tendencia a creer que la aceptación de las condiciones generales de un contrato supone la validez de dicho contrato, lo cual en Internet plantea dos problemas importantes:

1. ¿Es consentimiento la aceptación que de forma automática todos hacemos de los términos y condiciones que se nos piden antes de instalar una aplicación y que absolutamente nadie lee?, sinceramente me parece insuficiente la ley de condiciones generales de contratación o la ley de defensa de consumidores y usuarios, pues lo cierto es que más que una voluntad humana, estamos ante comportamientos automáticos.

El que en una web haya repartidas por numerosas páginas una información exhaustiva ¿implica que toda esa información es conocida y aceptada?

Cuando menos entiendo que el usuario de internet, frente al que presta el servicio digital, es un consumidor, por lo que tiene toda la protección que le da la ley de defensa de consumidores y usuarios, y no conviene olvidar un viejo latinajo que es la "**exceptio shcaedula non lecta**" que implica la posibilidad de impugnar cualquier contrato que se ha firmado sin leer.

¿Qué ha dicho?

Es muy importante distinguir lo que es la firma electrónica de una comunicación, de la firma electrónica del contenido de la documentación (esto segundo es el time stamp) pues no es lo mismo que se firme un mensaje, que el que se firme el contenido del mensaje enviado.

No sólo hay que comprobar la identidad del autor, hay que comprobar la autenticidad del mensaje, pues este puede ser manipulable, por lo que es importante no sólo que las comunicaciones digitales tengan lugar usando firma electrónica (cosa que siempre sucede) sino que la propia comunicación sea firmada electrónicamente (cosa que raras veces sucede).

¿Implica un registro electrónico prueba del acto y el negocio jurídico digital?

Brevemente (pues el post está superando con creces los límites del #Retoblog) dejo apuntada la tendencia a hablar de blockchain como alternativa al Notariado, y la confusión existente entre el Notariado latino y el Notariado anglosajón sobre lo que ha escrito mi compañero **Javier González Granado**.

Blochain simplemente es un registro seguro de cualquier hecho digital, más no acredita ni quién ha realizado algo (pues las identificación de las partes es anónima, y todo lo más habrá un tercero que identifique), y muchísimo menos ni la capacidad de las partes, ni la legalidad del acto realizado, ni tiene las ventajas procesales de una escritura pública (por ejemplo el carácter ejecutivo del **artículo 517 párrafos 4 y 5 LEC**).

Desde aquí prometo explicar más ampliamente este tema (anticipo que tengo todos los post ya programados hasta septiembre).

¿Puede un Notario dejar constancia en acta de evidencias digitales?

Creo que es importantísima la diferencia que hay entre el hecho y el negocio jurídico, pues mientras que los hechos son objeto de acta notarial, los negocios son objeto de escritura pública (**artículo 17 de la Ley Notarial**).

Actas Notariales de hechos digitales

Está claro que los hechos digitales pueden reflejarse en acta notarial, pues el artículo 17 de la Ley Notarial:

Las actas notariales tienen como contenido la constatación de hechos o la percepción que de los mismos tenga el Notario, siempre que por su índole no puedan calificarse de actos y contratos, así como sus juicios o calificaciones.

En materia de actas notariales son de aplicación los **artículos 198 y siguientes del Reglamento Notarial**, de los que vamos a centrarnos en algunos.

Art 198.2 del Reglamento Notarial, relativo al acta de archivos informáticos

Cuando un notario sea requerido para dejar constancia de cualquier hecho relacionado con un archivo informático, no será necesaria la transcripción del contenido de éste en soporte papel, bastando con que en el acta se indique el nombre del archivo y la identificación del mismo con arreglo a las normas técnicas dictadas por el Ministerio de Justicia. Las copias que se expidan del acta deberán reproducir únicamente la parte escrita de la matriz, adjuntándose una copia en soporte informático no alterable según los medios tecnológicos adecuados del

archivo relacionado. La Dirección General de los Registros y del Notariado, de conformidad con el artículo 113.2 de la Ley 24/2001, de 27 de diciembre, determinará los soportes en que deba realizarse el almacenamiento, y la periodicidad con la que su contenido debe ser trasladado a un soporte nuevo, tecnológicamente adecuado, que garantice en todo momento su conservación y lectura.

Sólo aprovecho para denunciar públicamente que, igual que en otros temas, y casi quince años después la DGRN no ha determinado absolutamente nada, ni hay normas técnicas del Ministerio de Justicia, siendo que cada vez son más las necesidades digitales de los ciudadanos y no estoy muy conforme con las soluciones que para el tema se ofrecen desde la Agencia Notarial de Certificación.

Artículo 199.2 impidiendo que el Notario de fe de hechos que requieran conocimiento periciales

El notario redactará el concepto general en uno o varios actos, según lo que presencie o perciba por sus propios sentidos, en los detalles que interesen al requirente, si bien no podrá extenderse a hechos cuya constancia requieran conocimientos periciales.

Coincido con mi compañero **José Carmelo Llopis Benlloch**, en que este artículo no impide dejar constancia en acta notarial de hechos digitales, sino que simplemente impide al Notario emitir juicios de valor que requieran conocimientos periciales, y que una cosa es que el Notario valore hechos (por ejemplo una alteración) y otra es que no pueda constatar cualquier hecho.

El fenómeno digital ha provocado además que haya empresas que han creado aplicaciones para dejar constancia de hechos que ocurren en Internet, más son meras aplicaciones informáticas, que puede usar cualquiera (incluso el juez) y no son pruebas periciales.

Especial importancia tiene en este punto las empresas que se presentan como **terceros de confianza**, sobre las que he escrito en este post, y que ni son Notarios, ni Prestadores de Servicios de Certificación, ni Peritos, ni en la mayoría de los casos prestan servicios que competen a lo que legalmente es un tercero de confianza (en este punto con la connivencia de algunos compañeros míos, que incomprensiblemente no entiendo por qué no es atajada por los órganos directivos del Notariado).

Artículo 207 que regula el acta de exhibición de cosas

En las actas de exhibición de cosas, el Notario describirá o relacionará las circunstancias que las identifiquen, diferenciando lo que resulte de su percepción de lo que manifiesten peritos u otras personas presentes en el acto, y podrá completar la descripción mediante planos, diseños, certificaciones, fotografías o fotocopias que incorporará a la matriz. En las actas de exhibición de documentos, además, transcribirá o relacionará aquéllos o concretará su narración a determinados extremos de los mismos, indicados por el requirente, observando en este caso, si a su parecer procede, lo dispuesto en el párrafo último del artículo 237.

Escrituras públicas de actos y negocios digitales

A diferencia del hecho digital, que es puede ser objeto de acta: los actos y negocios digitales son objeto de escritura pública, pues el artículo 17 de la Ley Notarial:

Las escrituras públicas tienen como contenido propio las declaraciones de voluntad, los actos jurídicos que impliquen prestación de consentimiento, los contratos y los negocios jurídicos de todas clases.

Al existir declaraciones de voluntad, el problema fundamental que plantea el mundo digital, y el verdadero reto que tiene el notariado es la constatación de quién dice algo, si esa persona puede decirlo, si tiene capacidad para hacerlo, y qué es lo que dice; por no hablar de si es o no posible una escritura pública completamente digital.

Vaya por delante que no cabe negar que los actos y negocios digitales existen, y si algo necesitan es de seguridad, por lo que entiendo que no estamos ante un reto para los notarios; sino una auténtica necesidad de la sociedad, a la que el notariado ha de dar respuesta.

Lo cierto es que: ni el estado de la técnica, ni la legislación, permiten encontrar soluciones satisfactorias, no obstante creo que esto es materia de otro #Retoblog.

¿Tiene algo que aportar el Notariado en estos temas?

La respuesta es afirmativa, y prueba de ello es lo que he escrito sobre el contrato de **escrow** en este mismo blog, o el post que tengo en elaboración sobre el crowdfunding, por no hablar de servicios de hosting, time stamp, firma electrónica, cloud computing, o conexiones directas con fiscalía (igual que las hay con el órgano centralizado de prevención del blanqueo de capitales)

respecto de las actas en las que constaten posibles delitos cometidos en redes sociales.

Sin embargo y por enésima vez creo que estamos ante un nuevo #Retoblog.

Francisco ROSALES DE SALAMANCA RODRÍGUEZ

Fuente original:
http://www.notariofranciscorosales.com/validez-y-eficacia-procesal-de-las-evidencias-digitales/

PARTE II:
Abogados

3

La alegalidad o limbo legal de la prueba electrónica

Sergio Carrasco Mayans[*]

@sergiocm

Cuando se habla de tecnologías que revisten una apariencia de novedad, resulta sencillo encontrar referencias a la *alegalidad* de su actividad, al *limbo jurídico* que en teoría rodea todo su funcionamiento. Este problema se agrava cuando los juristas empiezan a utilizar este concepto para analizar la posible validez de una prueba que requiere obtener información de una de estas tecnologías para presentarla ante el Juez, cuando en realidad no existe una problemática tan acusada como la que se quiere dar a entender.

El debate se ha centrado por parte de un sector, excesiva y erróneamente a mi parecer, en la herramienta concreta utilizada en un determinado caso para hablar de su admisibilidad como prueba. Sin perjuicio de determinados aspectos concretos que podamos encontrar en una aplicación, la realidad es que al final lo importante es la información en sí con la que trabajamos, así como las dificultades propias a la hora de trabajar con pruebas en soporte electrónico, y no tanto en qué servicio nos encontramos.

No, la Ley no nos deja desamparados y ante una laguna al producirse una vulneración de derechos a través de WhatsApp, Tinder, HushHush o cualquier

[*] Ingeniero de Telecomunicaciones, Informático, Politólogo y Licenciado en Derecho por la Universitat Oberta de Catalunya, especializado en Derecho de las Nuevas Tecnologías y en Derecho Público. Cofundador de Derecho en Red y consultor en Fase Consulting.

otra nueva app que aparezca en el futuro. No hay tal vacío legal hasta que el Supremo se pronuncia sobre los requisitos para su admisión y valoración. No existe un paraíso en que los infractores puedan utilizar las nuevas aplicaciones mientras el legislador responde.

Los medios son dados a grandes titulares al respecto, dando a entender que a partir de un momento concreto serán admisibles como prueba, o que se han establecido requisitos muy concretos para su admisión, pero la realidad es que en la mayoría de ocasiones no hay ninguna novedad real en lo sucedido, y los conceptos básicos nos acompañan en todos ellos.

¿Puede el abogado desconocer la importancia de preservar adecuadamente la prueba electrónica y cómo hacerlo?

La respuesta a esta pregunta es obvia. No, **el abogado debe dar la importancia que corresponde a la formación en las diversas pruebas electrónicas** ante las que pueda encontrarse en un proceso, cómo se han presentado y su naturaleza, y todo ello porque cada vez resulta menos extraño que se aporten en procedimientos judiciales este tipo de pruebas. Es importante analizar si son relevantes y han sido obtenidas de forma lícita, sin perjuicio del valor probatorio que pueda otorgarles el juez, pero debe irse más allá.

A mi juicio, la **naturaleza jurídica** a efectos probatorios de toda esta información encuentra su encaje claro en la definición de **documento electrónico** existente en el art. 3.5 de la Ley 59/2003, de 19 de diciembre, de firma electrónica:

Se considera ***documento electrónico*** *la información* ***de cualquier naturaleza en forma electrónica****, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.*

Tanto las imágenes, como textos, bases de datos en sí, y otros archivos presentados revestirán la condición de documento electrónico, y el abogado

encargado del caso deberá tener en cuenta las previsiones existentes al respecto para la fuerza probatoria de los mismos.

Es un error por desgracia más común de lo que debería el admitir la prueba presentada por la parte contraria, entrando entonces en juego dependiendo del caso el art. 326.1 de la Ley de Enjuiciamiento Civil.

Los documentos privados harán ***prueba plena*** *en el proceso, en los términos del artículo 319,* ***cuando su autenticidad no sea impugnada*** *por la parte a quien perjudiquen.*

Está claro que los abogados no pueden conocer las características particulares de toda herramienta tecnológica, y por ello existe la figura del perito , pero sí que (como mínimo) **debe tenerse claro que estos documentos son susceptibles de alteraciones** que, de demostrarse su posibilidad, podrían reducir de forma importante la valoración que de los mismos hará el órgano judicial. También debe conocerse **el concepto de firma digital**, y cómo puede permitirnos detectar cambios en los documentos con los que debamos trabajar.

Los datos almacenados en sistemas informáticos pueden ser en ocasiones modificados sin que quede ninguna huella al respecto, y nos encontramos con que los documentos electrónicos son en ocasiones generados utilizando la información existente en equipos bajo el completo control de la parte que va a aportarlos. Es por ello que debemos tener claro qué tipo de información buscar por resultar la relevante para el caso, y si existe algún mecanismo que nos permita asegurar ante el Juez que dichos datos son reales y no han sido modificados.

No hay que mitificar las aplicaciones

A la hora de enfrentarse a una prueba en documento electrónico **no debemos centrarnos exclusivamente en la naturaleza y/o novedad de la aplicación de que se trate, sino en la información con la que trabaja** y los posibles mecanismos de firma electrónica de la misma que pueda haber implementado para evitar su alteración o que pueda permitirnos probar su origen.

Con la proliferación de apps en terminales móviles, cada día nos encontramos con nuevas aplicaciones cuyo uso en procesos judiciales es posible que no se haya producido hasta la fecha, pero eso no supone un impedimento para extraer los datos que nos interesen y que un perito analice las garantías teóricas de los mismos.

La experiencia e interfaz de usuario pueden ser muy distintos entre sí, pero detrás de esto lo que tenemos en todos estos casos es información en bruto, bases de datos, imágenes, que podrán ser extraídos y preservados para garantizar posteriormente la cadena de custodia, así como la originalidad e integridad de la prueba de que se trate.

La pregunta inicial que debemos hacernos es "¿**Con qué datos trabaja esta aplicación**?". Viendo la lista de permisos podemos encontrar como mínimo parte de ellos: geolocalización, imágenes, conversaciones con nuestros contactos. Accediendo posteriormente al dispositivo podremos extraer dicha información con mayores o menores garantías, y sin que la denominación concreta de la aplicación sea determinante.

Condenas por el "estado de WhatsApp", por enviar mensajes en Facebook pese a existir una orden de alejamiento, por realizar tuits delictivos. En realidad nos encontramos con un cambio del canal utilizado, pero la información determinante de si se ha producido una infracción del ordenamiento jurídico es en sí la misma.

Si nos limitamos a obtener una captura de pantalla de una determinada aplicación, lo que obtenemos es únicamente aquello que el desarrollador ha decidido exteriorizar. Elementos que adoptan una forma más visual y comprensible para el usuario, pero que en realidad no es la totalidad de lo que se encuentra almacenado en el soporte electrónico de que se trate. Que reflejemos únicamente lo anterior en un documento electrónico, ya sea público o privado, va a suponer la **pérdida de importante información que potencialmente supondrá la merma de valor probatorio** ante la impugnación de la otra parte.

En la práctica podemos observar que una gran parte del sector aporta tanto la prueba impresa o transcrita como el documento electrónico, pero el principal problema aparece cuando convertimos esta prueba originalmente en soporte electrónico a copia impresa y únicamente facilitamos esta última.

La conversión del formato de la prueba

Un acto en apariencia tan inocente como la impresión de una imagen, un correo, o mensajes enviados por WhatsApp, para su posterior aportación al proceso judicial de manera simple en realidad suponen la omisión de importantes datos de los que puede depender la valoración que finalmente se haga de los mismos.

Además, no está quedando constancia de la integridad de los medios en que se almacenaba originalmente la información, y en particular su preservación a los efectos de posteriores comprobaciones e informes.

¿Es admisible su transcripción y presentación en papel? Sí, la norma no pone impedimentos para ello, pero a mi juicio su uso debe limitarse al de facilitar su lectura y valoración, pero siendo acompañado en todo caso por el documento electrónico correspondiente.

En el caso de documentos electrónicos contamos con herramientas que nos van a permitir crear la huella digital del mismo o hash, una cadena alfanumérica hexadecimal generada a partir de la aplicación de un algoritmo que debe identificar de manera inequívoca dicho documento, de tal manera que el menor cambio realizado sobre el mismo sería rápidamente detectado (aunque respecto a este último factor es importante ver si el algoritmo concreto utilizado para su generación es realmente adecuado). Esto además nos permitirá realizar duplicados de dichos documentos y probar que se corresponden plenamente con el original.

El problema surge de nuevo cuando las herramientas propias de la Administración Judicial Electrónica imponen el uso de determinados formatos y limitaciones de tamaño a la hora de aportar a través de los mismos documentos electrónicos.

Un cambio como la mera conversión de una imagen a otro formato que ocupe menos o simplemente a uno de los admitidos por el sistema (aunque en la práctica únicamente se compruebe en realidad la extensión), o la reducción de la misma, supone una alteración del documento que puede suponer dificultades posteriores si no aportamos asimismo el documento electrónico original. Obtenemos en realidad un nuevo documento, identificado por un hash distinto, y que puede haber perdido por el camino multitud de información que nos podría haber resultado útil.

Por si no fuera poco, se subestima de manera peligrosa la importancia de aquellos datos *no visuales*, con los que los equipos trabajan pese a no mostrarlos al usuario.

La importancia de lo *invisible*

Si hasta el momento hemos mencionado la facilidad de alteración de la prueba electrónica, no podemos olvidar que muchas veces nos olvidamos de la existencia de multitud de información asociada con nuestros documentos electrónicos, que se pierden en la impresión, y que pueden ayudarnos a la hora de conseguir una valoración adecuada de la prueba presentada.

Antes de eso debemos tener en cuenta lo siguiente

· No podemos negar categóricamente que no va a poderse probar la integridad de un documento electrónico concreto, como es el caso de un correo electrónico

La evolución en el estado de la técnica puede finalmente revelar que lo que se pensaba que podía probarse respecto de un documento era en realidad fácilmente modificable

Centrándonos en el caso de un correo electrónico, la realidad es que estos no son más que archivos en texto almacenados bien en nuestro servidor de

correo, bien en nuestro equipo, y a los que accedemos a través del cliente de correo que escojamos.

Que sean documentos de texto plano supone que (al menos en apariencia) podemos proceder a su modificación no detectable sin mayores dificultades que encontrar su localización y tener permisos para su edición a través de nuestro editor de textos favorito. Y, efectivamente, podemos realizar cambios en cualquiera de los datos que muestra nuestro cliente de correo: podemos cambiar el asunto, el cuerpo del mensaje, o incluso la documentación adjunta, y ante los ojos de alguien que visualice dicho correo electrónico revestirá la apariencia de ser el mensaje que se ha recibido inicialmente. Es aquí donde entra la importancia de la *información invisible*.

Pongamos el ejemplo de un correo electrónico básico, y la información que se nos muestra

En este correo electrónico de prueba nos encontramos con 89 caracteres (incluyendo espacios), donde se me informa del remitente, el destinatario, el asunto del correo electrónico, y la fecha en la cual he recibido dicho mensaje. Si se certificara exclusivamente lo que se puede ver en este caso, la modificación resultaría sencilla para cualquier usuario, sin necesidad de contar ni tan siquiera con herramientas específicas, y pudiendo obtener una prueba que (de no ser impugnada) podría gozar de un importante valor probatorio.

Podría discutirse que, dejando de lado las posibles modificaciones, muchas veces la infracción ya puede apreciarse con el mero acceso al correo electrónico, como parte del cuerpo del mensaje, con lo cual ya no resulta necesario acudir a más datos para probar la misma. El problema es que ese argumento no cuenta con la fuerza suficiente, dado que estamos eliminando gran parte de la información que nos podría permitir probar el origen y contenido del correo electrónico concreto. Es por ello que toda prueba debe consistir en el volcado completo de la información que constituye dicho mensaje.

Si pasamos ahora a analizar el contenido completo del correo electrónico que hemos recibido podemos observar lo siguiente:

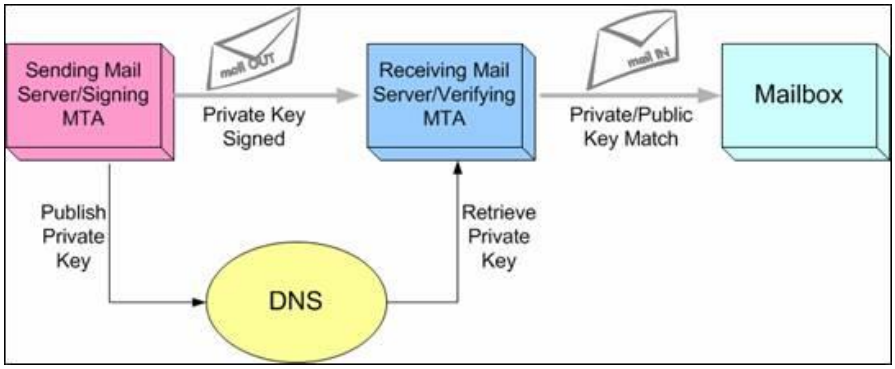
```
Delivered-To: d.sergiocm@gmail.com
Received: by 10.[redacted] with SMTP id ao2csp1535018lbc;
        Mon, 11 Apr 2016 10:31:37 -0700 (PDT)
X-Received: by 10.28.30.79 with SMTP id e76mr20869055wme.27.1460395897828;
        Mon, 11 Apr 2016 10:31:37 -0700 (PDT)
Return-Path: <sergioc@derechonntt.com>
Received: from [redacted]
        by mx.google.com with ESMTP id v124si9484889wmg.0.2016.04.11.10.31.37
        for <d.sergiocm@gmail.com>;
        Mon, 11 Apr 2016 10:31:37 -0700 (PDT)
Received-SPF: pass (google.com: domain of sergioc@derechonntt.com designates 195.[redacted] as permitted sender) client-ip=195.[redacted];
Authentication-Results: mx.google.com;
       dkim=pass header.i=@derechonntt.com;
       spf=pass (google.com: domain of sergioc@derechonntt.com designates 195.[redacted] as permitted sender) smtp.mailfrom=sergioc@derechonntt.com
Received: from www.derechonntt.com (localhost [IPv6::1])
        by [redacted] (Postfix) with ESMTPA id 6C07C59E2D88
        for <d.sergiocm@gmail.com>; Mon, 11 Apr 2016 19:31:07 +0200 (CEST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=derechonntt.com;
        s=mail; t=1460395867;
        bh=LPO0kP1e+kFzvxsQWDPjG8oRkycOKfPQBSeabvk1ZOM=;
        h=Date:From:To:Subject;
        b=SfQAR79kgd0kseD7P/s4jrSRL4j7cR3M2qUJqH1sKiQEz1DPHTtVisE1xW4PFbBmy
         cOwixMPLhfTQn4MbYOmkCmERHDIyCt/xikpvCJVPfhtrgZuOxXC0MQBUcveOXP0MH2
         HxaX++64DIITPLqw/1CuTDEFAu37FiM4Z/rBB204=
MIME-Version: 1.0
Content-Type: text/plain; charset=US-ASCII;
 format=flowed
Content-Transfer-Encoding: 7bit
Date: Mon, 11 Apr 2016 19:31:07 +0200
From: Sergio Carrasco Mayans <sergioc@derechonntt.com>
To: d.sergiocm@gmail.com
Subject: Mail
Organization: Derecho en Red
Message-ID: <2296ee490a237fe09fa33d171da8adff@www.derechonntt.com>
X-Sender: sergioc@derechonntt.com
User-Agent: Roundcube Webmail/1.1.0

Un mail
```

Pese a tratarse de exactamente el mismo mensaje, nos encontramos ahora con 1.835 caracteres (contando espacios) y un importante conjunto de información que hasta este momento desconocíamos. Cabeceras incluidas tanto por el remitente como por el servidor destinatario, y que quedarían fuera de la prueba si se limitara a certificar aquello que resulta visible con un mero cliente de correo electrónico.

Podría parecer que no resulta tan importante, pero si miramos el tipo de datos que se incluyen podemos observar algunos tan importantes como la IP origen del correo electrónico, que en este caso concreto ha superado la validación del Convenio de Remitentes o SPF. Ahora bien, en este caso también debemos reconocer que al tratarse de una mera cabecera en formato texto debería resultar sencillo alterarla (o incluso incluirla) si lo estimáramos oportuno, al igual que sucede con las cabeceras que incluyan direcciones IP. Dicho esto, existen otros datos que pueden resultarnos mucho más útiles.

En este caso me refiero a la cabecera DKIM, que nos permitirá comprobar si el mensaje ha sido modificado en tránsito o una vez recibido a través de un sistema de criptografía asimétrica.



En este caso concreto podría modificar el asunto o el cuerpo del mensaje, y visualmente podría prosperar, pero eso supondría que no superara la validación de la firma DKIM incluida en las cabeceras de este correo electrónico. En tanto no disponga de la clave privada utilizada por el servidor de correo saliente (y mientras el algoritmo de firma no cuente con una vulnerabilidad tal que me permita generar una colisión que incluya la información que me interesa) un perito experto podrá acceder a dicha cabecera e informar sobre si se ha producido una modificación del mensaje inicial. Por supuesto, también puede darse el caso de que el remitente haya firmado con su clave privada personal el correo electrónico, lo cual añadiría de nuevo un factor importante a nuestra prueba. Pero ello requiere que volquemos toda la información, tanto la que ve el usuario como la que no.

Dependiendo del caso es posible que el correo electrónico no solo se haya descargado en un equipo del cliente, sino que se mantenga una copia en un servidor de correo fuera de su control, y que podemos señalar para la obtención de información adicional. Por lo tanto, no podemos generalizar sobre las posibilidades de que prospere una determinada prueba en base únicamente a su naturaleza.

Los metadatos existentes en otros documentos como imágenes son también fácilmente modificables en nuestros equipos, y ya no se requiere de grandes conocimientos informáticos para realizar esta tarea al existir aplicaciones de fácil uso que podemos descargar en nuestros ordenadores.

El problema en la práctica es que muchas veces se descubren vulnerabilidades que revelan que incluso esta información oculta puede (en ocasiones) ser modificada de forma sencilla. Los terminales móviles pueden facilitar información de geolocalización falsa a las aplicaciones con las que trabajan, y

hay aplicaciones que incluyen la clave privada utilizada para firmar los ficheros como propios dentro de la propia aplicación y accesible para sus usuarios (de forma similar a lo sucedido en el caso de WhatsApp).

¿Podrá probarse su modificación?

A la pregunta de si puede probarse si un documento electrónico ha sido modificado por la parte que lo aporta la respuesta es "puede", y dependerá de otras circunstancias que deberán ser analizadas caso por caso, teniendo además en cuenta que lo que damos por válido hoy puede que nos sorprendamos mañana descubriendo que no resultaba tan certero como parecía.

Esto no debe llevarnos a una falta de esfuerzo en la aportación de nuestras pruebas, o en la impugnación de las pruebas de la parte contraria, porque de ello finalmente dependerá la valoración que realice el Juez. En el ámbito de la prueba electrónica no debemos dar nada por sentado.

Sergio CARRASCO MAYANS

Fuente original:
https://www.faseconsulting.es/legal/la-alegalidad-o-limbo-legal-de-la-prueba-electronica

4

La prueba electrónica envenenada

Ricardo Oliva León*
@RicardoOlivaON

Reflexión inicial: Abogado versus Juez

En una entrevista realizada el año 1993 se le preguntó a Alan M. Dershowitz **"¿No cree usted que un abogado está obligado a buscar una sentencia correcta y justa?"**. El reputado abogado norteamericano y profesor de Harvard Law School, respondió lo siguiente:

"No tengo ningún interés en lo correcto. *Mi único interés como abogado penalista es ganar. Los jueces deben imponer una sentencia correcta.* El denunciante (y el fiscal) deben exponer los cargos correctamente. Como abogado defensor no tengo el más mínimo interés en descubrir lo correcto. Mi único interés es ganar." [Las cursivas son mías]

Dershowitz retrata al abogado defensor, al fiscal y al juez en su actuación ordinaria dentro de un proceso judicial y deja claro que cada uno de estos sujetos protege diferentes intereses. Lo que no le dio tiempo de precisar fue que existen ciertas exigencias legales que condicionan la actuación de esos

* Abogado especialista en Derecho tecnológico y Derecho de sociedades. Letrado colegiado ejerciente en España y Perú. Socio de Lexmotive Law Group, boutique especializada en Derecho tecnológico. Profesor de Derecho Digital en el Centro Universitario Villanueva (Curso de Derecho Digital) y en la Universidad Antonio de Nebrija (Executive Master Business Innovation en Security & Safety y Medical & Health, coordinado por el Grupo GEES Spain). Miembro del equipo ganador del 1º Legal Hackathon de España, realizado en Bilbao en mayo de 2015. Ha estudiado y trabajado en Perú, Portugal, Alemania, Reino Unido, Francia, Italia y los Estados Unidos de América. Fundador y editor de Juristas con Futuro. Autor del blog Des-complicando el Lenguaje Jurídico. Puedes escribirle a ricardo@lexmotive.com. Junto con Sonsoles Valero Barceló ha sido el encargado de coordinar este eBook.

sujetos en el proceso y que limitan **la validez y la eficacia probatoria de los medios de prueba** aportados.

¿De qué trata este artículo?

Una de las exigencias legales más conocidas se refiere a las **pruebas de un delito obtenidas de modo ilícito** las cuales se consideran **nulas de pleno derecho** por lo que no podrán ser utilizadas en contra de persona alguna dentro de un proceso judicial. Un medio de prueba ilícito es aquél obtenido, directa o indirectamente, **violentando derechos y libertades fundamentales** (art. 11.1 LOPJ; arts. 283.3, 287 y 433.1 LEC).

A partir de lo dicho surgen las siguientes preguntas: **¿qué validez y eficacia probatoria tiene el medio de prueba obtenido a partir de otro que es ilícito? ¿Es aquél también nulo de pleno de derecho aun cuándo permitiera acreditar indubitablemente la existencia de un daño o la comisión de un delito?**

Veamos los siguientes casos:

1. En un proceso judicial de divorcio ocurrido en Italia (el caso se describe en la sentencia de 18.03.2015 del Tribunal Ordinario de Roma, siendo Cecilia Pratesi la juez relatora) el marido, con el fin de acreditar la relación adúltera que su mujer mantenía con otro hombre, aportó como medios de prueba mensajes de SMS intercambiados por su mujer con su amante desde el teléfono móvil de aquélla, y fotografías y mensajes de textos obtenidos de la red social Facebook. Tales mensajes, inequívocamente, acreditaban diálogos e intercambios de afectuosidad, palabras amorosas y claras referencias a una común sexualidad entre dos personas entre las que había una relación íntima en curso. La mujer cuestionó la **licitud** de tales medios de prueba alegando que **habían sido obtenidos vulnerando su derecho fundamental a la privacidad**. El Tribunal italiano dio la razón al hombre indicando que **no puede considerarse ilícito el descubrimiento casual del contenido de los SMS, aunque sean personales, fácilmente legibles en un teléfono móvil dejado en un espacio común de la casa familiar**.

2. Un trabajador utiliza el correo corporativo de su empresa para revelar y filtrar a terceros datos empresariales reservados. Posteriormente, el empresario accede a la cuenta de correo del trabajador a través del ordenador que utilizaba en el centro de trabajo, descubre la revelación no autorizada de secretos

empresariales, y procede a despedir al trabajador. Si consideramos que la intervención del ordenador del trabajador por parte del empresario constituye un caso de **intromisión ilegítima en el ámbito de protección del derecho fundamental a la intimidad** (según el art. 7 de LPCDHIPPI), la aportación del correo electrónico no debería ser admitida por como **prueba válida** ante un tribunal (ya que, por haberse obtenido vulnerando el derecho a la intimidad del trabajador, se consideraría una **prueba ilícita**). En esa hipótesis, por tanto, y aunque realmente haya existido **descubrimiento y relevación de secretos empresariales** este delito (tipificado en el art. 199 CP) no se podría probar. Si consideramos, por el contrario, que la intervención del ordenador del trabajador por parte del empresario ha sido un acto legítimo, el delito de descubrimiento y revelación de secretos sí podría quedar acreditado. Esto último fue lo que ocurrió en el caso recogido en la **sentencia del Tribunal Constitucional, Sala 1ª, de 7 de octubre de 2013** donde el TC apreció la **inexistencia de intromisión ilegítima** debido a que en el convenio colectivo aplicable se consideraba como **falta grave el uso del correo electrónico para fines diferentes a los laborales**, por lo que el trabajador debía tener la expectativa razonable de que sus correos electrónicos podían ser fiscalizados legítimamente por la empresa en cualquier momento, como efectivamente ocurrió.

Los casos mencionados aluden o se refieren a la doctrina denominada **teoría de los frutos del árbol envenenado** que sostiene que todo **resultado probatorio generado a partir de un medio de prueba ilícito** -porque vulnera derechos y libertados fundamentales, o porque implica la realización de una actividad prohibida por la ley- **adolece de nulidad insalvable y afecta a todos aquellos medios de prueba relacionados y derivados a partir de dicho medio de prueba**. Para una mejor comprensión de esta teoría recomiendo leer dos textos "**La doctrina del fruto del árbol envenenado**" y "**La grabación de imágenes y de sonido en el proceso civil y los derechos a la intimidad, propia imagen y secreto de las comunicaciones. Nuevas resoluciones jurisprudenciales**", y ver el film **Los Jueces de la Ley** (1983), dirigido por Peter Hyams y protagonizado por Michael Douglas.

Dicho lo anterior, el objetivo del presente artículo es analizar **cómo los tribunales de justicia deben valorar la aportación de un medio de prueba electrónico derivado de otro que es ilícito**. Esto explica el título del post: **La Prueba Electrónica Envenenada**.

La prueba judicial en España

En España el Código Deontológico de la Abogacía Española establece que el **abogado** asesorará y defenderá a su cliente con **diligencia y dedicación** asumiendo personalmente la responsabilidad del trabajo encargado (art. 13.10); y que mientras esté asumiendo la defensa deberá llevarla a término en su integridad **gozando de plena libertad para utilizar los medios de defensa que estime pertinentes, siempre que sean legítimos y hayan sido obtenidos lícitamente, y no tiendan como fin exclusivo a dilatar injustificadamente los pleitos** (art. 13.11).

Por su parte a los **jueces** (y a los magistrados) corresponde en exclusiva el **ejercicio de la potestad jurisdiccional** por lo que asumen la función de **resolver y dirimir los conflictos de intereses jurídicos en general, vale decir, juzgar y hacer ejecutar lo juzgado con arreglo al sistema de fuentes del derecho vigente** (art. 117 CE, art. 2.1 LOPJ).

En el ejercicio de esa potestad jurisdiccional la **prueba** constituye uno de los problemas fundamentales dentro del proceso judicial (independientemente de que estemos en el orden civil, penal, contencioso-administrativo o social) puesto que **la respuesta final que da el juez sobre la cuestión suscitada en la demanda o sobre los delitos imputados en la denuncia (la sentencia) tiene que apoyarse, necesariamente, en los hechos debidamente probados**. Por ello, merece la pena detenerse un momento para reflexionar sobre las **reglas procesales que regulan la prueba judicial**.

Leamos estas preguntas: ¿Cuál es la etapa más importante en un proceso judicial? ¿Está obligado el juez a conocer la verdad de los hechos antes de dictar sentencia? ¿Hasta dónde pueden o deben llegar los jueces en su búsqueda de la verdad? ¿Podría una sentencia sustentarse en hechos "correctamente" probados aunque "falsamente" ocurridos?

El proceso judicial existe porque hay "algo" que necesita ser acreditado (si todo estuviera claro para las partes y nada hubiera que probar, no existiría proceso judicial). Por eso se ha dicho con razón que **el arte del proceso es el arte de la prueba**. Hablar de la **prueba judicial** es referirse a **la determinación de los hechos justificativos de las resoluciones judiciales** (y, particularmente, de las sentencias).

Parto de la premisa siguiente: **si bien el objetivo de la prueba en el proceso judicial no puede ser otro que la averiguación de la verdad de los enunciados fácticos del caso, la justificación de las sentencias no exige –necesariamente- la verdad de un enunciado para que éste pueda ser considerado como probado**. Es decir, cuando una resolución judicial dice "***Está probado que X***" esto debe ser entendido como "***Hay elementos de juicio suficientes (en el expediente) a favor de X***", donde el juez (o el magistrado, según el caso) es quien toma la decisión racional acerca de la existencia o inexistencia de elementos de juicio suficientes para aceptar "**X**" como verdadera. Sigo aquí la tesis propuesta por Jordi Ferrer Beltrán, profesor de Filosofía del Derecho de la Universidad de Girona, en su libro **Prueba y Verdad en el Derecho**.

Por tanto, para quien escribe estas líneas una **sentencia válida y eficaz** para el Derecho (correcta y justa, en palabras de Dershowitz) es aquella donde los **elementos de juicio** disponibles son **suficientes** para que **resulte racional aceptar una proposición como verdadera** en el razonamiento decisorio, siempre que haya respetado las **reglas procesales sobre la prueba judicial**.

Reglas procesales generales aplicables a los medios de prueba judicial

El ordenamiento jurídico ha establecido un conjunto de reglas procesales sobre la prueba que imponen límites acerca de las posibilidades generales de probar válidamente un hecho dentro de un proceso judicial. Como veremos a continuación estas **reglas procesales** se refieren a tres aspectos: la **actividad probatoria**, los **medios de prueba** y el **resultado probatorio**.

Al respecto es pertinente resaltar que si bien existen reglas procesales propias para cada orden jurisdiccional, **la Ley de Enjuiciamiento Civil (LEC) ocupa un lugar especial en este marco**, ya que sus preceptos son siempre de aplicación, en defecto de disposiciones en las leyes que regulan los procesos penales, contencioso-administrativos, laborales y militares, a todos estos procesos (art. 4 LEC).

a) Reglas procesales sobre la actividad probatoria

Las reglas procesales que versan sobre la actividad probatoria **incluyen fundamentalmente aquellas que establecen el inicio y el final de la fase probatoria en el proceso judicial, el modo y la forma cómo deben practicarse las pruebas y la iniciativa de la actividad probatoria (proposición y aportación de la prueba)**.

Por ejemplo, en el **proceso civil** las pruebas se practicaran a instancia de parte aunque el tribunal podrá acordar, de oficio, que se practiquen determinadas pruebas o que se aporten documentos, dictámenes u otros medios e instrumentos probatorios cuando así lo establezca la ley (art. 282 LEC); las pruebas se practicaran contradictoriamente en vista pública, o con publicidad y documentación similares si no se llevasen a efecto en la sede del tribunal (art. 281.1 LEC); todas las pruebas se practicaran en unidad de acto aunque, excepcionalmente, el tribunal señalará, con al menos cinco días de antelación el día y la hora en que hayan de practicarse los actos de prueba que no sea posible llevar a cabo en el juicio o vista; si, excepcionalmente, la prueba no se practicase en la sede del tribunal, se determinará y notificará el lugar de que se trate (art. 291.1 LEC); en el **proceso penal**, las pruebas de cada parte se practicarán según el orden con que hayan sido propuestas en el escrito correspondiente (art. 701.5 LECriminal); no podrán practicarse otras diligencias de prueba que las propuestas por las partes, ni ser examinados otros testigos que los comprendidos en las listas presentadas (art. 728 LECriminal).

b) Reglas procesales sobre los medios de prueba

Estas reglas regulan las normas sobre los medios probatorios, es decir, **la tipología de medios de prueba admisibles, la definición de los medios de prueba, en qué circunstancias se pueden excluir o inadmitir los medios de prueba, y la obligatoriedad de practicar determinados medios de prueba en algunos procesos específicos**.

En relación con la **tipología de los medios de prueba admisibles** se establece que podrán utilizarse en juicio los siguientes: interrogatorio de las partes, documentos públicos, documentos privados, dictamen de peritos, reconocimiento judicial e interrogatorio de testigos (art. 299.1 LEC); cuando por cualquier otro medio de prueba no antes mencionado expresamente pudiera obtenerse certeza sobre los hechos relevantes, el tribunal, a instancia de

parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias (art. 299.3 LEC).

Sobre la **definición que se ofrece de los medios de prueba** la norma procesal define, por ejemplo, qué debe entenderse por **documento público** a los efectos de prueba en el proceso: "1º Las resoluciones y diligencias de actuaciones judiciales de toda especie y los testimonios que de las mismas expidan los Secretarios Judiciales. 2º Los autorizados por notario con arreglo a derecho (…)" (art. 317 LEC); por **documento privado** (art. 324 LEC); etc. Existen **normas extraprocesales** que ofrecen definiciones acerca de medios de prueba concretos, como la que hace la Ley de Firma Electrónica (LFE) -la Ley 59/2003 de 19 de diciembre, cuya vigencia se verá afectada a partir del 2 de octubre de 2016, debido a la aplicación del Reglamento eIDAS 910/2014- del **documento electrónico**, entendido como el documento redactado y archivado en soporte electrónico que incorpora datos que están firmados electrónicamente (art. 3.6 LFE).

Respecto a la **inadmisibilidad de ciertos medios de prueba** se establece la **exclusión general de la prueba ilícita** -como ya adelanté-, es decir, aquella que se obtiene **vulnerando derechos o libertades fundamentales y en general que implique la realización de una actividad prohibida por la ley** (arts. 283.3 y 287 y 433.1 LEC, y art. 11.1 LOPJ); otra exclusión se da en la apelación penal donde las partes podrán presentar, antes del día de la vista, los "documentos" que tuvieran por conveniente en justificación de sus pretensiones sin que sea admisible ofrecer "otro medio de prueba" (art. 231 LECriminal).

c) Reglas procesales sobre el resultado probatorio

Se trata de aquellas reglas que **establecen el grado de libertad que tiene el juez para valorar los medios de prueba específicos que hayan sido aportados al proceso**. Existen dos grandes sistemas de valoración de la prueba: el **sistema de la libre valoración** y el **sistema de la prueba legal o tasada**. El primer sistema maximiza la función decisoria del juez al encomendarle la determinación del resultado probatorio específico y conjunto de los medios de prueba aportado al proceso; el segundo sistema reduce a la mínima expresión dicha función al imponerle al juez ex ante una forma determinada de establecer el resultado probatorio de uno o diversos medios de prueba.

La legislación procesal española recoge el **sistema de la libre valoración de la prueba basado en las reglas de la sana crítica**, entendida ésta última como la combinación de criterios lógicos y de experiencia que debe aplicar el juez (arts. 316.2, 326.2, 334.1, 348, 376, 382.3 y 384.3 LEC). No obstante, existen algunos vestigios de **prueba legal** como sucede, por ejemplo, con el art. 319.1 LEC cuando establece que "los documentos públicos comprendidos en los números 1 a 6 del art. 317 ***harán prueba plena*** del hecho, acto o estado de cosas que documenten".

En todo caso, se establece que la valoración de la prueba no podrá ser arbitraria sino que deberá ser siempre motivada y fundamentada (art. 120.3 CE y 247 LOPJ).

La prueba electrónica

Presentadas las principales reglas procesales que regulan la actividad probatoria, los medios de prueba y el resultado probatorio toca ahora detenerme en el concepto de **prueba electrónica**.

La **prueba electrónica**, conocida también como **prueba digital, prueba tecnológica, prueba informática o ePrueba**, no ha sido definida como tal -hasta la fecha- por ninguna norma jurídica de carácter estatal o comunitaria europea. El Estado, como titular de la competencia exclusiva sobre la Administración de Justicia en España (art. 149.1.5ª CE), no ha aprobado ninguna ley que le provea de contenido. Sí, en cambio, ha definido lo qué es un **documento electrónico** y lo qué es la **firma electrónica** (Ley de Firma Electrónica y Reglamento eIDAS 910/2014). Frente a este panorama normativo **surge el reto de adoptar un concepto uniforme y válido de prueba electrónica**.

Hablar de **prueba electrónica** es hacer referencia a las tecnologías de la información y comunicación. La definición de prueba electrónica propuesta por Federico Bueno de Mata, profesor de Derecho Procesal de la Universidad de Salamanca, en su libro **Prueba Electrónica y Proceso 2.0**, me parece acertada ya que además de tener en cuenta la definición del término "electrónica" que ofrece la **RAE** incluye, por su amplitud, a cualquier **medio de prueba electrónico** que se nos pueda ocurrir crear en un futuro:

"cualquier prueba presentada informáticamente y que estaría compuesta por dos elementos: uno material que depende de un hardware, ***la parte física y***

visible de la prueba para cualquier usuario de a pie, por ejemplo la carcasa de un Smartphone o una memoria USB; y por otro lado ***un elemento intangible*** que es representado por un software consistente en los metadatos y archivos electrónicos modulados a través de unas interfaces informáticas" (p. 130). [El resaltado es mío]

Ahora bien, desde una perspectiva de Derecho Procesal, **no existe un procedimiento probatorio especial para valorar la prueba electrónica, es decir, para los medios de prueba electrónicos**. Esto tiene sentido ya que la prueba electrónica no es diferente, en esencia, a la prueba tradicional. Ambas pueden probar tanto la ocurrencia de hechos físicos como de hechos electrónicos. La única diferencia entre ambas es que la **prueba electrónica** se expresa mediante un **soporte electrónico** creado por las tecnologías de la información y comunicación motivo por el cual reviste de un **carácter efímero y manipulable** mayor que el de las otras pruebas. Por tanto, a la **prueba electrónica** le serán aplicables las reglas procesales generales sobre actividad probatoria, medios de prueba y resultado probatorio. No obstante, debe tenerse en cuenta las siguientes particularidades:

- Se le aplicarán las normas referidas a los llamados **medios probatorios análogos**, es decir, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso (art. 299.2, 299.3 y 384.1 LEC).
- Se le aplicarán además las reglas procesales referidas a los **medios audiovisuales (instrumentos de filmación, grabación o semejantes), cuando éstos sean electrónicos,** es decir, medios de prueba que permitan la reproducción ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación y otros semejantes (arts. 299.2, 382.1 y 382.2 LEC).
- El tiempo establecido para la proposición y aportación de la prueba electrónica debería ser el más temprano posible a fin de asegurar la cadena de custodia, vale decir, a fin de garantizar la **autenticidad, inalterabilidad e indemnidad** de la prueba electrónica.
- El modo de preservación y conservación de la prueba electrónica dentro del proceso judicial no está regulado debidamente en la LEC puesto que dicha ley solo contempla medidas de conservación,

únicamente, por parte del secretario judicial. Si bien la ley no lo exige expresamente, el Juzgado debería poder utilizar sistemas tecnológicos y humanos de salvaguarda de la prueba electrónica más seguros, tales como un sistema seguro de **cloud computing** o acudir a terceros de confianza.

- En cuanto a la forma de aportación de la prueba electrónica la LEC no se decanta por algún hardware "específico" por lo que el soporte multimedia es claramente admisible (art. 384.1 LEC).
- La admisibilidad de la prueba electrónica debe cumplir los requisitos exigidos a cualquier otro medio de prueba: pertinencia, utilidad y licitud. Respecto de esta última **la prueba lícita serás aquella que se obtiene sin violar derechos y libertades fundamentales**.
- Debido a la facilidad de manipulación de la prueba electrónica, la dificultad de la visualización o escucha de material intangible, y la dificultad para distinguir entre el original y la copia; la intervención de un **perito informático** para elaborar el correspondiente dictamen pericial puede ser muchas veces necesario y hasta determinante (art. 335 LEC).
- La prueba electrónica aportada debe analizarse, como cualquier medio probatorio ordinario o convencional, bajo los **principios de oralidad, contradicción, concentración, publicidad e inmediación**.
- El sistema de valoración aplicable a la prueba electrónica, como regla general, es el de la **libre valoración de la prueba bajo las reglas de la sana crítica**. El carácter técnico-informático de la prueba electrónica no justifica, en mi opinión, la aplicación automática de un sistema de valoración de prueba tasada. El juez siempre puede contar con el auxilio de un **perito informático** que le ayude a esclarecer si ha habido o no manipulación de un medio de prueba electrónico, y con el apoyo de un **prestador de servicios de certificación** que le ayude a determinar la integridad de los datos y la corrección del origen de los mismos. El sistema de prueba legal se aplicará –solo y exclusivamente- en los casos que la ley así lo disponga de modo expreso, cómo sucede cuando la prueba electrónica se basa en un documento público con firma electrónica avanzada (art. 319.1 LEC y art. 3.6 LFE), sin perjuicio de que en dicho caso el juez pueda realizar una valoración del

instrumento conforme a las reglas de la sana crítica, cuando éste haya sido impugnado (arts. 320 y 384.3 LEC).

La teoría del fruto del árbol envenenado

El Tribunal Supremo de los Estados Unidos desarrolló la **teoría del fruto del árbol envenenado** en el caso Silverthorne Lumber Company v. United States, 251 U.S. 385, 40 S. Ct. 182, 64 L. Ed. 319 (1920). El término "the fruit of the poisonous tree" fue usado por primera vez Nardone v. United States, 308 U.S. 338, 60 S. Ct. 266, 84 L. Ed. 307 (1939). En el primer caso, tras un registro, los agentes del Gobierno entraron con allanamiento en las oficinas de la empresa Silverthorne Lumber y detuvieron a su principales directivos (a Frederick W. Silverthorne y a su padre) en mérito a la información proporcionada por los libros de contabilidad hallados e incautados en dicho registro; posteriormente el directivo apeló y acogiéndose a la cuarta enmienda de la Constitución americana logró que el tribunal declarara **ilegal** todas las pruebas obtenidas en el allanamiento. En el segundo caso, se condenó a una persona en base a la información obtenida de una conversación telefónica interceptada por funcionarios del Gobierno; en vía de apelación el tribunal consideró **ilegal** la interceptación por lo que toda la información obtenida a partir de dicha conversación se consideró como prueba inválida.

La teoría analizada pretende **prohibir en juicio la utilización de una prueba secundaria que se obtuvo a partir de una prueba primaria ilegalmente obtenida por vulnerar de derechos fundamentales**. **El nombre "fruto del**

árbol envenenado" es una metáfora: el **árbol envenenado** es una prueba obtenida en una detención y/o interceptación telefónica ilegal (y, en general, obtenida vulnerando derechos y libertades fundamentales) realizadas por la policía. El **fruto envenenado** es una información descubierta (mensajes de texto, documentos, declaraciones, conversaciones, etc.) a partir de los conocimientos adquiridos en virtud de una detención o interceptación telefónica previas consideradas ilegales.

Veamos otro ejemplo: un agente de policía municipal que carece de funciones de Seguridad Ciudadana detiene a una persona por estar mal aparcada y sin su autorización procede directamente a revisar su vehículo, efectos personales y a cachearla, en mérito de lo cual encuentra una dosis pequeña de cocaína; sospechando que dicha persona podría ser un narcotraficante, el agente comunica este hecho al Ministerio Fiscal quien solicita al Juzgado una orden para registrar su domicilio; el Juzgado concede la orden sin tener en cuenta que el referido agente no estaba facultado para registrar el coche ni cachear al ciudadano; cuando se registra el domicilio de la persona se encuentra una bicicleta que había sido robada semanas atrás. Bajo la teoría del fruto del árbol envenenado dicha bicicleta no podría ser objeto de un delito de robo ya que el registro domiciliario donde ella se encontró se basó en una prueba obtenida de un registro previo que era ilegal.

Ambos, **el árbol** y **el fruto** envenenados deberán ser excluidos de la valoración judicial probatoria.

Trasladando la doctrina de esta teoría a **nuestra realidad jurisdiccional** diría que, cualquier medio de prueba que no haya sido obtenido respetando los derechos y las libertades fundamentales consagradas en la CE y los Tratados Internacionales ratificados por España, estará contaminado de **ilegalidad** y, por lo tanto, no debería poder ser utilizado en los tribunales de justicia como medio de prueba válido y eficaz. Cualquier prueba que se obtenga, posteriormente, a partir la prueba contaminada tampoco debería poder ser admitida en un proceso judicial.

Ahora bien, en **sede penal** existe una complejidad adicional: se requiere desvirtuar la **presunción de inocencia** que goza el denunciado/ investigado/acusado por mandato expreso de la Constitución (art. 24.2 CE). Precisamente, a continuación, voy a comentar una interesante sentencia de la

Sala Penal del Tribunal Supremo donde se analizan y valoran **medios probatorios electrónicos**.

La prueba electrónica proveniente de un árbol envenenado

La **Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1ª) nº 16/2014 de 30 enero**, recoge un caso donde se absuelve al acusado debido a que el **medio de prueba electrónico** que le podía condenar fue obtenido de modo ilícito. Si bien el Tribunal Supremo no hace referencia expresa, en ninguna parte de su sentencia, a la "teoría del fruto del árbol envenenado" sí que invita a reflexionar sobre su aplicación práctica en casos como el resuelto en autos. Esta sentencia **casó y anuló** la sentencia de la Audiencia Nacional siguiente:

Resumen de la sentencia de la Audiencia Nacional (información extraída de la propia sentencia del Tribunal Supremo):

- La **Audiencia Nacional (Sala de lo Penal, Sección Tercera)** condenó a Fructuoso Gonzalo, funcionario del Cuerpo Nacional de Policía, como autor penalmente responsable de un **delito de cohecho**. Le impuso las penas de cuatro años de prisión, multa de 45.000 Euros e inhabilitación especial para empleo o cargo público por tiempo de nueve años y seis meses, así como al pago de las costas generadas.
- Se le acusó de haber contactado con dos personas acusadas por **delito contra la salud pública** (Domingo Ruperto y Ildefonso Nazario) mediante **mensajes telefónicos SMS enviados desde su teléfono móvil** e **emails desde su cuenta de correo electrónico**, con la finalidad de ofrecerse como colaborador partícipe de ellos en una **operación de tráfico de estupefacientes** que proyectaban realizar tales personas. Para ello, habría exigido amenazadoramente a Ildefonso Nazario una compensación económica como contravalor de la información que podía proporcionar acerca del estado de las investigaciones policiales sobre su caso, información de la que disponía por razón de su oficio, lo que desconocían los mencionados receptores de la oferta.
- La policía identificó la **dirección "IP (Internet Protocol)"** desde la cual Fructuoso Gonzalo se conectaba a **Internet** para enviar los **correos electrónicos** a las dos personas antes mencionadas (un

cibercafé ubicado en Pontevedra) a través de una cuenta de **email de nombre ficticio** (Hugo Fructuoso).

- Domingo Ruperto, en atención a la solicitud dinerada de Fructuoso Gonzalo, le habría entregado en efectivo la suma de 30.000 Euros. El día de la entrega Fructuoso Gonzalo llegó en un vehículo plenamente identificado que había alquilado a Europcar en la estación de ferrocarril de Pontevedra. Domingo Ruperto, siguiendo sus instrucciones, le dejó un sobre con dicha cantidad de dinero dentro del vehículo, el mismo que habría sido recogido por Fructuoso Gonzalo. Domingo Ruperto únicamente conocía a Fructuoso Gonzalo como el "Invisible" y logró anotar los datos del vehículo alquilado a Europcar.
- Los **medios de prueba** determinantes que condujeron a la Audiencia Nacional a condenar a Fructuoso Gonzalo, en el caso mencionado, fueron los siguientes:

  1) Las **declaraciones** prestadas en sede policial y en el plenario por Domingo Ruperto e Ildefonso Nazario.

  2) El contenido de **44 correos electrónicos** supuestamente intercambiados entre Ildefonso Nazario y Gonzalo Fructuoso (prueba electrónica 1).

  3) La **conexión IP** desde donde Gonzalo Fructuoso se habría conectado a Internet (un cibercafé ubicado en Pontevedra) para remitir los correos electrónicos a las personas antes mencionados (prueba electrónica 2).

  4) El **disco CD** remitido por la empresa Microsoft conteniendo correos electrónicos y la transcripción de su contenido (prueba electrónica 3).

  5) Las **comunicaciones vía SMS** supuestamente intercambiadas entre Domingo Ruperto y Gonzalo Fructuoso (prueba electrónica 4).

  6) El **informe pericial informático** que analiza el contenido del **disco CD** remitido por Microsoft (prueba electrónica 5).

  7) El **informe pericial informático** que analiza los **SMS** enviados y recibidos desde determinados terminales telefónicos específicos (prueba electrónica 6).

  8) El **informe de la compañía Microsoft** sobre los datos contenidos en los **correos electrónicos** que se habrían enviado Fructuoso Gonzalo, Domingo Ruperto e Ildefonso Nazario (prueba electrónica 7).

9) El **informe de la compañía Telefónica** sobre los datos relativos a las **conexiones IP** respecto a la cuenta de correo electrónico atribuida a Fructuoso Gonzalo (prueba electrónica 8).

- Fructuoso Gonzalo interpuso recurso de casación por quebrantamiento de forma e infracción de ley.

Resumen y breve comentario a la sentencia de la Sala de lo Penal del Tribunal Supremo:

- La sentencia del Tribunal Supremo declaró haber lugar al recurso de casación interpuesto por Fructuoso Gonzalo contra la sentencia de la Audiencia Nacional, y en su virtud, casó y anuló dicha resolución, dictando nueva sentencia conforme a derecho.
- El Primer Fundamento de Derecho de la nueva sentencia deja claro la **ilegalidad de la prueba practicada** cuando señala: **"Tal como se ha argumentado en la sentencia precedente no se ha practicado prueba lícita, válidamente aportada al proceso, que sea suficiente para desvirtuar la presunción de inocencia de Fructuoso Gonzalo."**
- En primer lugar, las **declaraciones** prestadas en sede policial (confesión extrajudicial) por Domingo Ruperto e Ildefonso Nazario fueron **manifestaciones espontáneas y libres que nunca se documentaron, ni se prestaron con presencia de letrado, ni hubo lectura de derechos**. El Tribunal entiende, al respecto, que no existe

inconveniente en admitir como medio probatorio **el testimonio de los funcionarios policiales implicados ya que lo prohibido es la indagación, antes de la información de derechos o cuando ya se ha ejercido el derecho a no declarar**, **pero no la audición de manifestaciones por los funcionarios públicos.**

- En segundo lugar, el permiso voluntario concedido por Ildefonso Nazario a la Policía, sin autorización judicial previa, a fin de que acceda a su **correo electrónico** para verificar las comunicaciones mantenidas por dicho señor con Gonzalo Fructuoso, **implica para el Tribunal Supremo "consentimiento" del afectado que impide hablar de injerencia y afectación al secreto de las comunicaciones (art. 18.3 CE)**. Por tanto, **no resultan de aplicación** en este caso las sentencias del Tribunal Europeo de Derechos Humanos: caso Kostowski contra Francia de 24.2.90; caso Allan contra Reino Unido de 5.11.2002; caso M.M. contra Holanda de 8.4.2003 todas ellas sobre el secreto de las comunicaciones.
- En tercer lugar, el Tribunal considera **prueba ilícita** las solicitudes formuladas directamente por la Policía a las compañías **Microsoft** (de acceso y extracción de datos de los correo electrónicos intercambiados entre Fructuoso Gonzalo, Domingo Ruperto e Ildefonso Nazario, y de datos relativos a las conexiones IP de Gonzalo) y **Telefónica** (de informe sobre los datos relativos a las conexiones IP respecto a la cuenta de correo electrónico atribuida a Fructuoso Gonzalo) ya que dichas solicitudes las habría cursado motu proprio **sin obtener la autorización judicial** correspondiente (no obra documentada en la causa ninguna autorización judicial previa). **Se alude aquí a la nula e irregular obtención de mandamientos e intervención de correos electrónicos y datos asociados**.
- En cuarto lugar, el Tribunal considera también **ilícita** la obtención de los datos relacionados con la **cuenta de correo electrónico** atribuida a Gonzalo Fructuoso y sus conexiones desde una dirección IP determinada porque en la sentencia recurrida:
    - No se tomó en cuenta los dictámenes periciales informáticos aportados.
    - No se mencionó la diligencia de volcado de la información contenida en el disco CD en presencia del secretario judicial.

- Los correos electrónicos aportados policialmente estuvieron fuera del control judicial y no hubo contradicción de las partes afectadas.
- De acuerdo al dictamen de los peritos informáticos Belamino Segundo e Ignacio Alexander del estudio de los correos electrónicos atribuidos a Gonzalo Fructuoso, no se puede concluir que ellos correspondieran con la IP del cibercafé donde aquél era supuestamente usuario.
- En la diligencia de volcado en soporte de papel y archivos contenidos en el CD aportado por Microsoft, realizada en presencia del Secretario Judicial, no se encontraron correos electrónicos relacionados con los hechos objeto de enjuiciamiento.
- Los testigos que realizaron el reconocimiento fotográfico del acusado en sede policial no declararon en sede judicial (ni en la fase de instrucción ni en la fase de juicio oral) por lo que la primera diligencia carece de valor probatorio.

- En quinto lugar, el Tribunal Supremo concluye que **no existe prueba válida** acreditativa del contenido de los **mensajes de correo electrónico** intercambiados entre Ildefonso Nazario y Gonzalo Fructuoso y, por tanto concluye que no hay delito de cohecho.

Reflexiones finales: Límites del Derecho procesal digital

¿Qué puedo decir como cierre de este artículo? Planteo las siguientes reflexiones:

- El **derecho a la tutela judicial efectiva** consagrado en la Constitución y en los Tratados Internacionales (concretado especialmente en el derecho a un debido proceso con todas las garantías, incluido el derecho de defensa y el derecho a no confesarse culpable, y el derecho de prueba o de aportación de los medios de prueba que justifiquen mi inocencia o avalen mi pretensión) **no es un formalismo jurídico vacío de contenido**. Se trata de un derecho constitucional cuyo ejercicio en un Estado de Derecho puede desactivar causas criminales.
- En **materia probatoria el fin no justifica los medios**. Por tanto, ni el árbol envenenado ni su fruto podrán ser utilizados en juicio ni podrán

justificar resoluciones judiciales. Como dijo el apóstol **San Mateo** en este pasaje bíblico famoso (en 7:17-20): "**Así, todo buen árbol da buenos frutos, pero el árbol malo da frutos malos. No puede el buen árbol dar malos frutos, ni el árbol malo dar frutos buenos. Todo árbol que no da buen fruto, es cortado y echado en el fuego. Así que por sus frutos los conoceréis**."

- La **teoría del árbol envenenado tiene excepciones**. Es decir, hay casos en los que no se aplicará. He omitido ex profeso referirme a dichos casos ya que mi intención en este artículo ha sido resaltar **cuando sí se aplica la teoría**. Queda pendiente analizar en otra oportunidad las excepciones. Dicho esto, debo mencionar que la teoría del árbol envenenado no se aplica en **tres casos**: a) cuando existe una vía de investigación diferente que permite obtener las pruebas por un cauce distinto del empleado para recabar los elementos de prueba considerados ilegales (*teoría de la fuente independiente*); b) cuando las circunstancias hubieran llevado inevitablemente al mismo resultado, no existiendo vinculación de causalidad entre la obtención de la segunda prueba y la obtención de la primera (*teoría del descubrimiento inevitable*); y c) cuando el enlace jurídico entre una prueba y otra no sea evidente, no exista una indisoluble conexión fáctica entre ambas pruebas, y se requiera realizar un juicio de valor para encontrar rastros de dicha conexión (*teoría de la conexión de antijuricidad o prohibición de valoración*).

Abreviaturas:
CE: Constitución Española.
CP: Código Penal.
LEC: Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.
LECriminal: Ley de Enjuiciamiento Criminal.
LFE: Ley 59/2003, de 19 de diciembre, de firma electrónica.
LOPJ: Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.
LPCDHIPPI: Ley Orgánica 1/1982, de 5 de mayo, Ley de Protección Civil de Derechos al Honor, Intimidad Personal y Propia Imagen.

Ricardo OLIVA LEÓN

Fuente original:
http://www.lenguajejuridico.com/la-prueba-electronica-envenenada/

5

La prueba electrónica en la banca digital. El soporte duradero

José María Anguiano Jiménez*

@garrigues_es

1.- Introducción

Probablemente una de las palabras de moda sea "digitalización". Parece que nadie quiere perder el tren del jugoso negocio digital que se avecina o de eludir amenazas en la irrupción digital en los negocios tradicionales.

Los procesos de digitalización afectan inevitablemente a las corporaciones. Requieren su transformación hacia el entorno digital y lo hacen transversalmente; también a los abogados.

Efectivamente, en una sociedad digitalizada es previsible un importante aumento de las transacciones bancarias electrónicas y, como consecuencia, también de la necesidad de acreditar la existencia y contenido de las mismas. Para lograrlo será necesario sustentar las pretensiones procesales o extra procesales de las entidades mediante exhibición o aportación de los ficheros

* Abogado, CEO de Logalty y socio de Garrigues, con una dilatada experiencia en contratación electrónica, asesoramiento mercantil a compañías titulares o comercializadoras de software, así como a compañías que prestan servicios informáticos de diversa índole. Desde el año 2004 coordina el Foro de las Evidencias Electrónicas, Think Tank de prueba electrónica, dedicado al análisis, discusión y divulgación de la prueba electrónica. Secretario general de la Asociación Española de Derecho de la Propiedad Intelectual. Profesor de Propiedad Intelectual y Nuevas Tecnologías (ICADE).

que las acreditan. En definitiva, la acreditación de la veracidad de los relatos fácticos en los que las entidades sustenten sus pretensiones se logrará previa aportación y ulterior valoración judicial de estos ficheros.

En consecuencia, los letrados de las entidades tienen dos principales tareas derivadas de su futuro digital: (i) establecer procedimientos probatorios adecuados al nuevo soporte probatorio y (ii) capacitarse para afrontar con solvencia la aparición de esta nueva fuente de prueba; el fichero electrónico.

Antes de entrar a analizar las tareas jurídicas derivadas de los procesos de digitalización conviene reflexionar brevemente de la naturaleza jurídico probatoria del fichero electrónico, así como de las características de la prueba electrónica.

2.- El fichero como fuente de prueba. Breve reflexión sobre la naturaleza jurídico probatoria del fichero electrónico.

No es cuestión sencilla ni pacífica la determinación de la exacta naturaleza jurídica del fichero electrónico. Para aproximarnos a esta cuestión significar que según el art. 26 del Código Penal documento es "*todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier tipo de relevancia jurídica".*

De acuerdo con la definición al soporte que incorpore el fichero electrónico se le consideraría, a los efectos penales, como prueba documental. Efectivamente, el fichero electrónico puede incorporar datos, hechos o narraciones con eficacia probatoria y/o relevancia jurídica.

Sin embargo, en jurisdicción civil la automática consideración del fichero como prueba documental no parece tan sencilla. Así, el artículo 299 de la LEC incluye como medio de prueba *los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables de otra clase [...]"...*

Es evidente que el fichero electrónico es un instrumento que permite archivar (grabar y guardar), conocer y reproducir. En definitiva puedo guardar un dato para luego consultarlo (conocerlo) o puedo grabar y guardar el video de una conversación para luego poder reproducirlo y así también conocer su contenido o hacer que terceros lo conozcan, divulgación. Mediante su divulgación.

Con la inclusión en la lista de medios de prueba del 299 de la LEC de los dos; el documento y el fichero, se distingue entre el medio de prueba documental y otro distinto; el instrumento, considerándolos dos medios de prueba distintos e independientes.

De otro lado, el apartado quinto del artículo 3 de la Ley de Firma Electrónica (LFE) define documento como *todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica.* Nótese que calca la definición acuñada por el CP. Sin embargo, si leemos el apartado 8 del mismo artículo de la LFE, se asegura que *el soporte en el que se hallen los datos firmados electrónicamente será admisible como prueba documental en un juicio.*

Lo que antecede sugiere diversas reflexiones:

En primer lugar se habla de "soporte material" que en cierta medida dificulta la consideración como prueba documental de aquel fichero que no haya sido incorporado a un dispositivo de almacenamiento (disco duro, pendrive, CD....etc). Es claro que el fichero es inmaterial. Puede ser telemáticamente transportado. Interpretando literalmente el artículo, el fichero solo gozaría de la condición documental cuando se incorporase a un dispositivo de almacenamiento, que es el soporte material. De optar por esta interpretación se podría llegar a excluir de la condición documental al fichero telemáticamente remitido al proceso. Sería un error, sobre todo teniendo en consideración la novedosa tendencia a la remisión telemática de determinadas aportaciones judiciales.

Además no hay motivo alguno para dotar al soporte material de mayor valor acreditativo que al "inmaterial". En realidad, lo aportado en soporte material no es sino una copia de una realidad digital generada por aparatos y programas de ordenador. En realidad lo que se aporta no es lo material sino lo inmaterial. No se puede confundir el continente con el contenido. Por eso en mi opinión y en lo relativo a los ficheros electrónicos, la prevalencia probatoria debería determinarse en función de la robustez de su contenido inmaterial; la autenticidad e inalterabilidad de este. Nada desvirtúa la autenticidad e inalterabilidad de los ficheros cuando se aportan al proceso mediante remisión telemática en lugar de hacerlo mediante entrega de un soporte material. Por este motivo, la normativa y jurisprudencia comunitarias han acuñado y delimitado el término "soporte duradero" al que nos referiremos in extenso.

Parece que el legislador distingue entre los documentos firmados electrónicamente y aquellos que no lo están. Los primeros tendrían la consideración de prueba documental y los segundos de instrumento del 299 de la LEC. Para ser así considerados, no sería preciso firmar los ficheros con ningún tipo específico de firma electrónica.

En consecuencia, se consideraría prueba documental cualquier fichero electrónicamente firmado. No siendo objeto de este trabajo el análisis de los tipos de firmas que contempla nuestra vigente LFE, solo poner de manifiesto que es habitual que se entienda que la consideración documental sólo se alcanza cuando el fichero es rubricado con una "firma electrónica reconocida". La realidad sin embargo es que la condición documental se otorga bajo la única condición de firma. Sin requerir que esta sea de un concreto tipo.

En definitiva, cada vez va a ser más frecuente la aportación al proceso judicial de ficheros con propósito acreditativo. Para la consideración de estas aportaciones como prueba tasada se requerirá que la manifestación de voluntad que se acredita esté firmada por quien la emite. En caso contrario se considerará una aportación del 299 de la LEC que se valorará judicialmente en aplicación de las reglas de la sana crítica. Por último, la condición documental se adquiere cuando el emisor de la manifestación de voluntad utiliza cualquiera de las modalidades de firma previstas en la vigente LFE.

3.- Características de la prueba electrónica

Conviene analizar las diferencias entre la tradicional prueba documental y la acreditación mediante aportación de ficheros electrónicos.

El papel rubricado es una añeja forma de probar. Se trata de una prueba tasada porque a los pactos plasmados en papel se les otorga las características de perdurabilidad e inalterabilidad. Efectivamente, la consideración de la prueba documental como especialmente robusta deriva de sus intrínsecas características. El papel permite que los pactos escritos permanezcan en el tiempo frente a la acreditación de la existencia y contenido de estos mediante el testimonio de un tercero que los presenció. Es obvio que al tercero le puede fallar la memoria o la buena fe y que resulta sin duda más fiable la formalización de los pactos por escrito.

En relación a la inalterabilidad, la escritura en papel permite detectar con relativa facilidad los cambios que se puedan producir en documento ya

formalizado que, junto a la existencia de tantas copias idénticas del pacto como partes intervienen en el mismo, ofrece razonables garantías de que el contenido de un pacto que se pueda aportar en un procedimiento judicial no ha sido alterado desde la fecha de su formalización.

Sin embargo, es obvio que en el tránsito del mundo analógico al digital, se dejan de usar tanto el papel como las firmas manuscritas sobre este. En el entorno digital la aportación de documentos en papel rubricados con firmas manuscritas es sustituida por la de ficheros firmados electrónicamente.

De acuerdo con lo anterior, para plantearse una adecuada estrategia probatoria en el nuevo entorno habrá que analizar las características del fichero electrónico y sus diferencias con el papel. De esta forma se pueden relacionar las características de la prueba electrónica, que coincidirán con las del fichero y que resultarán útiles para la valoración de lo aportado.

3.1.- La prueba electrónica es volátil.

La prueba electrónica es fácilmente manipulable sin que las modificaciones que en esta se produzcan sean fácilmente detectables. Efectivamente, si se circulariza un documento en papel entre un colectivo de personas pidiendo que se implementen cambios, cuando el documento impreso es recuperado estará lleno de tachones. Las modificaciones son fácilmente detectables. Sin embargo, si se hace lo mismo con un documento electrónico (fichero), al recuperarlo de vuelta, las modificaciones son de difícil o imposible detección. El fichero modificado tendrá la misma apariencia que cualquier otro que no lo haya sido.

De la misma opinión parece el TS cuando la sentencia de su sala 2ª 300/2015, de 19 de mayo dice:

La posibilidad de manipulación de los archivos digitales mediante los que se materializa el intercambio de ideas forma parte de la realidad de las cosas.

Del mismo modo, la prueba electrónica es de fácil destrucción, tanto de forma casual como intencionada. Efectivamente, con una sencilla instrucción puede borrarse un fichero electrónico. Si bien lo anterior es cierto, también lo es que los discos duros de los ordenadores no son tan fáciles de borrar como parece. Así, cuando se borra un fichero en un ordenador personal, en realidad no se borra del disco duro, sino que se marca para que las cabezas lectoras del ordenador no se dirijan a ese sector del disco. No obstante, los que quieren

borrar de forma efectiva un disco duro siempre pueden optar por (i) llenarlo de información re- escribiendo encima de lo que se quiere borrar (ii) formatear el disco duro con opciones disponibles en el propio sistema operativo del ordenador.

En definitiva, cabe concluir que la prueba electrónica es una prueba frágil, que puede desaparecer o transformarse con relativa facilidad sin dejar rastro aparente que la detecte o que señale al autor de la misma.

Un buen ejemplo de lo antedicho es el supuesto en el que a una persona le roban en su casa y poco después navegando por Wallapop conoce que parte de los objetos sustraídos están siendo vendidos en esta conocida página web de venta de artículos de segunda mano. En los anuncios aparece siempre el mismo número de teléfono. Cuando el perjudicado va a comisaría a presentar denuncia, se encuentra con la desagradable noticia de que los anuncios que permitían iniciar la investigación para descubrir a quien comercializaba los productos robados, han desaparecido.

Una adecuada estrategia probatoria requiere análisis sobre la adopción de medidas de aseguramiento de la prueba en un entorno tan volátil como el digital.

3.2.- La prueba electrónica es intrusiva.

La generación y custodia de la prueba electrónica pudiera llegar a resultar lesiva para la intimidad de las personas vinculadas con ella. Efectivamente, al tratarse de relaciones electrónicas entre ausentes, requieren de procesos comunicativos entre las partes que las mantienen. La obtención de evidencias derivadas de un proceso comunicativo pudiera llegar a suponer una injerencia en el derecho al secreto de las comunicaciones y/o a la intimidad de los que intervienen en el proceso comunicativo. Por esto, los procedimientos de obtención de la prueba de las transacciones electrónicas deberían evitar que, en aplicación del artículo 11.1 de la LOPJ, se produjese una vulneración de alguno de estos derechos que convirtiese en inservible la prueba obtenida. En definitiva, la condición electrónica de la prueba siembra de sospechas la licitud en el acceso a la fuente y abre el camino a impugnaciones por ilicitud de difícil dilucidación.

3.3.- La prueba electrónica es unilateral

Como se ha comentado, las transacciones electrónicas siempre lo son entre ausentes. Para que las relaciones se produzcan, las partes que intervienen tienen

que converger en un recurso informático que suele ser titularidad y estar controlado por una de ellas. Un claro ejemplo lo encontramos en el acceso a páginas web donde se presta algún tipo de servicio. Quien lo hace también tiene el control técnico de los recursos informáticos que conforman esa página web y en consecuencia es el único habilitado para generar una prueba electrónica de lo que en esa página web ocurre. También es el único que tiene la posibilidad de alterar o borrar los registros informáticos acreditativos de los allí sucedido.

En consecuencia con lo anterior la interposición resulta un recurso probatorio útil, que considero debe ser tenido en consideración en la implementación de estrategias probatorias.

3.4.- La prueba electrónica es de visualización mediata.

Mientras la prueba documental es de visualización inmediata tras su aportación al procedimiento, la electrónica requiere el concurso de hardware y software que permitan esa visualización. Así, si se aporta una carta impresa al procedimiento, cualquiera que la lea, si conoce el idioma en que está escrita, podrá acceder a su contenido. Sin embargo, si aporto un pendrive con un fichero que incorpora el correo electrónico remitido, se precisará del concurso de un ordenador así como del software de gestión de correo adecuado (gmail, outlook....) para la visualización del mismo. En definitiva, se puede concluir que mientras la prueba documental es de visualización inmediata, la electrónica lo es de la mediata, con los inconvenientes de práctica de la prueba que estas circunstancias pudieran acarrear.

En conclusión, resulta evidente que la sustitución del soporte probatorio, pasando de pasta de celulosa a byts, plantea interrogantes que conviene tener en consideración. Pudieran verse afectadas la totalidad de las actividades típicamente probatorias; el acceso a la prueba, la aportación al proceso, o, en su caso, su práctica.

4.- Sobre el soporte duradero

4.1.- Introducción.

Ninguna norma define fichero o relaciona las características que ha de tener para desplegar eficacia probatoria. Sin embargo tanto la normativa comunitaria como la nacional han acuñado un novedoso término que parece coincidir con

los *instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas* a los que hace referencia el 299 de la LEC. Me refiero al soporte duradero.

Efectivamente, la normativa comunitaria ha acuñado un término que responde a la necesidad normativa derivada de la sustitución del soporte papel por el electrónico. Se acuño con denominación "soporte duradero".

Aunque el término surge para dar respuesta a una concreta necesidad acreditativa, la de haber informado, lo cierto es que no parece descabellado pensar en la aplicación del soporte duradero, con lógicas adaptaciones, a otros menesteres. No en vano, nuestra propia normativa no se limita a exigir la utilización de papel u otro soporte duradero para acreditar un cumplimiento de la obligación de informar. También para otros supuestos como la obligación de entrega al consumidor de ejemplar del contrato ya formalizado.

El término ha cobrado especial relevancia en el ámbito civil, cuando la normativa europea se refiere a las obligaciones de puesta a disposición de información o de documentación acreditativa de alguna circunstancia. Surge en la normativa que regula procesos de contratación para establecer los requisitos con los que dicha información ha de ser puesta a disposición de los consumidores y usuarios. El legislador comunitario en los considerandos de las Directivas en las que aparece este término declara su intención de que el uso de los medios tecnológicos no sirva como disculpa para mermar el derecho de los consumidores a tener cumplida información de determinadas cuestiones en los procesos de contratación en línea.

La obligatoriedad en la utilización de soportes duraderos se establece en dos fundamentales momentos del proceso de contratación en línea; (i) en el de la puesta a disposición de la información precontractual a los consumidores y (ii) en el de la puesta a disposición de un instrumento acreditativo de la existencia de un determinado pacto entre el empresario y el consumidor.

La obligatoriedad en la utilización de soportes duraderos para la puesta a disposición de información viene normativamente complementada así como la imposición de la carga de la prueba del cumplimiento de la obligación de informar al obligado y con la declaración de nulidad contractual cuando no se puede acreditar su cumplimiento.

Por ello, la concreta delimitación de los requisitos normativos y jurisprudenciales del término es útil para concluir en el cumplimiento o no por

parte del obligado cuando la relación entre informante e informado se produzca a mediante técnicas de comunicación a distancia.

4.2.- Sobre la obligación de puesta a disposición de información.

El art. 1.261 del Código Civil enuncia los tres requisitos esenciales para la formación de contrato; (i) el consentimiento de los contratantes, (ii) que sea materia del contrato un objeto cierto y (iii) que las obligaciones contractualmente establecidas tengan una lícita causa.

Centrándonos en la prestación del consentimiento, el art. 1.265 del Código Civil establece que será nulo el consentimiento prestado por error, violencia, intimidación o dolo.

Sobre el error, señala CASTÁN que, en su sentido más general, el error consiste en el conocimiento equivocado de una cosa o de un hecho, basado sobre la ignorancia o incompleto conocimiento de la realidad de esa cosa o de ese hecho, o de la regla jurídica que lo disciplina.

DÍEZ-PICAZO entiende que el error consiste en una equivocada o inexacta creencia o representación mental que sirve de presupuesto para la realización de un acto jurídico.

El artículo 1.266 del mismo texto dice que para que el error invalide el consentimiento, deberá recaer sobre la sustancia de la cosa que fuere objeto del contrato, o sobre aquellas condiciones de la misma que principalmente hubiesen dado motivo a celebrarlo.

Considera DE CASTRO que el error relevante, como vicio del negocio, consiste en la creencia inexacta, respecto de algún dato que se ha de valorar como un motivo principal del negocio, según y conforme resulte de la conducta negocial de las partes, en las concretas circunstancias del negocio.

DÍEZ-PICAZO sitúa el problema del error contractual en el terreno de los intereses de las partes y en el de la justicia o injusticia de la vinculación, por lo que para llegar a una u otra solución estima que habrá que pondere una serie de circunstancias:

1ª. La responsabilidad que al que ha sufrido la equivocación debe imputarse respecto de ella. Es inexcusable el error cuando el que lo padece ha podido y ha debido, empleando una diligencia normal, desvanecerlo.

2ª. El carácter básico o no básico en la intención del contratante del elemento sobre el cual el error recae.

3ª. La situación del contratante contrario de quien padece el error.

La jurisprudencia, siguiendo una concepción subjetiva del error, exige que para que el error vicie la voluntad que ésta sea sustancial, imputable, desconocido, y de una importancia tal que con una diligencia regular no haya podido ser evitado por la persona que lo sufre (cfr. ss. 26 noviembre 1974, 7 de abril de 1976).

En relación con los errores que vician el consentimiento prestado para una perfección contractual la STS de 21 de noviembre de 2012 dice que para que el error pueda invalidar el consentimiento prestado, es preciso (1) que se muestre como suficientemente seguro y no como una mera posibilidad dependiente de la concurrencia de inciertas circunstancias; (2) que recaiga sobre la sustancia de la cosa que constituye el objeto del contrato o sobre aquellas condiciones de la misma que principalmente hubieren dado motivo a celebrarlo, en el sentido de causa concreta o de motivos incorporados a la causa (arts. 1261-2 y 1266 CC) ; (3) que concurra en el momento de la perfección o génesis del contrato y (4) que sea excusable.

La obligación de puesta a disposición de información a los consumidores está íntimamente ligada al consentimiento viciado por error. La asunción de un negocio jurídico de naturaleza compleja por parte de quien no tiene suficientes conocimientos vicia su consentimiento.

En la formalización de contratos con consumidores el empresario predisponente está doblemente obligado: (i) por un lado, tiene la obligación de entregar determinado tipo de información con carácter previo a la formalización del contrato y (ii) por otro lado, está obligado a la acreditación del cumplimiento de esta obligación. En definitiva, recae sobre el empresario predisponente la carga de la prueba de que se puso a disposición del consumidor dicha información, ya sea mediante la remisión en papel o en un soporte duradero.

En relación con los errores ocasionados por la ausencia o deficiente información prestada por quien está obligado a ello, concluye la STS de 20 de enero de 2014 al referirse a una solicitud de nulidad contractual solicitada por un adquirente de un producto financiero complejo que *a partir de tal incumplimiento, cabrá presumir el error con los requisitos de esencial y excusable- pues el mero hecho de venir impuesta por el artículo 79 bis 3 LMV demuestra que la obligación de ofrecer una información previa que incluya "orientaciones y advertencias sobre los riesgos*

asociados" es "imprescindible para que el cliente minorista pueda prestar válidamente su consentimiento".

Así mismo, la Sentencia de 10 de octubre de 2013 de la Audiencia Provincial de Álava señala:

"Respecto a la información, cuando de consumidores y usuarios se trata, como sucede en el presente caso, según el artículo 2.1 de la Ley de Consumidores y Usuarios de 1984, vigente cuando se suscribieron el contrato de depósito y administración de valores y la orden de valores, era (y, lo continua siendo) un derecho básico de aquellos: la información correcta sobre los diferentes productos o servicios.

En el ámbito de la contratación o intermediación bancaria, y, en general, con o de las entidades financieras, la importancia de la negociación previa y de la fase precontractual alcanza especial intensidad, exigiéndose un plus de atención y diligencia por parte de la entidad que comercializa u ofrece, y dentro de su actividad que no es gratuita, los productos financieros al informar al cliente, precisamente por su posición preminente y privilegiada respecto del cliente. Los clientes-contratantes han de recibir toda la información necesaria para tomar conciencia de lo que significa el contrato o el producto y su alcance, de los derechos y obligaciones derivados del mismo, y valorar su interés en el mismo.

Sobre la base de tan estricta regulación debe valorarse la situación de la relación de autos, pues el error invocado se encuentra en la esencia de las mencionadas obligaciones, concretamente la de informar, que debe cumplir la entidad financiera, de tal suerte que si el actor adquirió una idea equivocada y sustancialmente desviada de la que realmente representa el producto contratado, podemos concluir que ese desconocimiento no le es imputable, ni siquiera por omisión, al existir una obligación legal positiva que impone a la entidad financiera la carga de asegurarse no sólo la idoneidad del producto y su adecuación a lo que realmente quiere el cliente, sino también que el cliente comprende en su integridad la operación, con sus consecuencias. En definitiva, la entidad debe asegurarse que se cumplen los precedentes requerimientos.

En la misma línea se pronuncia la Sentencia de 5 de septiembre de 2013 de la Audiencia provincial de Valladolid. Dice:

"Debemos consignar seguidamente que el motivo fundamentador de la nulidad contractual interesada en la demanda es el error que se dice padecido por los actores a la hora de formar su consentimiento, error que se califica de sustancial y excusable y que se achaca a una falta de la debida información por parte de la entidad financiera. No se ejercita acción alguna en reclamación de los posibles daños y perjuicios irrogados a los actores en base a un defectuoso o

negligente cumplimiento por parte de la entidad de crédito demandada del contrato de depósito y administración de los valores…

En base a lo antedicho no cabe sino ratificar la conclusión alcanzada por el juzgador de instancia, en el sentido de que la entidad demandada no ha acreditado en absoluto haber proporcionado la imprescindible información para que unos clientes como los actores pudieran formar correcta y completamente su consentimiento acerca de las complejas y arriesgadas características del producto que les ofreció y que contrataban, lo que les hizo incurrir en un error esencial y excusable que vicia de nulidad el contrato"…

Por lo tanto, conforme con el artículo 62 del RD *la entidad financiera debe suministrarse a todo cliente minorista la referida información que minuciosamente regula el* RD *en un soporte duradero, de donde resulta evidente que no basta con las explicaciones verbales que la demandada sostiene (sin prueba suficiente, como luego veremos) que en este caso que suministró a los actores, sino que es necesario que esa información se suministre en un soporte duradero…*

De todo lo expuesto es fácil llegar a la conclusión que el legislador español y europeo, tiene como objetivo ser extremadamente puntillosos sobre los derechos de los clientes al suscribir este tipo de contratos, entre ellos el derecho a la información, que debe de garantizarse de la forma expuesta. Por consiguiente, al celebrar el "contrato sobre operaciones financieras" de 27 de mayo de 2008 que es objeto de estos autos la entidad financiera debió de realizar los test "mifid" sobre conveniencia e idoneidad y debió de facilitar en soporte duradero (esto es, no basta la mera comunicación verbal) la información sobre los extremos antes aludidos derivados de la suscripción de este contrato…

En relación con la segunda de las obligaciones, sobre la obligación de acreditar el cumplimiento de la obligación de puesta a disposición de la información, la doctrina de los tribunales también es clara. Frente a la práctica habitual de predisponer condiciones generales en las que el consumidor declara haber recibido y conocer la información que el predisponente tiene obligación de poner a su disposición, la jurisprudencia es clara cuando dice:

Ante la falta de prueba del contenido de la información ofrecida, se revelan como simples fórmulas predispuestas por la Caja vacías de contenido (STS de 18 de abril de 2013, rec. 1979/2011 y arts. 5 y 7 LCGC).

La Sentencia de la Audiencia Provincial de Álava de 10 de octubre de 2013 también se refiere a ello cuando dice:

*La carga probatoria acerca de tal extremo debe pesar sobre el profesional financiero, respecto del cual la diligencia exigible no es la genérica de un buen padre de familia, sino la específica de un ordenado empresario y representante leal en defensa de sus client*es.

En relación al plazo de caducidad de la acción de impugnación, según el artículo 1.301 C.C., dura la acción cuatro años, a contar desde la consumación del contrato.

Sobre las consecuencias de la declaración de nulidad de los contratos celebrados sin la previa remisión de la información precontractual, habrá que estar a lo establecido en el art. 1.303 del Código Civil; reciproca restitución de las prestaciones.

4.3.- El término "soporte duradero" en la normativa comunitaria y nacional

4.3.1.- Normativa comunitaria.

En los considerandos 9, 11, 13, y 22 de la Directiva 97/7 el legislador comunitario justifica la necesidad de inclusión en ésta de preceptos que impongan concretas obligaciones en la puesta a disposición de información en los procesos de contratación en línea. Su declarado interés se centra en: (i) que la utilización de técnicas de comunicación a distancia no conduzca a una reducción de la información facilitada al consumidor, (ii) que la información que se ponga a disposición de los consumidores no tenga carácter efímero y (iii) que la carga de la prueba del cumplimiento de las concretas obligaciones sobre la puesta a disposición de la información a los consumidores recaiga sobre el proveedor o predisponente del contrato a formalizar.

« (9) [...] los contratos negociados a distancia se caracterizan por la utilización de una o más técnicas de comunicación a distancia; [...] la evolución permanente de estas técnicas no permite establecer una lista exhaustiva, pero requiere que se definan unos principios válidos incluso para aquéllas que todavía se utilizan poco en la actualidad;

(11) [...] la utilización de estas técnicas no debe conducir a una reducción de la información facilitada al consumidor; [...] es conveniente, por tanto, determinar la información que debe transmitirse obligatoriamente al consumidor cualquiera que sea la técnica de comunicación utilizada; [...]

(13) [...] la información difundida por determinadas tecnologías electrónicas tiene a menudo un carácter efímero en la medida en que no se recibe sobre un

soporte duradero; [...] resulta necesario que se hagan llegar al consumidor, por escrito y con la debida antelación, los datos necesarios para la correcta ejecución del contrato;

(22) [...] en la utilización de las nuevas tecnologías, el consumidor no domina la técnica; [...] es necesario prever que la carga de la prueba pueda recaer sobre el proveedor».

El artículo 5 de dicha Directiva, con el título «Confirmación escrita de la información», establece:

El consumidor deberá recibir confirmación por escrito o mediante cualquier otro soporte duradero a su disposición de la información mencionada en las letras a) a f) del apartado 1 del artículo 4, a su debido tiempo durante la ejecución del contrato y, a más tardar, en el momento de la entrega cuando se trate de bienes, a menos que se haya facilitado ya la información al consumidor antes de la celebración del contrato, bien sea por escrito o sobre cualquier otro soporte duradero disponible que sea accesible para él.

El artículo 14 de la Directiva 97/7, con el título «Cláusula mínima» establece:

Los Estados miembros podrán adoptar o mantener, en el ámbito regulado por la presente Directiva, disposiciones más estrictas, compatibles con el Tratado FUE, a fin de garantizar una mayor protección del consumidor y dichas disposiciones incluirán la prohibición, por razones de interés general y en cumplimiento del Tratado, de la comercialización en sus territorios, mediante contratos celebrados a distancia, de determinados bienes o servicios, en especial de medicamentos.

En definitiva, el legislador comunitario establece un artículo de mínimos, dando opción a los Estados miembros para endurecer las exigencias para la comercialización en sus territorios mediante contratos celebrados a distancia de determinados bienes o servicios. Así mismo y en consecuencia con lo anterior, los Estados miembros no podrán, so pena de incurrir en una deficiente trasposición, dictar normas que no incluyan los requisitos mínimos establecidos por el legislador comunitario.

En la normativa comunitaria no nos encontramos con una única definición de soporte duradero. Las distintas Directivas que han legislado sobre la obligación de puesta a disposición de información a los consumidores han ido perfilando la definición de este concepto a lo largo del tiempo. No obstante lo anterior, a

pesar de la existencia de "matices" se puede concluir en que el "núcleo duro" de la de definición permanece invariable con el transcurso del tiempo.

De las distintas definiciones que ofrece la normativa comunitaria se puede concluir que todas ellas presentan elementos comunes, que permanecen invariables a través del tiempo (desde el año 2002 hasta el año 2011) con lo que habrá que entender que estamos ante una definición de soporte duradero consolidada. Los elementos comunes a todas las definiciones comunitarias de soporte duradero son cinco:

1.- La normativa comunitaria se refiere a instrumentos; cualquier instrumento que sirva o todos los instrumentos que sirvan. La definición coincide con la normativa nacional sobre los nuevos medios de prueba que así mismo se refieren al fichero electrónico y a los que también se denomina como instrumentos. (Artículo 299 LEC)

2.- De las cuatro definiciones de soporte duradero que ofrece la normativa comunitaria tres se refieren a almacenar y una a conservar. En cualquier caso, parece claro que el legislador comunitario está pensando en un instrumento que permita al consumidor almacenar la información que se le remite.

3.- El instrumento debe permitir que la información sea dirigida / enviada / transmitida personalmente al consumidor. Con independencia de que el legislador comunitario utiliza tres términos distintos – dirigir, enviar y transmitir- lo auténticamente relevante es que esa transmisión de información tiene que ser una transmisión personalizada al consumidor. La conclusión lógica de lo anterior es que el legislador comunitario está pensando en una transmisión personalizada y no en una publicación de la información que el predisponente tiene que poner a disposición del consumidor para que este acuda a recibirla.

4.- El cuarto elemento de la definición es que el instrumento permita que lo guardado por el consumidor pueda ser recuperado por este de forma fácil y durante un período de tiempo adecuado a los fines de la información transmitida. De acuerdo con lo anterior, la recuperación de la información por parte del consumidor tiene que tener dos características; (i) ha de ser fácil, huyendo de todo tipo de procedimientos que dificulten el acceso a la misma por parte del consumidor y (ii) la recuperación tiene que ser posible durante el tiempo necesario en función de los fines que el acceso a la misma por parte del consumidor tenga.

5.- Que el instrumento garantice que la recuperación por parte del consumidor de la información almacenada se produce sin cambios en la misma. En definitiva se exige al instrumento (soporte duradero) un requisito de integridad de la información que se recupera por el usuario tras ser almacenada.

4.3.2.- Normativa nacional.

La normativa nacional ha transpuesto las Directivas comunitarias con la inclusión del concepto "soporte duradero". Como se puede observar, no se aprecian cambios sustanciales en los elementos analizados de la redacción comunitaria de dicho concepto. La normativa nacional permite el uso de soportes duraderos tanto para la puesta a disposición de la información precontractual como para la posterior remisión, tras la perfección, de un instrumento acreditativo de la existencia del pacto. La normativa que incluye el concepto es la que a continuación se relaciona:

Ley General para la defensa de los consumidores y usuarios, Ley 22/2007 de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores, Ley 50/1980 de 8 de octubre, del contrato de seguro tras la modificación introducida por el apartado 3º del art. 2º de la Ley 34/2003 de 4 de noviembre, RD 217/2008, de 15 de febrero, sobre el régimen jurídico de las empresas de servicios de inversión y de las demás entidades que prestan servicios de inversión y por el que se modifica parcialmente el Reglamento de la Ley 35/2003, de 4 de noviembre, de Instituciones de Inversión Colectiva o la Circular 3/2013, de 12 de junio, de la Comisión Nacional de Mercado de Valores, sobre el desarrollo de determinadas obligaciones de información a los clientes a los que se les presta servicios de inversión, en relación con la evaluación de la conveniencia e idoneidad de los instrumentos financieros.

4.5.- Sobre la doctrina del TJUE en relación al soporte duradero. Sobre la S.T.E.J de 5 de julio de 2012 en el asunto C-49/11 (El caso Content Services)

Mediante cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en definitiva, si el artículo 5, apartado 1, de la Directiva 97/7 debe interpretarse en el sentido de que una práctica contractual que incluye dar acceso al consumidor a la información prevista en la Directiva sólo mediante un hipervínculo a un sitio de Internet de la empresa predisponente cumple lo exigido por dicha disposición.

Los consumidores, antes de celebrar un contrato a distancia con la mercantil Content Services, sólo pueden acceder a la información sobre el derecho de resolución haciendo clic sobre un enlace que remite a una parte del sitio de Internet de Content Services. Estos, tras haber formalizado su pedido, reciben del predisponente un correo electrónico que no contiene ninguna información sobre ese derecho, pero en el que figura un enlace hacia el sitio de Internet de Content Services en que pueden obtener información sobre el derecho de resolución.

En el litigio principal se plantea la cuestión de si la práctica contractual adoptada por Content Services incluye facilitar al consumidor la información pertinente en un soporte duradero antes de la celebración del contrato o, con posterioridad, la recepción por dicho consumidor de la confirmación de esa información mediante tal soporte.

En primer lugar la Sala Tercera del Tribunal Europeo analiza si, en el marco de dicha práctica contractual, la información pertinente es «facilitada» al consumidor o «recibida» por él, en el sentido del artículo 5, apartado 1, de la Directiva 97/7.

Sobre esta cuestión se pone de manifiesto que ni la Directiva 97/7 ni los trabajos preparatorios de ésta, aclaran el alcance exacto de los términos «recibir» y «facilitada», mencionados en el artículo 5, apartado 1, de dicha Directiva. De acuerdo con lo anterior concluye que, la determinación del sentido de esos términos debe efectuarse conforme a su sentido habitual en el lenguaje corriente, teniendo en cuenta el contexto en el que se utilizan y los objetivos perseguidos por la normativa de la que forman parte.

Para la Sala, los términos «recibir» y «facilitada», empleados en dicha disposición, se refieren a un proceso de transmisión, el primero desde el punto de vista del consumidor y el segundo desde el del predisponente. Para la Sala, en un proceso de transmisión de información no es necesario que el destinatario haga nada. Sin embargo, cuando se envía un enlace al consumidor, éste sí debe hacer algo para acceder a la información.

También recuerda los precedentes normativos. Mientras que en el artículo 4 de la Directiva 97/7 el legislador optó por una formulación neutra, según la cual el consumidor debe «disponer» de la información pertinente, en el artículo 5, apartado 1, de esta Directiva prefirió un término más coercitivo para el

predisponente; el consumidor debe «recibir» la confirmación de dicha información.

También recuerda el objetivo del legislador con la promulgación de la norma; según se desprende del considerando 11 de la Directiva, evitar que la utilización de técnicas de comunicación a distancia dé lugar a una disminución de la información facilitada al consumidor.

En consonancia con lo anterior la Sala concluye que cuando la información que se encuentra en el sitio de Internet del predisponente sólo es accesible a través de un enlace comunicado al consumidor, tal información no es ni «facilitada» a ese consumidor ni «recibida» por él, en el sentido del artículo 5, apartado 1, de la Directiva 97/7.

En segundo lugar, la sentencia analiza si un sitio de Internet cuya información es accesible para los consumidores a través de un enlace presentado por el predisponente debe considerarse como un «soporte duradero», en el sentido del artículo 5, apartado 1, de la Directiva 97/7.

Para analizar esta cuestión la Sala señala que la disposición ofrece una alternativa, a saber, la información pertinente debe ser recibida por el consumidor «por escrito» o «mediante cualquier otro soporte duradero».

De lo anterior, el juzgador europeo concluye en un requisito de equivalencia de tales soportes; un sustituto del soporte papel puede considerarse que satisface los requisitos de protección del consumidor, en el contexto de las nuevas tecnologías, siempre y cuando cumpla las mismas funciones que el soporte papel.

De acuerdo con lo anterior, la Sala concluye que el soporte duradero en el sentido del artículo 5, apartado 1, de la Directiva 97/7, debe garantizar al consumidor, al igual que el soporte papel, la posesión de la información mencionada en esa disposición para que, en caso necesario, pueda ejercitar sus derechos.

En consecuencia considera que un soporte es «duradero» en el sentido de dicha disposición en la medida en que permita al consumidor almacenar dicha información dirigida personalmente a él, garantice que no se ha alterado su contenido, así como su accesibilidad por un período adecuado, y ofrezca a los consumidores la posibilidad de reproducirla de modo idéntico, reproduciendo en definitiva la definición comunitaria de soporte duradero.

Por último concluye que tras el análisis de los autos no se deduce que el sitio de Internet del vendedor, al que remite el vínculo indicado al consumidor, permita a este último almacenar la información dirigida personalmente a él, de manera que pueda acceder a ella y reproducirla de modo idéntico durante un período adecuado, excluyendo cualquier posibilidad de modificación unilateral de su contenido por el vendedor.

De acuerdo con todo lo hasta aquí expuesto, la Sala falla:

Habida cuenta de todas las consideraciones precedentes, procede responder a la cuestión planteada que el artículo 5, apartado 1, de la Directiva 97/7 debe interpretarse en el sentido de que una práctica comercial que consiste en dar acceso a la información prevista en esta disposición sólo mediante un hipervínculo a un sitio de Internet de la empresa en cuestión no cumple lo exigido por dicha disposición, ya que tal información no es ni «facilitada» por esa empresa ni «recibida» por el consumidor, en el sentido de esta misma disposición, y un sitio de Internet como del que se trata en el litigio principal no puede considerarse un «soporte duradero» a efectos de dicho artículo 5, apartado 1.

4.6.- Sobre las consecuencias de la sentencia en la puesta a disposición de información contractual mediante enlace.

Del análisis de la Sentencia se concluye que su fundamentación es cicatera en lo relativo al concreto incumplimiento de Content Services en relación con la puesta a disposición de la información mediante soporte duradero. Efectivamente se limita a decir que la forma de remitir la información utilizada por Content Services no se ajusta a la definición comunitaria de soporte duradero. Dice:

Tras el análisis de los autos no se deduce que el sitio de Internet del vendedor, al que remite el vínculo indicado al consumidor, permita a este último almacenar la información dirigida personalmente a él, de manera que pueda acceder a ella y reproducirla de modo idéntico durante un período adecuado, excluyendo cualquier posibilidad de modificación unilateral de su contenido por el vendedor.

No obstante lo anterior, lo cierto es que, retomando los elementos comunes de las definiciones comunitarias de soporte duradero, uno de los requisitos para considerarlo así de acuerdo con la normativa comunitaria es que se trate de un instrumento que permita la transmisión de la información dirigida personalmente al consumidor.

Surge entonces la duda de que se entiende por "dirigir personalmente la información a alguien". La respuesta nos la da la doctrina del TS y TC, que contraponen la notificación personal a la edictal obligando para el cumplimiento del trámite de notificación a intentar la opción personalizada (a su domicilio o dirección de correo habitual) antes de proceder a la edictal (mediante publicación). Solo acreditada la imposibilidad de notificación se concede subsidiariamente al obligado a notificar la posibilidad de cumplir el trámite de la notificación mediante publicación edictal.

Aclarado lo anterior, conviene plantearse si la puesta a disposición de la información mediante enlace a la misma puede ser considerado como una comunicación personal, de acuerdo con la referida doctrina del TS y TC.

La puesta a disposición de la información mediante enlace supone un claro acto de publicación en contraposición con la puesta a disposición de esa información mediante comunicación personalizada.

La sentencia analizada pone dos fundamentales reparos a la puesta a disposición de la información mediante este procedimiento: (i) la información no es recibida sino que es el receptor el que tiene que acceder a ella y (ii) el obligado a informar no puede acreditar la ulterior integridad de la información comunicada. Toda vez que el obligado a informar es quien controla el sitio al que se enlaza, está en disposición de alterar la información a su conveniencia.

En relación al primero de los reparos de la Sala, sobre que la información no es recibida por el receptor sino que tiene que acceder a ella, la Sala entiende que la evolución del precepto propicia una interpretación restrictiva y garantista con los derechos del consumidor. Recuerda que el legislador comunitario ha sustituido el término "disponer" por el término "recibir" Para el TJU esta modificación implica la voluntad del legislador comunitario de no exigir al usuario una actitud activa para el acceso a la información.

Por otro lado, también argumenta que teniendo en consideración que la puesta a disposición de la información en soporte duradero pretende ser una alternativa a la puesta a disposición de la información en papel. Sentado lo anterior, el juzgador comunitario entiende que el papel confiere al receptor de la información en ese soporte la posesión de la copia de la información, mientras que con el acceso mediante enlace a la misma, el receptor de la información no tiene la efectiva posesión de la misma.

Este segundo reparo está íntimamente relacionado con el primero y también tiene concreto reflejo en los elementos analizados de la definición comunitaria de soporte duradero; el instrumento utilizado para la puesta a disposición de la información tiene que garantizar la no alteración de la información cuando el receptor de la misma la quiera volver a consultar. Lo cierto es que un enlace controlado por la parte predisponente carece de esa cualidad. Si el consumidor alegase que la información recibida que sustentó su decisión de contratación ha sufrido variaciones, la acreditación de la integridad de esta quedaría al único arbitrio del predisponente.

5.- Sobre las tareas jurídicas sugeridas ante la digitalización de los servicios financieros

Una vez analizada la naturaleza jurídico probatoria del fichero electrónico y profundizado en el emergente soporte duradero, prosigamos recordando las tareas sugeridas al inicio de este trabajo; (i) establecer procedimientos probatorios adecuados al nuevo soporte probatorio y (ii) capacitarse para afrontar con solvencia la aparición de esta nueva fuente de prueba; el fichero electrónico.

Aunque no soy quien para siquiera sugerir la capacitación de nadie, lo cierto es que, los procesos de digitalización suponen un auténtico reto probatorio. Afecta a la adquisición de la prueba, a su aportación y a su práctica. Además lo anterior puede condicionar en buena medida la valoración judicial que de la misma se haga. Se plantean interrogantes en relación a los dos principales motivos impugnatorios; por autenticidad y por licitud y en los próximos años su aportación requerirá abundantes explicaciones y la capacidad de entender y combatir los argumentos técnicos que se esgriman de contrario. Entiendo por lo tanto que los litigadores harán bien familiarizándose con los ficheros que tienen un propósito acreditativo.

En cualquier caso, hay una tarea anterior y en mi opinión más importante: el establecimiento de procedimientos probatorios adecuados para una correcta adquisición de las pruebas acreditativas de las transacciones bancarias que vinculan a las entidades. Es frecuente que en las compañías los letrados nada tengan que decir en los procesos de digitalización. Estas entienden que la revolución digital es cosa de los departamentos informáticos, de operaciones y comerciales de las compañías. En mi opinión es un error. Los procesos de digitalización deben prever la necesidad de obtener pruebas electrónicas

robustas de las transacciones que sucedan alrededor de sus negocios y los únicos capaces de evaluar la robustez de estos procedimientos son los juristas. Sólo desde una perspectiva jurídica se puede diseñar un sistema de adquisición y custodia de ficheros acreditativos. Nadie mejor que quien ha de aportarla y combatir las impugnaciones que de contrario se puedan sustentar para saber los requisitos formales que condicionan su eficacia.

José María ANGUIANO JIMÉNEZ

Fuente original:
https://www.logalty.com/al-dia/2016/04/la-prueba-electronica-la-banca-digital-soporte-duradero/

6

La prueba digital en el ámbito laboral ¿son válidos los "pantallazos"?

Raúl Rojas Rosco[*]

@rrojasrosco

En el ámbito procesal laboral cada vez es más frecuente la aportación de pruebas o evidencias de origen digital o electrónico con la finalidad de acreditar determinados hechos o incumplimientos laborales cometidos tanto por los empleados como por las propias empresas (prueba digital). Esta generalización en la aportación de pruebas electrónicas en sede judicial tiene su origen sin duda en la irrupción y la democratización del uso de las nuevas tecnologías de la información y comunicación (TIC) en el entorno de trabajo y que es propio de la nueva "Era digital" en la que estamos inmersos. En este nuevo paradigma digital prácticamente toda la prestación laboral se desarrolla en entornos digitales, ya sea a través de la generación, almacenamiento y tratamiento de la información digital (softwares, servidores informáticos, archivos digitales, *logs*, etc.), ya sea a través del uso de sistemas de comunicación electrónica (correo

[*] Socio del área laboral de ECIJA. Raúl cuenta con una amplia experiencia en el asesoramiento laboral integral a empresas, negociaciones a nivel federativo, así como en defensa letrada en procedimientos laborales. Se incorporó a ECIJA en 2011. Con anterioridad trabajó durante ocho años en una boutique de laboral del mercado español. Máster en Asesoría Jurídico-Laboral de Empresas por el Centro de Estudios UDIMA. Licenciado en Derecho por la Universidad Carlos III de Madrid. Raúl Rojas es miembro de CEAL (Asociación Española de Auditores Socio-Laborales). Colaborador habitual en revistas y publicaciones especializadas: Expansión, Fiscal & Laboral, El Derecho, Diario Jurídico, Revista del Consejo General de la Abogacía.

electrónico, *sms*, aplicaciones de mensajería instantánea, como *Line*, *WhatsApp*, *Yahoo Messenger*, chats, etc.). Sin embargo, como veremos a lo largo de este artículo no toda aportación de información contenida en soporte electrónico constituirá prueba digital en *stricto sensu*.

De toda esta actividad digital quedan rastros o "evidencias" que a su vez, en determinadas circunstancias, pueden servir para probar conductas infractoras en el ámbito laboral (conductas de ciber-acoso laboral, competencia desleal, fugas de información confidencial, uso indebido o abusivo de medios tecnológicos propiedad de empresa, etc.).

La cuestión es sí este tipo de pruebas o evidencias digitales tienen suficiente amparo normativo en nuestro ordenamiento jurídico para considerarlas válidas y eficaces como medio de prueba en un juicio, y en caso afirmativo, cuál será la forma correcta de aportar judicialmente estos documentos electrónicos, no sólo en orden a ser considerados como documentos *literosuficientes* para su admisión como prueba, sino también para que adquieran pleno valor probatorio en el proceso judicial.

En la práctica forense laboral no es infrecuente la aportación de meras impresiones en papel de correos electrónicos, redes sociales (*Tuenti*, *Twitter, Facebook*, etc.) o páginas webs, o incluso simples capturas de pantalla, también denominados "pantallazos", con la intención de probar determinados hechos en el acto de juicio. En este artículo analizaré algunos de los pronunciamientos judiciales más recientes sobre la eficacia probatoria de este tipo de pruebas y cuáles son los criterios que actualmente se entienden aceptados por los Jueces y Tribunales para la aportación y validez de estos documentos.

Con carácter previo a analizar el concepto de evidencia o prueba digital, debemos partir de la definición que nos ofrece de "***documento electrónico***" el **artículo 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica**, por la cual, se considerará "*documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado*".

Por lo tanto para que la información almacenada de forma digital en un soporte electrónico tenga carácter de documento electrónico se exige que la información contenida dicho soporte pueda ser identificada de forma autónoma, constando tanto la fecha de su creación como la identidad de su autor.

Sin embargo, como señala la autora Purificación Puyol en su recomendable obra "*La nueva prueba documental en la era digital*" (PUYOL CAPILLA, P., 2014, Editorial Sepín), la mayor parte de la información digital que se utiliza como prueba en los procesos judiciales carecen del rigor suficiente para ser considerados legalmente como documento digital.

Es por ello que debemos acudir en primer lugar a las normas procesales para analizar si el documento electrónico tiene encaje como prueba válida en juicio.

Tanto la **Ley 36/2011, de 10 de Octubre, Reguladora de la Jurisdicción Social (LRJS)**, como de forma subsidiaria, la **Ley 1/2000, de 7 de Enero, de Enjuiciamiento Civil (LEC)**, si bien **no regulan expresamente el concepto de documento o prueba electrónica**, sí que contemplan **su aportación a través de "*medios, procedimientos o instrumentos*"** que permitan archivar, conocer y reproducir la información digital (**arts. 299.2 y 384.3 LEC**). Por su parte, y concretamente en el ámbito procesal laboral, la LRJS admite que las partes en el proceso, previa justificación de la utilidad y pertinencia de las diligencias propuestas, puedan "[…] *servirse de cuantos medios de prueba se encuentren regulados en la Ley para acreditar los hechos controvertidos o necesitados de prueba, incluidos los* ***procedimientos de reproducción*** *de la palabra, de la imagen y del sonido o* ***de archivo y reproducción de datos****, que deberán ser* ***aportados por medio de soporte adecuado y poniendo a disposición del órgano jurisdiccional los medios necesarios para su reproducción y posterior constancia en autos***" (**art. 90**).

La acreditación en juicio de estos "procedimientos" para la reproducción de archivos (digitales) o documentos electrónicos es lo que se denomina evidencia o prueba electrónica. Esta **evidencia digital** se puede aportar al proceso, de acuerdo con las normas procesales de admisión de prueba (**arts. 90 y ss. LRJS**), **como un documento privado o mediante un documento público**, en función del origen e intervención en el propio documento; a través de la aportación de un **informe pericial de expertos**; o también mediante la constatación directa del propio Juzgado a través del denominado **reconocimiento judicial**, si bien, como veremos, **no todas estas fórmulas tendrán el mismo valor probatorio** quedando su valoración sometida a las reglas de la sana crítica del juez.

Por lo tanto, en una primera aproximación, podemos definir la **evidencia digital**, dentro del proceso judicial, como **toda aquella prueba que incluye**

cualquier información, documento, archivo o dato, almacenado en un soporte electrónico y susceptible de poder ser tratado e identificado digitalmente para su posterior aportación en un proceso judicial. Posteriormente **el valor probatorio de la evidencia digital dependerá del procedimiento elegido para su aportación en juicio**, así como de las **garantías** ofrecidas para la verificación judicial de su **autenticidad e integridad** de la evidencia, características que luego analizaremos desde un punto de vista técnico.

Con carácter general, antes de entrar a analizar cada uno de los procedimientos existentes para la aportación de pruebas electrónicas, decir que, especialmente **en el orden procesal laboral**, **todas las pruebas que se hayan obtenido vulnerando los derechos fundamentales del trabajador, como puede ser un acceso al correo electrónico del empleado sin que exista una información previa sobre dicho control empresarial, serán objeto de inadmisión judicial**, sin perjuicio de la posible nulidad de la propia medida disciplinaria que se haya podido imponer con base a dichas pruebas.

Como adelantábamos, la prueba "electrónica" puede ser practicada de varias formas, una de ellas es mediante la aportación como un mero **documento privado**, por ejemplo, a través de su impresión directa del equipo informático particular sin la intervención de un fedatario público, como puede ser la impresión de un correo electrónico o el simple "pantallazo" de un mensaje de *WhatsApp*. Sin embargo, esta forma de presentar la prueba puede generar al juzgador serias dudas sobre su autenticidad y en consecuencia disminuir su valor probatorio obligando al Juez a valorar esa prueba en conjunto con el resto del ramo probatorio presentado por las partes como puede ser el propio interrogatorio de la parte o declaraciones de otros testigos (**STSJ Madrid, Sala de lo Social, 10-6-15, Rec. 817/2014**), o incluso puede llevar a denegar su consideración como documento en sí mismo (**STSJ Galicia, Sala de lo Social, 28-1-16, Rec. 4577/2015**).

Especial mención requiere el **caso *Tuenti*** analizado recientemente también por el Tribunal Supremo (**STS, Sala de lo Penal, 19-5-15, Rec. 2387/2014**). En esta importante sentencia se enjuició la validez y autenticidad de unos pantallazos extraídos de la red social Tuenti en un caso de acoso sexual. El Alto Tribunal concluyó que si bien la valoración de **la prueba en estos casos de mensajería instantánea "*debe ser abordada con todas las cautelas*" por la posibilidad real de manipulación**, en este caso se debía valorar otras

pruebas circunstanciales como el hecho de que la propia víctima hubiera puesto a disposición del Juez de Instrucción su contraseña de Tuenti con el fin de se pudiera solicitar un informe pericial, que hubiera obtenido los pantallazos también en presencia de la guardia civil, o la circunstancia de que el otro interlocutor de los mensajes hubiera acudido como testigo al juicio.

En lo que respecta a la posibilidad de impugnación de los documentos privados presentados, una vez aportado el documento en la fase probatoria del juicio, y en el supuesto de que alguna de las partes dude sobre su autenticidad o integridad deberá impugnarlo y proponer prueba sobre su autenticidad a través del llamado *cotejo pericial de letras*. En la práctica es habitual manifestar la falta de reconocimiento del documento por la parte que no lo ha propuesto, ya que **el reconocimiento expreso tiene el valor de plena prueba en el proceso**, tanto del contenido como de la fecha e identidades que constasen en dicho documento reconocido por ambas partes. Igualmente si el documento no es impugnado expresamente la valoración judicial suele tender a presumir su autenticidad salvo prueba en contrario (*iuris tantum*).

A diferencia de los documentos privados, los **documentos públicos** a priori no son susceptibles de impugnación salvo que se tenga la seguridad de que sea una falsificación, en cuyo caso se solicitará su cotejo con el original (matriz notarial si se trata de una escritura pública) o bien la ratificación del funcionario que intervino el documento.

Siguiendo con el ejemplo anterior, la aportación de un correo electrónico o mensaje de *WhatsApp* (similar para la documentación de redes sociales, páginas webs, etc.), si se opta por incorporarlo a un documento público, dicha aportación se podrá efectuar mediante un acta notarial (**fe pública notarial**) en la cual se constatará por el Notario (fedatario público) la existencia de dichos mensajes, otorgando fe pública del acceso a la cuenta de correo o del dispositivo móvil donde esté instalada la aplicación de mensajería, y procediendo a imprimir los mensajes elegidos incorporándolos finalmente al acta notarial. En el acta de "protocolización" de los mensajes además se incluirá la dirección de correo electrónico o el número de teléfono desde los que se hayan enviado o recibido los mensajes, las fechas de los referidos mensajes, así como las identidades de los intervinientes que figuren en los textos protocolizados.

El mismo valor probatorio de documento público tendrán las diligencias de constancia realizadas en el propio Juzgado a petición de los interesados (**fe pública judicial**). En este caso, será el Letrado de la Administración de Justicia (anteriormente el Secretario Judicial) el que levante acta del contenido del concreto correo electrónico o mensaje de *WhatsApp*, identidades que figuren en dichos mensajes, así como del dispositivo móvil utilizado.

Adicionalmente a las anteriores fórmulas de aportación de pruebas electrónicas, y como un plus de garantía de autenticidad y no manipulación, se presenta la posibilidad de practicar una **prueba pericial informática** sobre el contenido de los mensajes electrónicos, y en general sobre cualquier otro contenido almacenado digitalmente, como pueden ser ordenadores, dispositivos móviles, páginas webs, redes sociales o similares.

En este caso el trabajo del perito informático consistirá principalmente en el desarrollo de procedimientos encaminados a "preservar" las evidencias digitales que se puedan derivar del contenido electrónico que se pretenda aportar en juicio. Esta preservación se obtiene a través de la realización de copias forenses "exactas" de la información digital almacenada dando lugar a un código alfanumérico de dicha información (código *hash*). Dicha copia se realiza por duplicado, depositando una de ellas ante Notario, y quedando la segunda copia en poder del perito para su posterior análisis técnico. Las técnicas utilizadas en este análisis suelen ser de carácter selectivo, es decir, sólo se busca aquella información que resulte necesaria para la investigación, a través, por ejemplo, de búsquedas "ciegas", evitando con ello posibles injerencias en datos o informaciones de carácter íntimo o privado del trabajador investigado.

Finalmente los resultados de la investigación se trasladarán a un **informe pericial técnico** que será el que se aporte en juicio. Es frecuente en la práctica que acuda el perito el día del juicio para ratificar el informe evitando con ello posibles impugnaciones de la parte contraria.

La **finalidad** de la aportación de pruebas electrónicas mediante informe pericial informático es **garantizar en el proceso judicial la originalidad, autenticidad e integridad de la información digital** que se presente como prueba digital. Por lo tanto, esta opción será útil en aquellos casos en los que exista un gran volumen de datos e información a analizar, como puede ser el disco duro de un ordenador, o bien cuando la prueba electrónica es la

principal, o incluso la única disponible, y existen facilidades (y dudas) de manipulación, como pueden ser los mensajes de aplicaciones móviles. También es recomendable utilizar este tipo de informes en casos de constatación de un uso abusivo o indebido de navegación en internet, o averiguación de identidades en redes sociales a través de complejos sistemas de patrones comunes de actuación, puesto que en muchos casos se utilizarán distintos perfiles o "avatares" que no se corresponden fácilmente con la identidad del investigado.

Para finalizar, me parece de utilidad exponer los criterios que actualmente están aplicando los tribunales para considerar válida la aportación judicial de la prueba de mensajería instantánea, en particular la referida a la prueba de mensajes de *WhatsApp*. Siguiendo las consideraciones efectuadas por el **Tribunal Superior de Justicia de Galicia en su reciente sentencia de 28 de Enero de 2016**, mencionada anteriormente, y en lo que respecta a los "pantallazos", para "*considerar una conversación de WhatsApp como documento –a los fines del proceso laboral–, sería preciso que se hubiese aportado no sólo la copia en papel de la impresión de pantalla o, como se denomina usualmente, <<pantallazo>> –que es lo único que cumple el actor–, sino una transcripción de la conversación y la comprobación de que está se corresponde con el teléfono y con el número correspondientes. Esto podría haber conseguido a través de la aportación del propio móvil del Sr. Abel y solicitando que, dando fe pública, el LAJ* [actual Letrado de la Administración de Justicia] *levante acta de su contenido, con transcripción de los mensajes recibidos en el terminal y de que éste se corresponde con el teléfono y con el número correspondiente; o, incluso, mediante la aportación de un acta notarial sobre los mismo extremos*".

En definitiva, como señala el Tribunal, **para que se pueda aceptar como documento una conversación o mensaje de este tipo (algo diferente de su valor probatorio)** se establecen **cuatro supuestos**: a) cuando la parte interlocutora de la conversación no impugna la conversación; b) cuando reconoce expresamente dicha conversación y su contenido; c) cuando se compruebe su realidad mediante el cotejo con el otro terminal implicado (exhibición); o, finalmente, d) cuando se practique prueba pericial que acredite la autenticidad y envío de la conversación, para un supuesto diferente de los anteriores.

En conclusión, **la elección de la fórmula concreta de presentación o aportación de una prueba digital**, por otro lado extremadamente usual en nuestros días, será **capital a la hora de acreditar** con visos de seguridad y

fiabilidad **los hechos y/o la información que puedan estar almacenados en cualquier tipo de soporte digital**, y cometer un error en esta fase de preparación de la prueba puede marcar definitivamente el éxito o fracaso en un proceso judicial.

Raúl ROJAS ROSCO

Fuente original:
http://raulrojas.es/234-2/

7

¿Puede WhatsApp (u otro prestador de servicios de comunicaciones) acreditar el contenido de una comunicación?

David Maeztu Lacalle*

@davidmaeztu

Este post se enmarca dentro del denominado Reto Juristas con Futuro, lanzado para debatir sobre el valor probatorio de los documentos electrónicos, y una serie de aspectos relacionados con este particular.

Como sobre el valor probatorio de documentos electrónicos ya he publicado varios post a lo largo de los años, y que nada ha cambiado en lo esencial, podemos concluir que **nuestro sistema procesal no presenta ningún problema para aportar documentos electrónicos en su formato correspondiente**.

---

* Abogado, licenciado en la Universidad de La Rioja, especializado en derecho de internet, propiedad intelectual y tecnología, y ha sido responsable del departamento de Propiedad Intelectual y Nuevas Tecnologías del Bufete de Abogados Ruiz de Palacios y Asociados de Logroño. Actualmente es socio del despacho ABANLEX. Además, es colaborador de Creative Commons España y miembro de la Junta Directiva de la Asociación de Usuarios de Linux de La Rioja. Participante en numerosas charlas de software libre y propiedad intelectual, desde su blog personal realiza números escritos para acercar materias complejas para el ciudadano medio, realizando análisis de un gran nivel técnico. En su blog, "Del Derecho y las normas" analiza diversos aspectos relacionados con la Ley y las Nuevas Tecnologías desde un punto de vista técnico, incluyendo temas relacionados con el software libre y la Propiedad Intelectual.

El régimen general que tenemos en nuestro ordenamiento jurídico es el de que siempre que la prueba haya sido obtenida con respeto a los derechos fundamentales, las partes pueden disponer de ella como consideren.

Por lo tanto, aunque todas las semanas leamos en prensa artículos sobre si se puede o no aportar un WhatsApp en un juzgado, la respuesta no cambia, supongo que los periodistas lo buscan constantemente aunque sea una cuestión más que superada.

Así, **si las partes no presentan una impugnación** cualquier medio o soporte es válido para acreditar hechos o circunstancias, ya sea un WhatsApp, ya sea un papel o ya sea un petroglifo, un vídeo o unas grabaciones.

Resuelta la cuestión principal, sin que haya mucha polémica sobre ello (en ocasiones se cuestiona si es documento electrónico o nuevo medio de prueba, pero nada relevante sobre su validez o no) creo interesante analizar otro aspecto que en ocasiones se cita como un mecanismo de verificación del contenido de una conversación, la intervención de la plataforma de mensajes como tercero que certifique el contenido de la conversación.

Se trataría de que en caso de impugnación de un mensaje de WhatsApp (o un correo o un sms) la parte solicite del juzgado que se libre un requerimiento al prestador de servicios de comunicaciones electrónicas para que indique cual fue el contenido del mensaje que se intercambiaron las partes.

En un procedimiento judicial, la parte que ve impugnada la prueba que ha aportado puede proponer que se practique otro medio de prueba sobre la autenticidad de lo aportado, **artículo 326 de la LEC**:

2. Cuando se impugnare la autenticidad de un documento privado, el que lo haya presentado podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto.

Si del cotejo o de otro medio de prueba se desprendiere la autenticidad del documento, se procederá conforme a lo previsto en el apartado tercero del artículo 320. Cuando no se pudiere deducir su autenticidad o no se hubiere propuesto prueba alguna, el tribunal lo valorará conforme a las reglas de la sana crítica.

3. Cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica.

Pero **como ya expliqué**, frente a esa proposición también la otra parte puede solicitar prueba que demuestre la imposibilidad de acreditar la autenticidad del mensaje, por lo que en materia de prueba electrónica en la que ambas partes tienen acceso a los mensajes, esta tiene muy poco valor.

En ausencia de otras pruebas, el impulso es buscar en los servidores del servicio los mensajes para que el prestador aporte copia de las comunicaciones mantenidas entre las partes.

Pero, ¿pueden estos prestadores proporcionar acceso al contenido de las comunicaciones.

El **artículo 39 de la Ley General de Telecomunicaciones** establece que:

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público ***deberán garantizar el secreto de las comunicaciones*** *de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.*

Este artículo debe conjugarse con lo dispuesto en la **Ley 25/2007 de Conservación de Datos**, en relación a su ámbito de aplicación, que en su artículo 1 establece que:

3. Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas.

A ello debemos sumar lo que dispone el artículo **18.3 de la Constitución Española**, que garantiza el secreto de las comunicaciones de la siguiente manera:

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

La conclusión, de una lectura integradora de todos estos preceptos, es que quienes prestan servicios de comunicaciones no pueden acceder al contenido de las comunicaciones que establecen las partes.

Es por eso que ningún operador de telefonía nos proporcionará el contenido de un sms intercambiado con la contraparte. Y en el caso de que se proporcionase se podría denunciar la obtención del mismo, tal y como dispone el **artículo 287 de la LEC**:

*1. **Cuando alguna de las partes entendiera que en la obtención u origen de alguna prueba admitida se han vulnerado derechos fundamentales habrá de alegarlo de inmediato, con traslado, en su caso, a las demás partes.***

Sobre esta cuestión, que también podrá ser suscitada de oficio por el tribunal, se resolverá en el acto del juicio o, si se tratase de juicios verbales, al comienzo de la vista, antes de que dé comienzo la práctica de la prueba. A tal efecto, se oirá a las partes y, en su caso, se practicarán las pruebas pertinentes y útiles que se propongan en el acto sobre el concreto extremo de la referida ilicitud.

2. Contra la resolución a que se refiere el apartado anterior sólo cabrá recurso de reposición, que se interpondrá, sustanciará y resolverá en el mismo acto del juicio o vista, quedando a salvo el derecho de las partes a reproducir la impugnación de la prueba ilícita en la apelación contra la sentencia definitiva.

Sin embargo, siendo esto indiscutible para los operadores de telefonía tradicionales, parece existir cierta laxitud sobre cuando el caso afecta a operadores de servicios de comunicaciones sobre internet. Así no parece importar indicar que se puede solicitar a estos operadores acceder al contenido de los mensajes intercambiados.

Para ello se alega que los mismos no son operadores en el sentido definido por la Ley General de Telecomunicaciones, pero el artículo 39, como he indicado, se refiere a operadores "*que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público"*

Debemos acudir a las definiciones de la propia ley para ver quiénes son aquellos a los que se dirige.

Así, el **operador** es:

persona física o jurídica que explota redes públicas de comunicaciones electrónicas o presta servicios de comunicaciones electrónicas disponibles al público y ha notificado al Ministerio de Industria, Energía y Turismo el inicio de su actividad o está inscrita en el Registro de operadores.

Red pública de comunicaciones se define como:

los sistemas de transmisión y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos, incluidos los elementos que no son activos que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes terrestres fijas (de conmutación de circuitos y de

paquetes, incluida Internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada.

Y **servicio de comunicaciones electrónicas**:

el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o de las actividades que consistan en el ejercicio del control editorial sobre dichos contenidos; quedan excluidos, asimismo, los servicios de la sociedad de la información definidos en el artículo 1 de la Directiva 98/34/CE que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas.

Las exclusiones que prevé el artículo son de transmisión de contenidos (como televisión por cable, etc.) y servicios como el hosting o alojamiento de contenidos. Por lo tanto, no puede decirse que las empresas, como WhatsApp, no debieran estar sujetas a esta norma.

Pero incluso, aunque no lo estuviera, la lectura del artículo 18.3 de la Constitución no podría resultar en una situación de menor respeto al secreto a las comunicaciones en función del método empleado.

Podría argumentarse que el mensaje al que se accede por el destinatario del mismo, en el momento de la lectura deja de verse afectado por el secreto de las comunicaciones y es considerado como un documento, sujeto al derecho a la intimidad. Pero la copia que se almacenaría lo hace antes de ser leído, lo que se generaría de manera ilícita.

En conclusión, **no debería ser admisible que los proveedores de servicios de comunicaciones electrónicas**, o como se consideren este tipo de servicios, **accedan o puedan acceder al contenido de los mensajes intercambiados por una persona**, al menos si una de las partes no ha hecho participe de la comunicación a terceras personas, que en un momento determinado puedan acreditar ese contenido.

Esa sería la labor de terceros de confianza o prestadores de servicios de certificación, que realizan el envío de la comunicación por cuenta de una de las

partes o bien figuran como destinatarios del mensaje, de tal manera que ante una impugnación actúen como testigos de la parte proponente.

David MAEZTU LACALLE

Fuente original:
http://derechoynormas.blogspot.com.es/2016/04/puede-whatsapp-u-otro-prestador-de.html

8

Cifrado de WhatsApp y aportación de prueba

Sara Molina Pérez-Tomé*

@SaraMolinaPT

Marta Sánchez Valdeón**

@MartaSanchezVal

¿Qué se puede hacer, cuando hay un problema real y necesitamos utilizar una conversación de WhatsApp o cualquier otro tipo de prueba que solo existe en formato digital?

En primer lugar deberemos tener en cuenta que su uso no sea contrario a nuestra legislación en concreto al artículo 18 CE:

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

---

* Abogada y consultora especializada en Marketing Jurídico y Estrategia. Posee un Máster en Derecho de Telecomunicaciones y Nuevas Tecnologías. Es Coach por la AICP y colaboradora del Observatorio Iberoamericano de Protección de Datos. Socia de ENATIC y social fundadora de MARKETINGNIZE, bloguera y colaboradora en diferentes medios especializados del sector a nivel nacional e internacional. Formadora en Marketing jurídico, estrategia y desarrollo de negocio, en 2014 publicó su libro titulado "EL ABOGADO 3.0".

** Licenciada en Derecho y experta universitaria en Criminología, desde el año 2011 es consultora jurídica en seguridad de la información, sobre todo en materia de Protección de Datos, Ley de Servicios de la Sociedad de la Información, Comercio Electrónico y Blanqueo de Capitales. Asesora legal y formadora en dichas materias ha obtenido varias becas. Es colaboradora del Observatorio Iberoamericano de Protección de Datos, ha realizado varias publicaciones en su blog.

El uso de este tipo de pruebas se está extendiendo y proliferando como el uso de la propia tecnología y no siempre es fácil demostrar la fiabilidad y validez de dichas pruebas.

La incidencia más obvia es que este tipo de pruebas pueden ser manipuladas.

Cualquier usuario de aplicaciones de mensajería instantánea del tipo WhatsApp, puede borrar un determinado mensaje y posteriormente sacar una captura de pantalla, ocultando así partes que podrían ser determinantes y modificando el contexto de la conversación.

Hay que tener en cuenta que en multitud de procedimientos judiciales estas pruebas han sido rechazas por entenderse que los contenidos no han sido reconocidos por el acusado ni se han practicado sobre los mismos prueba pericial informática que acredite su autenticidad y envío. Luego la única alternativa para hacer valer dicha prueba si la otra parte no reconoce su existencia, es a través de un perito informático.

La intervención de este perito debe ser lo más rápida posible ya que pueden existir ya que se corre el riesgo de que determinados elementos puedan desaparecer al ser borrados por su autor original.

Una vez que el perito ha elaborado el informe, se debe de acudir al notario para que de fe del contenido o bien utilizar alguna herramienta de tercero de confianza, acompañando en ambos casos el peritaje informático.

¿El prestador de servicios no puede "ayudar" en este trámite?

El problema es que la aplicación no conserva la conversación en un servidor externo perteneciente al administrador y sólo se conserva en el dispositivo de quienes se comunican, tal y como manifiesta WhatsApp a través del reciente encriptado de sus mensajes.

La aplicación no tendrá acceso a los mismos, tampoco si se lo piden las autoridades y en su nota oficial afirman que no mantienen registro de los mensajes en sus propios servidores y que el fin del cifrado de extremo a extremo se busca protegerlo "manos indebidas". Una decisión en línea con la actual polémica con Apple y el FBI respecto al móvil que se han negado a desencriptar.

De hecho en la nota especial para los usuarios de otros países, WhatsApp dice que el servicio está en EEUU y va dirigido a los usuarios de este país y que si

eres un usuario que accedes desde la Unión Europea, Asia , o cualquier otra región con una regulación en materia de protección de datos diferente de la estadunidense (en este caso por la ley de California) la aceptación de los términos del servicio implica la transferencia de esos datos personales y el consentimiento expreso para que rijan las leyes californianas.

Además recordemos que WhatApp pertenece a Facebook pero que desde un inicio han querido mantenerse como empresas diferentes y con términos y condiciones independientes.

Para que el cifrado se considere "end-to-end", tal y como dice **Ruth Benito Martín**, "implica que ni siquiera el prestador del servicio puede acceder al contenido cifrado. Por lo tanto, aunque a través de una comisión rogatoria (que ya es complicado) consiguiéramos requerir a WhatsApp que nos facilitara el contenido de una conversación entre usuarios suyos, esta compañía, a día de hoy, debería respondernos que no le es posible". La única opción en palabras de **Héctor Guzmán** sería **acceder (como en el caso de Apple) al/los dispositivos o buscar el usuario colaborador que permita el acceso a la conversación.**

Y en cuanto a la solicitud a WhatsApp tal y como dice **Rubén Vazquez** "Deberemos ir viendo caso a caso como va a afectar este cifrado "end to end", pero si algo es cierto, es que los requerimientos de información a WhatsApp con respecto al contenido de las comunicaciones va a acabar, al menos, mientras la CNMC no lo considere un prestador de servicios de comunicaciones electrónicas y que por tanto, tenga el deber de colaboración que afecta a las mismas".

En todo caso, habrá que tener en cuenta también la tipología del posible delito cometido, ya que si nos referimos al ámbito penal, nuestra Ley de Enjuiciamiento Criminal no contempla especialmente estos medios de prueba y sin embargo si lo hace la Ley de Enjuiciamiento Civil.

Su art. 299.1 regula los medios de prueba clásicos de los que pueden valerse las partes y se admitiría este supuesto de conversación de WhatsApp como prueba pericial, a través del reconocimiento judicial o inspección personal del juez o a través de la prueba de instrumentos tecnológicos del art. 299.2.

Además, el art. 299.3, establece que *"cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos*

relevantes, el tribunal, a instancia de parte, lo admitirá como prueba adoptando las medidas que en cada caso resulten necesarias".

Por todo ello, y tal y como especificó la **Sentencia de la Sala II del Tribunal Supremo número 300/2015, de 19 de mayo**, "*la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido*".

Parece que está claro, y bajo nuestra opinión es así, que debe haber una valoración conjunta del material probatorio, es decir que se tengan en cuenta, además de los propios mensajes, el resto de pruebas prácticas como la declaración de las partes o incluso la constatación pericial de que no ha habido una manipulación y se pueda acreditar su contenido, lo cual no resulta sencillo.

Sara MOLINA PÉREZ-TOMÉ

Marta SÁNCHEZ VALDEÓN

Fuente original:
http://www.lawandtrends.com/noticias/penal/cifrado-de-whatsapp-y-aportacion-de-prueba.html

9

Exiftool:
¿Los metadatos sirven de algo?

Rafael Perales Cañete*

@D_mas_I

¿Qué documento gráfico consideras que tiene más peso como prueba?

¿Éste?

Fotógrafos del estudio Marceau (Joseph Byron, Ben Falk, Pirie MacDonald, Pop Core y el propio Marceau) realizan en diciembre de 1920 el que puede que sea el primer selfie de la historia de la fotografía.
Foto del post: http://www.que.es/ultimas-noticias/curiosas/201402272128-sabes-primer-selfie-historia.html

¿O éste?

Selfie realizado en la gala de los Oscars de 2014.
Foto del post: http://www.abc.es/estilo/gente/20141227/abci-selfies-famosos-anio-201412261842_1.html

* Abogado del Ilustre Colegio de Abogados de Córdoba, en ejercicio desde el año 1.996 y con despacho profesional en Córdoba. Es actualmente letrado asesor de la Delegación en Córdoba del Ilustre Colegio de Gestores Administrativos de Sevilla y las especialidades de su despacho profesional son Derecho Administrativo, Derecho Informático y sobre las Tecnologías de la Información y Comunicación, y Derecho a la Protección de Datos Personales. Es especialista universitario en protección de datos y privacidad. Es miembro de ENATIC (Asociación de Expertos Nacionales de la Abogacía TIC) miembro de APEP (Asociación Profesional Española de Privacidad) y socio promotor fundador de ANPhacket (Asociación Nacional de Profesionales del hacking ético) de la que es Secretario y Asesor Jurídico. También es miembro de la Comisión de Nuevas Tecnologías del Ilustre Colegio de Abogados de Córdoba.

Una persona de principios de siglo XX si viera ambas fotos diría que ambos documentos gráficos tienen igual valor. Una persona del siglo XXI además diría que la segunda foto, ya que está realizada con un Smartphone de última generación incluye en su archivo digital una serie de datos que pueden aportar más información por ejemplo la ubicación donde fue realizada, el autor, la hora de su captura, etc...

La primera foto, que solamente consta en soporte papel ¿qué capacidad o forma de modificarla existe? Pues mínima, ya que difícilmente se podría realizar algún cambio sin dañar o modificar la celulosa donde se ha impregnado o sin alterar los productos químicos utilizados tales como nitrato de plata (AgNO3) y Bromuro de sodio o de potasio (NaBr/KBr).

Y la segunda foto, que figura en un soporte digital ¿qué capacidad hay de editarla? Se puede intuir hoy en día que bastantes más posibilidades ¿verdad?, por ejemplo esta:

Foto de http://www.que.es/gente/fotos/selfie-famoso-mundo-f808432.html

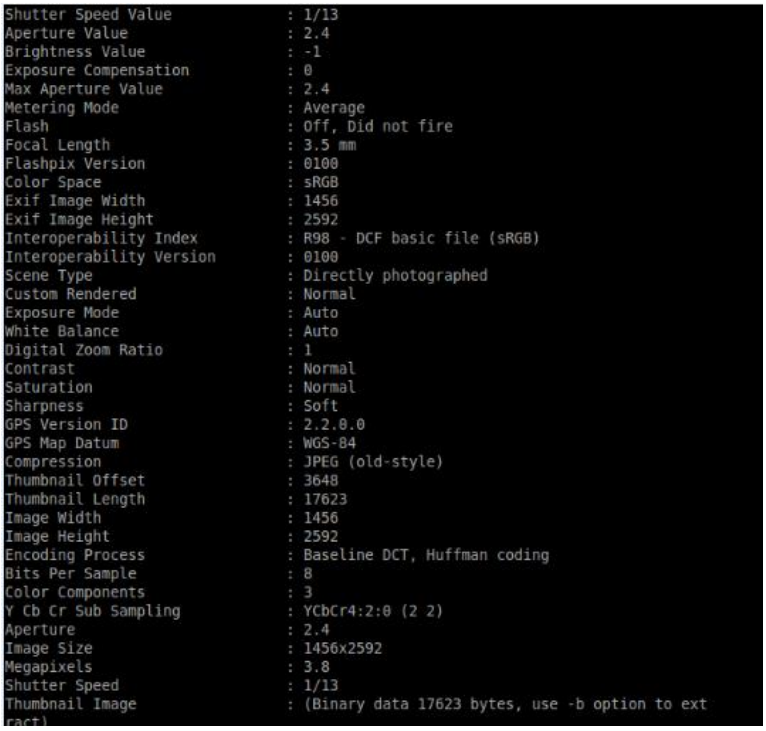
O incluso pedir que alguien te la modifique:

Ignorantes y analfabetos digitales

Después de lo expuesto ya no está tan claro que si una foto que existe en soporte digital se imprime en papel ¿es una prueba tan "sólida" como la primera fotografía? Obviamente el contenido gráfico y visual que muestra puede o no coincidir con lo expuesto en ambos soportes: el automatizado y el manual, y ha podido ser modificado antes de su impresión mediante todo tipo de software: Photoshop, Gimp, Imageforce, etc...

La aparente solución para que no pierda veracidad o autenticidad es no "sacarla" de su mundo digital: allí se generó y allí ha de permanecer, pero hay otra solución informática que puede ayudarnos a comprobar su veracidad (por lo menos, en principio).

Todo archivo informático, por lo general, dispone de un grupo de datos "ocultos" que describen el contenido informativo de un objeto al que se denomina recurso, son los denominados **metadatos**.

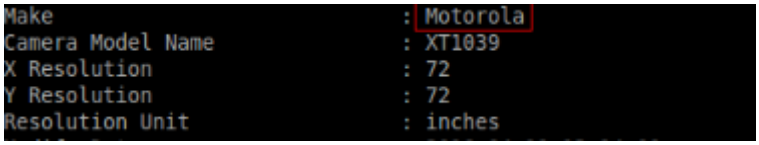


Si por ejemplo se aporta como prueba en un procedimiento judicial una fotografía digital (un documento gráfico en soporte automatizado, para ser más correcto) y el juzgador ignora los conceptos básicos informáticos puede que le dé el mismo valor que una fotografía analógica (un documento gráfico en soporte manual, para seguir siendo correcto) También podemos alegar que dicho soporte automatizado puede analizarse y mediante sus metadatos comprobar sus características, modificaciones de dicho archivo, información sobre su realización (lugar, hora, fecha) etc… aportando más datos e información complementaria.

Todo bien ¿no? Pero... a estos datos se accede mediante software, y, atención para quién no lo conozca, también existen herramientas de software que pueden modificarlos o suprimirlos, por ejemplo una herramienta *open source* "Exiftools" al alcance de cualquiera.

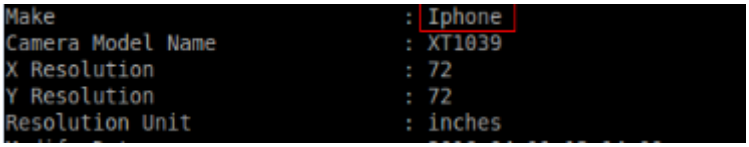
¡ Jugemos con Exiftools !

Hagamos una pequeña demostración.



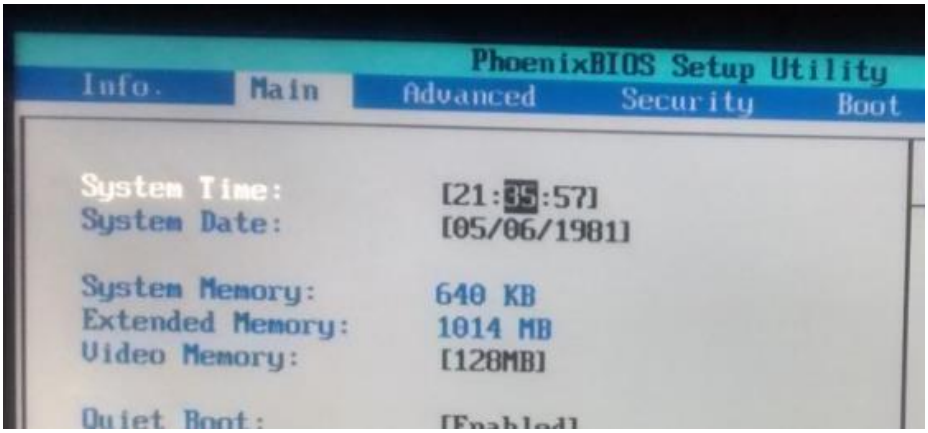
Podemos comprobar en un archivo de imagen que fue realizada con un Smartphone marca *Motorola,* y con este sencillo comando...

podemos hacer que …



que resulte de sus metadatos que fue realizado con un *iPhone* (obviamente también habría que cambiar el modelo de la cámara …) Y si dicho archivo va a ser objeto de una pericial informática, o lo vamos a enviar a un tercero de confianza para su custodia, o si lo entregamos a un Notario para que de fe

pública del contenido de los metadatos … puede que se note un poco que ese fichero ha sido modificado, pues en los metadatos figura también la fecha de la creación y modificación del archivo. ¡No hay ningún problema! Cambiemos la fecha de la Bios del sistema, por ejemplo al año 1.981...



Volvamos a utilizar la "magia" de Exiftools, y …

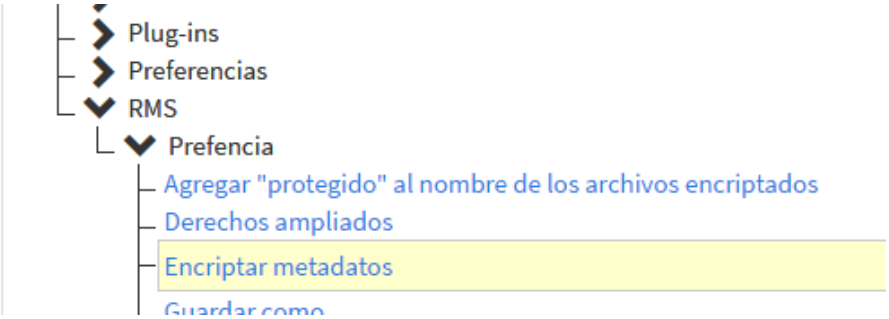
```
File Modification Date/Time     : 1981:05:06 21:37:04+02:00
File Access Date/Time           : 1981:05:06 21:37:04+02:00
File Inode Change Date/Time     : 1981:05:06 21:37:04+02:00
File Permissions                : rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : Iphone
Camera Model Name               : XT1039
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Modify Date                     : 2016:04:11 13:14:00
```

Los metadatos nos "demostrarán" que hemos realizado una foto con un iPhone en el año 1.981 (también habría que cambiar todas las referencias al genuino Motorola que creó el archivo, no soy un experto hacker, todavía …)

Si nos fallan los metadatos ¿qué nos queda?

Si la imagen impresa de un soporte automatizado puede no servir porque puede haber sido editada y si la imagen aportada en soporte digital con metadatos tampoco porque estos pueden ser haber sido modificados, por lo que ¿todo archivo digital puede incurrir en una sospecha de poder haber sido modificado o editado? Aparentemente, sí.

Si nos vamos a desenvolver y actuar en el mundo digital hay que conocer dicho mundo informático, pues también existen medios y herramientas que aportan garantías y protegen los contenidos en soportes automatizados, lo que nos obliga a que si queremos aportar un documento en soporte electrónico se hayan adoptado una serie de cautelas que de ordinario no se adoptan, entre ellas la más efectiva es encriptar el archivo, incluido si es posible los metadatos, por ejemplo una herramienta que lo permite es la aplicación Foxit Reader:



Pero esto sería una garantía frente a terceros, nada impediría que fuese el autor o creador del documento digital el que modificase su propio archivo con los datos que le apeteciera.

Si alegamos que para la garantía de un documento digital, cuando existan dos partes, también se puede firmar digitalmente el archivo automatizado, ya que si se realiza alguna modificación se perdería la incrustación del certificado digital en el archivo (la firma digital consiste en la incorporación a un archivo automatizado de un certificado digital, que no es más que otro archivo digital con el cual se combina) pero esto es para el caso de que existan los partes, comprueben y estén de acuerdo del contenido y entonces procedan a su firma digital, porque si yo firmo una fotografía digital (en cualquier formato) ¿quién

me puede asegurar que antes de realizar el proceso de firmado digital mediante un certificado electrónico no ha sido modificado el archivo, tanto lo que muestra como sus metadatos?

La grandeza y la miseria de la Sociedad de la Información

Aquí está la grandeza y la miseria del actual mundo digital: toda la facilidad para comunicarse y representar la realidad no se basa en la seguridad sino en la facilidad, y debido a esa falta de seguridad todo medios electrónicos que pueden servir de prueba de hechos o contener actos jurídicos, pueden ser de ordinario fácilmente manipulables, siempre por su creador, y por una falta de cautelas y de medidas de seguridad mínimas por terceros.

Recuerdo que cuando comenté en mi ámbito informático (mi otro ámbito es el jurídico) la famosa sentencia que argumentaba sobre la validez como prueba de las captura de pantalla o "pantallazos" (Sentencia del Tribunal Supremo de fecha 19 de mayo de 2015, número 300/2015) ¡creían que al comentar el texto de la sentencia estaba contando una chiste! Me decían: "*¿en serio se ha admitido alguna vez una captura de pantalla como prueba?*

Sí, y podría ser como la que adjunto ahora:

(Imagen retocada de un navegador y capturada en pantalla)

Desde mi punto de vista, ¿por qué se tuvo que "esforzar" el mundo jurídico en argumentar la validez o certeza de una prueba que consistía en una captura de pantalla? Simplemente porque no conocen el mundo informático, solamente lo usan, no saben cómo funciona. Un informático o simplemente un nativo

digital o una persona que no sea analfabeta digital entendería rápidamente el "fake" anterior, una persona educada y criada entre papeles lo miraría "como si fuese un papel de toda la vida" y conforme a lo que para él representa "Un Papel" (en sentido genérico) quedaría atónito, y no hay que extrañarse, ya que las expresiones populares "Hablen papeles, callen bocas" o "Callen barbas y hablen cartas" tienen su peso entre los descendientes de Gutenberg, no entre los nativos digitales.

Conclusiones

La prueba electrónica es hoy en día, desde mi punto de vista, la más "sospechosa" pues es la más susceptible de modificación, ya que no se adoptan de forma corriente ninguna precaución o cautela en su creación y conservación, y siempre, siempre, puede haber sido modificada por su creador tanto en su contenido (retoques) como en la información adjunta al fichero (cambio en los metadatos).

Dicha prueba digital ha de ser valorada y considerada junto con el resto de elementos probatorios, pues la prueba digital no es ni más ni menos que cualquier otro medio de prueba. Así, si una fotografía digital o incluso un "pantallazo" o captura de pantalla, encaja con el resto de elementos probatorios puede ser perfectamente un medio válido de prueba. No obstante si es el único medio de prueba, se debería sospechar (si no se admite de contrario, obviamente).

¿Sabemos distinguir si un documento en soporte digital ha sido objeto de modificación? En lo que respecta a documento en un soporte automatizado que configure un acto jurídico, por ejemplo un contrato, tendríamos suficientes garantías si el soporte digital donde estuviese contenido tuviera incorporados los certificados digitales de las partes intervinientes, o sea, que hubiese sido firmado digitalmente por ambas partes. Pero ¿y el resto?, por ejemplo fotografías o archivos de imagen u otros archivos automatizados. Gracias a aplicaciones como Exiftools, deberemos de buscar más pruebas, y en todo caso deberemos confiar en la pericia de los ingenieros informáticos, para el análisis informático del soporte, que dicho sea de paso, de los cuales no pienso separarme ya en lo que resta de mi vida profesional.

Rafael PERALES CAÑETE

Fuente original:
http://derechomasinformatica.es/bitacora/?p=751

10

Geolocalización y práctica probatoria, condenados a encontrarse

Rubén Vázquez Romero*

@rvazquezromero

Que la geolocalización y la práctica probatoria están condenados a entenderse no es nada que nos vaya o pillar desprevenidos.

Por un lado, la geolocalización es ya algo sumamente habitual en nuestro día a día, enviar a los amigos nuestra ubicación por WhatsApp o a hacer check in en plataformas como Yelp o Facebook, por no hablar de Google Maps y demás navegadores, no es ya nada novedoso.

Esto se debe principalmente a la telefonía móvil, que a través de los smartphones nos ha permitido hacer uso y disfrute de todas las posibilidades con las que nos beneficia la geolocalización, no obstante, esta geolocalización, ni es nada nuevo, ni es tan bonita como la pinta, y puede llegar a tener una trascendencia probatoria bastante amplia, toda vez que la información, se acumula en un terminal o en las operadoras de telefonía, con lo cual, es utilizable en nuestro favor o nuestra contra en un proceso judicial.

* Abogado especializado en Derecho informático, privacidad, redes móviles, redes sociales y telecomunicaciones. Mentor y consultor jurídico en ámbito TIC en El Cubo (Andalucía Open Future). Escribe acerca del fenómeno de la innovación tecnológica asociada al Derecho en Diario de un e-letrado.

Lo primero, para algún despistado, la geolocalización se define, según Wikipedia, como:

Neologismo que refiere al posicionamiento con el que se define la localización de un objeto espacial (representado mediante punto, vector, área, volumen) en un sistema de coordenadas y datum determinado.

Basándonos en una definición menos técnica, supone la localización de cualquier dispositivo móvil (Véase desde un GPS hasta un portátil,) a través de cualquier tipo de red inalámbrica de información, ya sea satélites de telefonía o a través de señales wifi, que permita la ubicación más o menos aproximada del mismo sobre un plano determinado, siendo para el caso que nos ocupa, dada su trascendencia y habitualidad, el caso referente a los teléfonos móviles o smartphones y su información asociada.

Sabiendo ya que es la geolocalización, debemos, a efectos de práctica probatoria, hacer una serie de consideraciones al respecto para ver todas sus posibilidades.

En primer término, debemos identificar como la misma debe aportarse al proceso, que no sería otra que a través de un documento electrónico, dada su naturaleza electrónica, siendo motivo de impugnación la aportación en formato diferente a este, como por ejemplo en papel, fotocopiadas de un terminal o similares (Por mucho que suene a broma no lo es), como establece David Maeztu en distintos **artículos** al respecto, toda vez que partiendo de la naturaleza jurídica electrónica del elemento a analizar, al desvirtuar la misma por el cambio del soporte , se pierde la prueba en sí misma.

Una vez visto cómo debe aportarse dicha información al procedimiento, con respecto a la geolocalización en sí, debemos diferenciar entre dos tipos de geolocalización en función de su origen:

1) La realizada por los propios operadores de telefonía a través de sus antenas de repetición, conforme a la Ley de Conservación de Datos.

2) La realizada a través de las distintas aplicaciones móviles o el propio terminal, donde a su vez distinguiremos entre las que acreditan o no la información asociada a la geolocalización...

Y sobre las mismas hay que hacer distintas precisiones y referencias:

Respecto a la geolocalización realizada por los operadores de telefonía, dicha solicitud debe venir solicita por un juez y sólo para el supuesto de delitos

graves conforme al Código Penal, conforme al artículo 1.1 de la Ley de Conservación de datos personales:

1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

No obstante, el requisito de la gravedad del delito en su interpretación, difiere bastante entre tribunales, habilitando incluso para el caso de delitos menos graves en función de la trascendencia social del bien jurídico protegido, como en el caso del Auto de 25 de febrero de 2015, aunque no es el tema que nos interesa ahora mismo.

Es la misma Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones., la que en su artículo 3 F la que determina la obligación de almacenamiento de dichos datos de geolocalización.

f) Datos necesarios para identificar la localización del equipo de comunicación móvil:

1.° La etiqueta de localización (identificador de celda) al inicio de la comunicación.

2.° Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

Sobre esto, poco hay que decir, la información con respecto a la ubicación de los terminales móviles conectados a las redes es difícilmente modificable, toda vez que no depende de la información facilitada por el terminal sino de las antenas de repetición sobre las que la información se transfiere, siendo esta información, por tanto, sumamente valiosa en un proceso judicial como prueba, debiendo entenderse esta herramienta como una evidencia con un alto valor probatorio per se, que quedará matizado en función de la distancia sobre la que triangule la información en función de los repetidores y o conexiones wifi en el caso de que las mismas utilicen esta información al respecto.

Sobre los datos de geolocalización derivados de aplicaciones móviles debemos hacer a su vez dos precisiones:

A) Con respecto a lo que serían aplicaciones terceras como las ya comentadas, su validez, desde mi punto de vista no debe ser si quiera indiciaria, toda vez que dicha geolocalización es fácilmente manipulable sin ser ningún experto, conforme explico a continuación.

En el caso de los terminales Android, dicha modificación se puede realizar desde los propios ajustes del terminal, habilitando las opciones de desarrollador, entre las cuales el sistema te permite ya las ubicaciones simuladas, para más detalles echad un ojo **aquí.**

A su vez, Android permite que determinadas aplicaciones como **Fake GPS** o **Fake GPS Location** para conseguir la misma finalidad, poder falsear la geolocalización sobre las aplicaciones del terminal móvil.

En el caso de los terminales de la manzana, Iphone, las posibilidades de falsear la información relativa a la geolocalización también está presente, aunque con la necesidad de tener un Jailbreak en esos terminales (Entendiendo por Jailbreak la operación por la cual se suprimen algunas de las limitaciones impuestas por Apple en dispositivos que utilicen el sistema operativo iOS mediante el uso de kernels modificados

Obviamente, viendo las posibilidades de falseo, y especialmente, la facilidad de llevar a cabo dichas acciones, recomiendo en caso de que se planteen las mismas en un proceso judicial, se proceda a su impugnación por los motivos ya vistos, recayendo en la parte que aporta la prueba, el deber de peritación y acreditación de dicha prueba aportada, conforme a lo determinado por el Tribunal Supremo en la **Sentencia de 19 de mayo de 2015**, como bien explica el compañero Alfredo Herranz en su **blog**, al menos en la vía penal, entendiendo que para órdenes distintos, dada la fundamentación aportada por el Alto Tribunal, debería llevarse el mismo razonamiento, sin que esto a día de hoy con respecto a la prueba electrónica quede claro en otros órdenes, a pesar de la redacción del artículo 326.2 de la Ley de Enjuiciamiento Civil, que parece ir por la misma tendencia.

B) El segundo apartado sobre el que debemos de incidir en el supuesto de apss móviles, son aquellas que a través de sistemas técnicos y o terceros de confianza, acreditan la información de geolocalización del terminal con relevancia en el ámbito legal, y por tanto, en el ámbito probatorio.

En este sentido, hace pocas fechas JAEP, Consultor sobre seguridad informática, en el blog "Un informático en el lado del mal" ha escrito un más que interesante artículo al respecto de este tipo de aplicaciones móviles que acreditan la **geolocalización**, que os recomiendo encarecidamente leer, y del que paso a hacer un breve resumen ya que está estrechamente vinculado a lo que comentamos.

Básicamente, es posible, a través de habilitar el falseo de la geolocalización y las aplicaciones para ello antes mencionadas, siempre que dicha instalación se lleve a cabo en la root del terminal, falsear la información de aplicaciones que aseguran acreditar la información de geolocalización, toda vez que al hacerlo a través de la root o nucleo del terminal, el tercero de confianza no puede sino dar por buena esa información a pesar de ser falsa.

Obviamente, en este caso, la gestión ha sido llevada a cabo por un informático y sí que requiere cierta capacidad técnica como para que tengan la misma consideración probatoria que en el caso de aplicaciones que simplemente usan la geolocalización como herramienta para facilitar información adicional al usuario, no obstante, vistas las posibilidades, tengo que coincidir con el autor que la misma sólo puede ser considerada como indicio, al igual que en el caso anterior, y a su vez, es susceptible de ser impugnada, al menos, en el caso de la

aplicación a la que hace referencia el artículo, toda vez que queda desacreditada su validez, eso sí, con muchas más precauciones que en el caso de las aplicaciones que simplemente toman la información sin ningún medio adicional de acreditación de la misma.

Por todo ello, como es obvio, aún hay mucho que trabajo por hacer a los efectos de acreditar la geolocalización como una prueba plena en el proceso judicial, al menos, dentro del ámbito de las aplicaciones terceras que acrediten dicha información en el proceso.

Rubén VÁZQUEZ ROMERO

Fuente original:
http://mcaconsultores.com/geolocalizacion-practica-probatoria/

PARTE III:
Peritos informáticos y desarrolladores web

11

Érase una vez... un Perito Informático

Carlos Aldama Saínz*

@carlosaldama

Son múltiples los temas a tratar, todos ellos relacionados con la "Validez y Eficacia procesal de Evidencias Digitales", sin embargo uno ve que han participado perfiles de la talla de @josecarmelollb y @notarioalcala (en calidad de Notarios), diferentes abogados y especialistas de la talla de @sergiocm o @D_mas_I, unido a compañeros y amigos como @JagmTwit en calidad de perito informático y se pregunta… ¿No se habrá dicho ya todo?

En primer lugar, toca presentarme, soy Carlos Aldama, Perito Ingeniero Informático. Estoy colegiado en el Colegio de Ingenieros en Informática de Madrid y pertenezco a numerosas asociaciones (ISACA, ALI, APAJCM,…) orientando mi trabajo en exclusiva a la maravillosa labor de los peritajes informáticos y realizando también diferentes cursos y seminarios en universidades y eventos.

No seré yo quien entre a valorar las magníficas y diferentes aportaciones de mis compañeros que han aceptado el reto y que he leído con sumo gusto y que

* Ingeniero Informático por la Universidad Antonio de Nebrija y Bachelor of Science in Computer Science por la Universidad de Wales. Su carrera profesional comienza en 1.996 y desde entonces ha ejercido como consultor, auditor y perito informático, además de ser socio de varias empresas en Madrid relacionadas con las Nuevas Tecnologías y Sistemas Informáticos.

"casi" de manera íntegra también suscribo. Siempre he sido de los que he defendido que el Notario da fe de lo que ve y no garantiza si lo que ve está siendo o no manipulado, sin embargo tras las lecturas de los artículos escritos por dos conocidos "Notarios TIC" en este reto, me queda poco más que reconocer su gran artículo y darles la razón al trabajo que desempeñan, haciendo un pequeño matiz respecto a las diferencias que pueden existir con los peritos ingenieros informáticos que nos dedicamos a esta labor de manera continuada y que creo podemos aportar más valor técnico a la prueba. Si, ya sé que la respuesta a esto es sencilla: Depende del perito que tengamos en frente y depende del Notario, es por ello que me quito el sombrero ante la calidad de los participantes al reto y les doy mi enhorabuena por el trabajo realizado.

Más allá de todo lo anterior, uno siempre se pregunta: ¿Para qué sirve un perito informático? ¿Cuál es su labor principal? ¿Cómo es el trabajo de un perito y que procedimientos usa? Pues bien, sin entrar a hablar de la cadena de custodia en profundidad (tarea realizada de manera excelente por un gran compañero **@JagmTwit**), pasaré a tocar todos los puntos básicos necesarios para realizar una pericia eficaz y que sea plenamente válida en un proceso judicial.

Los peritos siempre nos apoyamos en el Principio de Intercambio de Locard, que decía básicamente que "cada contacto deja un rastro". Siempre existirá una pista o huella que permita realizar el inicio de recogida de evidencias para generar nuestro análisis y sacar conclusiones en nuestra investigación. ¿He dicho SIEMPRE? ¿Seguro que SIEMPRE?…. bueno, dejaremos un "casi siempre" para aquellos que aseguran que en informática TODO es manipulable. Sin embargo debemos pensar que si ya asumimos que toda prueba es manipulable y no deja huella, podríamos muchos de nosotros buscar una nueva profesión. La respuesta a esto es sencilla, nuevamente se debe decir que "todo contacto deja rastro". Podemos escribir artículos indicando que WhatsApp es manipulable y que no deja rastro, sin embargo deberíamos ser coherentes y matizar que para realizar manipulaciones se deben dar una serie de condicionantes y que además tendríamos otros rastros paralelos que nos indicarían obligatoriamente a garantizar la manipulación de la prueba (pongo WhatsApp como ejemplo dado que es del que más se ha escrito últimamente, pero este ejemplo es extensible a cualquier otro soporte digital).

Cada pericia informática siempre es un mundo diferente, casos diferentes, sistemas diferentes, personal diferente…. el único punto que siempre es común a todos ellos es el perito informático que realiza la investigación y la objetividad

a la hora de tratar los datos técnicos que tiene. El perito siempre debe realizar una misma sistemática y esta comienza por algo necesario:

El acotamiento de la escena

Si el perito realiza un acotamiento muy amplio llevará a investigar fuera del objeto deseado, mientras que si el acotamiento es muy estrecho es muy probable que perdamos evidencias importantes.

Una vez realizado correctamente el acotamiento, recopilaremos y garantizaremos de manera segura el traslado de las evidencias para su estudio, siempre preservando todos los datos adquiridos y trabajando con un escenario replicado idéntico al original. En este punto NO estoy hablando únicamente de cadena de custodia de un disco duro con sus clonaciones, HASH, custodia y demás pruebas, estoy hablando en general de CUALQUIER prueba que vayamos a analizar.

¿Se imaginan un análisis de una aplicación sin dar traslado de la misma con garantías a la parte contraria para poder contrastar nuestra prueba? ¿Se entiende un análisis de un terminal móvil sin presentar en formato digital la prueba? Debo recordar que trabajamos con medios digitales y por tanto estos deben ser presentados en su HABITAT ORIGINAL, es decir en formato digital, para dar traslado a la otra parte y que pueda ejercer su derecho a defensa.

¿Es esto siempre posible? Pues nuevamente debo decir que se debe estudiar el caso, pero si hablamos de analizar un software integrado en un sistema que no

se permite extraer, lo que nos debemos plantear es hacer un acotamiento correcto de la prueba y posteriormente poder presentar la prueba de otra manera que no implique "arrancar" la máquina de una cadena de producción y presentarla en el Juzgado… las formulas existen y únicamente queda a criterio de cada perito el pensar la mejor manera de hacerlo (grabar posición y prueba íntegra realizada en vídeo, generando un hash posterior del vídeo ante testigos y posterior custodia del mismo podría ser una de las decenas de opciones que habitualmente se usan para estos casos "extremos").

Llega el momento de ponerse a trabajar en el despacho con la evidencia en nuestra mesa, la cual está correctamente asegurada y nos hemos garantizado que tenemos un clon idéntico. Obviamente sobra decir que habremos tomado todas las medidas necesarias para que no se modifique la prueba. ¿Imaginamos un móvil que estemos examinando y tengo un software de control remoto y nos borren la prueba? Obviamente NO, por ello lo introduciremos en una jaula Faraday mientras se clona el dispositivo para examinar. Ni que decir tiene tampoco las modificaciones "sobre la marcha" de medios digitales… los cuales también deben ser correctamente asegurados y con un sellado de tiempo que nos permita hacer un análisis con garantía… Esta casuística se repetirá con cada caso, cada cliente y cada examen que hagamos, si aquí tenemos problemas y fallamos es mejor que no continuemos con el trabajo.

En este punto es cuando nos encontramos que al comenzar el análisis vemos que las pruebas han sido muchas veces modificadas… ¿Cómo? Muy fácil, hablas con el cliente y te indica que tras la salida del trabajador accedieron al equipo y vieron "sospechas" o bien te indican que tras la ruptura de contrato con el desarrollador de la aplicación, accedieron al código para hacer unas mejoras…. entonces, ¿nos hemos cargado la cadena de custodia y se ha

infectado la prueba? Pues obviamente no es lo deseable, pero es lo más común que nos encontramos y es aquí donde más énfasis tenemos que hacer los peritos, en primer lugar NO ocultándolo y en segundo lugar documentando durante todo el espacio de "rotura" todas las actividades que han realizado y las implicaciones que pueden tener.

Después ya continuaremos con el análisis y entraremos en una eterna lucha de cómo se ha examinado la prueba. ¿Hemos roto el secreto de las comunicaciones? ¿Vulnerado algún derecho fundamental? ¿Estamos haciendo el examen con software forense de garantía? Es aquí donde tenemos que hacer un detallado análisis de todo nuestro trabajo. En primer lugar, es "igual" si el análisis lo hacemos con un software libre o con un software de pago, siempre que este sea forense, sin embargo y por mi experiencia en Juzgados en muchas ocasiones se ha preguntado si he usado software de código abierto. ¿Qué sentido tiene esa pregunta? Pues está claro, el software de código abierto permite manipulaciones y alteraciones en el código, con lo cual puede infectar la prueba. Es por ello que siempre recomiendo que se incorpore el HASH de este tipo de software y se aporte además en formato digital al informe para evitar cualquier problema.

Por otra parte debemos dejar muy claro el tipo de búsquedas que hemos realizado y hasta donde hemos llegado (y de qué manera).

Si tuviera que definir los pasos a realizar para una pericia informática serían los siguientes:

1. Identificación del incidente o proceso a analizar
2. Acotación del entorno a investigar
3. Recopilación de evidencias
    (a) Recuperación de datos
    (b) Aplicación de diferentes técnicas de investigación
4. Preservación de Evidencias
    (a) Almacenamiento de las mismas
    (b) Etiquetado
    (c) Cadena de Custodia
5. Análisis de Evidencias
    (a) Reconstrucción
    (b) Respuestas
6. Documentación y Resultados (Informe Pericial)
7. Ratificación en Juzgado y Defensa del Informe

De todos estos puntos es importante la correcta cadena de custodia y la posterior documentación a realizar en el informe pericial. Un trabajo correcto mal documentado (o viceversa) de nada sirve. Es por ello importante que nuestros informes sean claros en estructura y redacción, haciéndolos entendibles para legos en la materia, pero sin obviar un ápice de tecnicismos necesarios para la descripción correcta de la prueba, recordando además que cada afirmación debe estar correctamente fundamentada.

Dentro del informe deberá figurar claramente la autoría del mismo, dejando este documento correctamente firmado (la firma es la expresión escrita del 335.2 LEC). Particularmente siempre recomiendo una estructura similar a la siguiente:

- Firma de la pericia
- Resumen ejecutivo
- Objeto del encargo (Antecedentes y Objetivos)
- Fuentes de información
- Análisis (SIN conclusiones)
- Limitaciones encontradas para la realización del trabajo
- Conclusiones
- Curriculum del Perito
- Anexos

Con todo lo anterior y medidas prudenciales tendremos nuestro trabajo bien realizado. Ahora bien, no todo en el monte es orégano… Esto no es siempre lo que uno se encuentra en el Juzgado. Desde mi punto de vista y a modo de anecdotario he encontrado detalles que creo que debo resaltar en este artículo para que se tenga prudencia y no se permitan:

· Muchos peritos incluyen la geolocalización de su propio despacho (con mapa incluido) en sus informes, siendo datos irrelevantes y que distraen el foco del trabajo

· Cada vez se hacen más pericias de terminales móviles, sin embargo el 90% de estos informes nunca llevan adjunto un soporte digital o una cadena de custodia especificada.

Los timestamping se realizan abriendo una página de periódico online y haciendo captura de fechas.

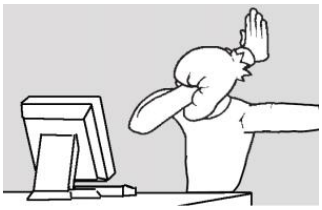
· Se apoyan en la figura del Notario para certificar autenticidad de mails, sin revisar cabeceras, servidores,…

· Se aportan pantallazos de redes sociales sin garantía alguna.

· Aportan datos extraídos de otros equipos que no han sido custodiados correctamente.

· No se comprueba ni contrasta el HASH

Se realizan opiniones no técnicas sobre los resultados obtenidos



Se podría escribir un anecdotario completo y muy extenso de diferentes casos encontrados en Juzgados, no pudiendo pasar por alto temas tan impactantes y dichos en juzgado como los siguientes:

> "Las cadenas de custodia no sirven para nada"
> "¿Clonadora? No, era muy cara, encendí el ordenador y analicé sus datos"
> "Yo simplemente digo lo que me comentó mi abogado que escribiera"
> "No he podido ver el terminal móvil" (tras presentar pericia de autenticidad de WhatsApp)
> "He accedido a la cuenta personal de correo del trabajador, pero eso no lo he puesto en el informe"

…. estas y otras lindezas que ahora pueden sorprender han sido dichas en Sala en los últimos meses y desde luego el resultado ha sido el esperado. Es por ello que además de tener cuidado durante todo el proceso del trabajo, es luego sumamente importante el saber expresarlo en un informe y mucho más el saber ratificarlo, siendo siempre imparcial y claro en el trabajo a realizar.

A modo de finalización de este artículo: PRUDENCIA, SABER HACER y SABER CONTARLO es la máxima que se debe seguir en todo trabajo técnico si queremos que tenga plena validez y eficacia en un proceso judicial.

¿Es necesario el perito ingeniero informático para la presentación de Evidencias Digitales? Es TOTALMENTE recomendable, debido a nuestra preparación y continua formación. Realmente es el mejor aliado que un abogado y un juez se van a encontrar en sala a la hora de defender la validez de unas evidencias digitales.

Carlos ALDAMA SÁINZ

Fuente original:
http://informatica-legal.es/reto-perito-informatico/

12

Cadena de custodia vs mismidad

José Aurelio García Mateos*

@JagmTwit

Todos los profesionales que nos movemos en este mundo relacionado con la Justicia (FCSE, Jueces, Fiscales, Abogados, Peritos, etc.), sabemos ya de la trascendencia y el significado que tiene el término "Cadena de Custodia", pero no está de más que repasemos de nuevo su definición:

Según el portal digital La Ley: *"…La cadena de custodia es el nombre que recibe el conjunto de actos que tienen por objeto la recogida, el traslado y la custodia de las evidencias obtenidas en el curso de una investigación criminal que tienen por finalidad garantizar la autenticidad, inalterabilidad e indemnidad de la prueba…".*

* Ingeniero Técnico en Informática de Sistemas por la Universidad de Salamanca. Es igualmente Diplomado como Perito en "Piratería Industrial e Intelectual" por la Universidad de Valladolid, y por la Escuela de Criminología de Cataluña. Además es Auditor y Perito Informático, titulado por la Universidad de Ávila. Compagina su carrera profesional como desarrollador de sistemas de interconexión de redes seguras y Cloud Computing, con la del Despacho de Auditoría y Peritaje Informático de Salamanca. Es además vicepresidente de la Asociación Nacional de Ciberseguridad y Pericia Tecnológica (ANCITE). Ha sido administrador de sistemas UNIX y profesor experto en diversas áreas de programación y sistemas computacionales, impartiendo cursos en colaboración con varios organismos estatales y privados.

Si nos acogemos a la definición ofrecida por la Wikipedia, podríamos definir la CdC como *"…el procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis, normalmente peritos, y que tiene por fin no viciar el manejo que de ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones…"*.

Sigue diciendo Wikipedia que *"…Desde la ubicación, fijación, recolección, embalaje y traslado de la evidencia en la escena del siniestro, hasta la presentación al debate, la cadena de custodia debe garantizar que el procedimiento empleado ha sido exitoso, y que la evidencia que se recolectó en la escena, es la misma que se está presentando ante el tribunal, o el analizado en el respectivo dictamen pericial…"*.

Quisiera destacar aquí tres frases referenciadas más arriba y que considero esenciales en el proceso de elaboración de la Cadena de Custodia. Esto es:

1. Ha de garantizarse la indemnidad de la prueba
2. Han de evitarse alteraciones, sustituciones, contaminaciones o destrucciones, y
3. La evidencia que se recolectó en la escena ha de ser la misma que se está presentando ante el tribunal.

En las tres definiciones expuestas anteriormente se llega a la misma conclusión: la cadena de custodia es necesaria no solo para dejar constancia sobre qué se ha hecho con la prueba (en nuestro caso, con la evidencia electrónica), y en qué manos ha estado, desde que se recolecta hasta que llega a manos de Su Señoría, sino que además ha de acreditar que lo que justamente llega al Juzgador –e incluso a la parte contraria, no nos olvidemos nunca-, ha de ser necesariamente lo mismo que lo que se recolectó en su día. Es decir: ha de acreditarse el denominado "principio de mismidad de la prueba", del que no tantos profesionales (reconozco que muchos de ellos pertenecientes al ámbito de la pericial informática), son conocedores.

Por tanto, la cadena de custodia –al menos en informática- tiene la dificilísima misión de asegurar que la prueba que se presenta en el litigio es exactamente la misma que la obtenida en su día y de la que se extrajeron los datos relevantes presentados para el juicio en cuestión, de tal forma que permita a la parte contraria realizar sus propias pruebas –o incluso realizar las mismas que practicó el primer perito-, con la plena garantía de que "aquello con lo que trabaja es lo mismo que aquello que se intervino".

Llegados a este punto me atrevo a decir que (al menos en informática), "quizá ya no importa tanto –aunque sigue siendo un dato esencial-, quién ha custodiado la prueba, o dónde ha quedado ésta guardada, como el estar plenamente convencidos de que la prueba no ha sido alterada", cosa por otra parte que puede ocurrir con suma facilidad. Doy un ejemplo: el mero hecho de introducir un disco duro, o un pendrive, en un puerto USB controlado por Windows altera la prueba sin remedio… A no ser que se tomen las debidas precauciones para garantizar la imposibilidad de escritura en estos dispositivos, como bloquear los puertos USB, o configurarlos mediante hardware (en aquellos dispositivos donde se pueda, claro), mediante switches, etc, como los que llevan los adaptadores de tarjetas MMC.

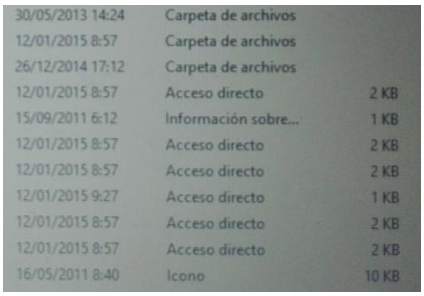
Volviendo al principio de mismidad, éste viene a decir que (tomado del Auto 2197/2012, del TS), *"…es necesario tener la completa seguridad de que lo que se traslada, lo que se mide, lo que se pesa y lo que se analiza es lo mismo en todo momento, desde el instante mismo en que se recoge del lugar del delito hasta el momento final en que se estudia y destruye…".*

En este auto se menciona que el gran problema que plantea la cadena de custodia es justamente garantizar que desde que se recogen las evidencias (en nuestro caso, digitales), relacionadas con el delito, hasta que éstas llegan a concretarse como prueba en el momento del litigio, el elemento sobre el que recaerán los principios de inmediación, publicidad y contradicción, tanto de las partes como de los juzgadores, es el mismo.

Y aquí viene la pregunta –al menos en informática-, ¿Cómo sabemos, en el momento en que realizamos nuestra práctica forense, que estamos ante lo mismo que se recolectó en su día? Tomemos el ejemplo con un Disco duro: por muchas fotos que podamos hacerle, por muchos listados de ficheros que podamos sacar, el contenido de esos archivos puede modificarse, respetando la

fecha, la hora y el tamaño en bytes, sin mayor dificultad. No en vano, la información almacenada "no es visible", salvo que se abran los ficheros.

Cabe la posibilidad (muy recomendable), de que un Notario certifique que "existe tal fichero, con tal extensión, creado en tal fecha y a tal hora", pero éste podría ser alterado de forma parcial, o completamente, sin mayor dificultad; nadie podría acreditar entonces que lo que está depositado en dependencias notariales es lo mismo que se obtuvo en su momento. Cierto que no es algo que ocurra con frecuencia pero, desde luego, sí es algo que podría ocurrir.



Con todo, lo que sí podría suceder –y de hecho sucede-, es que durante la fase de recopilación de pruebas, la evidencia se altere sin remedio, perdiendo ese principio de mismidad. Esto podría ocurrir por el simple hecho de que el dispositivo a analizar tenga un troyano (software malintencionado), o un virus que se replique por la máquina o el propio disco duro externo, en caso de carecer de antivirus el ordenador del analista, en el momento en que es conectado. Y en el supuesto de que el ordenador con que se analice el dispositivo externo tenga instalado un antivirus, esta herramienta chequeará ese dispositivo y eliminará de forma automática las formas víricas que encuentre, suprimiendo información que –aunque en el caso forense "suele" no ser importante-, alterará de forma irremediable el principio de mismidad. Más grave es aún el hecho de conectar a un ordenador un disco duro externo de tecnología SSD (de estado sólido), pues la orden "TRIM"-por la que el sistema operativo comunica al disco SSD qué bloques de datos ya no están en uso-, recoloca la información, de tal forma que borra los datos de los sectores marcados con información marcada para borrar, ya sea por inservible o eliminada intencionadamente.

Como vemos, es muy fácil alterar la prueba, o muy complicado preservar su inalterabilidad. El ejemplo de la imagen anterior (un disco duro intervenido en 2012, pero en el que se aprecian ficheros y directorios generados en años

posteriores), demuestra que "el hecho de que un elemento esté perfectamente custodiado –e incluso precintado-, y de que se sepa en todo momento quién ha tenido acceso al dispositivo, o qué ha hecho con éste-, no significa que la prueba mantenga su carácter de inalterabilidad, pues la evidencia puede haber sido desprecintada en un momento y vuelto a precintar posteriormente.

Esta es la tesis en que nos basamos para afirmar que "La cadena de Custodia no garantiza el principio de mismidad".

Sin embargo, y por suerte, las nuevas técnicas y tendencias en forense informática están evolucionando y por ende, dando solución a muchos de los problemas existentes hasta hace relativamente poco tiempo.

La gran ventaja que tiene la evidencia informática es que ésta puede ser reproducible tantas veces como se precise, conservando tanto el original como las copias información idéntica. A este proceso se le llama clonación, o duplicado "bit a bit" de los datos del dispositivo. Además, existen herramientas que permiten calcular los denominados "HASH", o funciones matemáticas que generan una cadena alfanumérica única hexadecimal (compuesta por números del "0" al "9" y letras de la "a", a la "f"), en función de un algoritmo establecido (MD5, SHA1, SHA2, etc. –el Md5 se considera obsoleto-), de tal forma que, si se cambia un simple bit en el dispositivo, el nuevo cálculo del HASH devolverá una cadena hexadecimal diferente.

Existen en el mercado, desde máquinas "clonadoras", capaces de crear varias copias idénticas en un mismo acto –calculando incluso el Hash de los datos-, hasta software específico que permite bloquear los puertos USB o SATA (los de los datos de los discos duros internos), contra escritura, de tal forma que se pueda duplicar/leer información de los dispositivos, con plena garantía de inalterabilidad de su contenido.

En cualquier caso, y como más vale prevenir que curar, el procedimiento que ha de seguirse a la hora de acceder y tratar las evidencias electrónicas debe ser siempre el mismo: clonar la información o, en su defecto, crear imágenes exactas del contenido (una imagen del contenido de un pendrive, por ejemplo, suele almacenarse en un fichero con extensión .img, o .dd, según sea la aplicación que crea el fichero que almacena los datos y la estructura exacta del dispositivo), tras lo que será preciso calcular los hashes de ambos elementos, el origen y el destino. En caso de que se trate de una imagen habrá que calcular igualmente el HASH de la misma. Por otra parte habrá que realizar –al menos-, dos copias idénticas del dispositivo de origen, de tal forma que no sea preciso acceder a éste de nuevo, y así trabajar con la segunda copia, preservando la primera como fuente, en el supuesto de que sea preciso clonar de nuevo. No obstante, siempre que se realice un nuevo duplicado habrá que calcular el HASH, para dejar constancia de que –una vez más-, estamos trabajando "con lo mismo que había al principio".

Todo esto, evidentemente, asegurándonos de que en caso de que no podamos hacer las clonaciones vía Hardware con máquinas clonadoras dedicadas y de que tengamos que realizar la copia utilizando programas informáticos, los puertos USB estén debidamente protegidos contra escritura, ya sea mediante parámetros del propio sistema Operativo bajo el que se realice la operación de copia, o por medio del programa que la va a efectuar. Un ejemplo sencillo de cómo pueden bloquearse los puertos USB contra escritura puede consultarse en **este artículo** de nuestro blog **www.informaticoforense.eu**

Concluyendo:

La cadena de custodia es un procedimiento fundamental que hay que establecer dentro del proceso de aseguramiento de la prueba, pero por sí misma no garantiza la inalterabilidad de la evidencia electrónica.

Existen multitud de herramientas, tanto de hardware como de software, que nos permitirán hacer copias idénticas de los dispositivos originales, o imágenes de éstos que se guardarán en un fichero, para su posterior recuperación y evaluación.

Lo único que garantiza (en informática), que la evidencia digital no ha sido alterada a lo largo de su vida (que comprende desde que es recolectada, hasta que ya no se precisa y se destruye), es su huella digital, su HASH, que variará en el momento que se modifique un simple bit de información.

Antes de hacer una clonación hay que asegurarse de que no hay posibilidad de alterar la evidencia original, ya sea mediante el bloqueo de puertos contra escritura, o haciendo copias (la opción más recomendable), bit a bit, mediante clonadoras diseñadas a tal efecto.

Como siempre ocurre en informática, todo es infinitamente diferente, dependiendo de si es cero, o es uno.

José Aurelio GARCÍA MATEOS

Fuente original:
http://www.informaticoforense.eu/custodia-vs-mismidad/

13

La necesidad de evidenciar lo evidente

Óscar Domínguez Merino*

@oscardom78

No podía dejar la oportunidad de participar también en el **#Reto2JCF** que con gran entusiasmo anunciamos hace unas semanas desde el **segundo desafío legal de Juristas con Futuro**. Por un lado, porque mi profesión así me lo obliga. Por otro lado, porque mi compromiso como miembro del equipo de Juristas con Futuro así me lo requiere. Y, por último, porque mi pasión y devoción por la informática y lo digital así me lo pide. Así que, aquí dejo mi evidente contribución.

Si algo he sacado en claro en todos mis años profesionales es que, **en lo que a informática se refiere, cualquier elemento es manipulable**. Todo aquello que pueda ser manipulado, más tarde o más temprano se manipulará, directa o indirectamente, con intención o sin ella. Esto es algo evidente.

---

* Experto en Posicionamiento Web (SEO) y Optimización Web (WPO). Desarrollador Web e informático de profesión y devoción. Como programador, ha desarrollado cientos de aplicaciones de escritorio de diferente índole, tanto para empresas como para organismos públicos de España. Actualmente compagina su trabajo como profesional independiente con el trabajo para 3 de las empresas locales más punteras en materia de artes gráficas, fotografía, desarrollo web y marketing online. Ha publicado varios artículos sobre SEO y marketing online en diferentes portales de Internet, destacando su blog personal y profesional en http://www.oscar-dominguez.com/blog/ Ha participado en numerosos proyectos web, sigue participando en otros tantos y seguirá haciéndolo. Apasionado del mundo de Internet y el Marketing Online es el Director Técnico de Juristas con Futuro.

Al fin y al cabo, cualquier dispositivo electrónico (un ordenador, una tablet, un smartphone, un gps, un ipod, una cámara digital, etc.) tiene ficheros almacenados en su disco duro o en su memoria que le permiten funcionar y realizar aquello para lo que fueron programados. Sean como sean dichos ficheros, su aspecto, formato, diseño o tamaño, al final sólo son ficheros. Y todo fichero, de una forma o de otra, puede copiarse, moverse, borrarse y editarse.

Cierto es que existen medidas de seguridad que dificultan la manipulación de cualquier fichero. Medidas que cada vez son más difíciles de saltar. Y digo más difíciles y no infranqueables. Cansados estamos de ver y escuchar miles de casos de pirateo desde que la sociedad es más digital y tecnológica. Viajemos un momento al pasado.

Seguro que muchos recordaréis **aquellas viejas casetes donde los artistas de los 70 y 80 editaban y publicaban sus nuevas obras musicales y que podían ser copiadas**, replicadas de forma idéntica. Sólo necesitabas comprar una casete "virgen" o vacía y disponer de una cadena de alta fidelidad con doble pletina: una para reproducir la casete original y la otra, donde se introducía la casete vacía, para grabar lo que se reproducía en la primera. Comprar la casete vacía era fácil. Disponer de doble pletina ya era otra cosa, pues sólo algunos privilegiados disponían de una en sus casas. Podíamos decir que esto ya era piratería.

Las viejas cintas de casete donde grabábamos nuestras canciones favoritas.
Resultaba evidente que se crearon para crear réplicas.

Con la aparición de los CDs **en la década de los 80 y 90** ocurrió lo mismo. Al principio, sólo se podían pasar a casetes para tener una copia del álbun musical. En cuanto las grabadoras de CD de los ordenadores estuvieron a un precio bastante asequible para la mayoría de usuarios, **la copia de CDs piratas se disparó**, lo que hizo temblar los cimientos de la industria musical. En aquellos tiempos, ya se pirateaban juegos de ordenador, cuya seguridad era mínima o, en ocasiones, nula. Luego apareció el "top manta" famoso, que aún vemos por algunas playas de la costa española.

Con la entrada del nuevo siglo XXI, la tecnología ha seguido avanzando de forma exponencial a través de su propio camino que se vislumbra como interminable. Nuevos dispositivos, nuevas tendencias, nuevo software, nuevas aplicaciones, nuevos chips, nuevas máquinas… Portátiles, videoconsolas, tablets, smartphones, GPSs… Todos, todos, con una parte física y una parte electrónica y digital. Todos manipulables.

¿Quién no ha oído a amigos o a familiares que buscaban a alguien que les pirateara la Wii, la Play o la Nintendo, o que, sencillamente, les bajara de Internet no sé qué programa pirata para el ordenador? El problema ha llegado hasta los vehículos, ¿o acaso no recordáis **el reciente caso de la manipulación que hizo el fabricante Volkswagen** a algunos de sus modelos?

Creo que la piratería, por mucho que nos pese, va ligada a la informática por naturaleza. Simplemente por el hecho del poder que otorga la manipulación de controlar una máquina y cambiar su comportamiento. Y el pirata informático, más elegantemente denominado *hacker*, nunca saciará su sed de manipular. Todos sabemos que en cuestión digital, más tarde o más temprano, alguien copiará o manipulará un producto que acaba de salir al mercado. Sólo es cuestión de tiempo.

Y es este escenario tan manipulable y aparentemente falso donde **el sector jurídico tiene un hueso duro de roer**. ¿Qué es real? ¿Qué es falso? ¿Qué está manipulado y qué no? ¿Podemos creer lo que perciben nuestros sentidos? ¿Confiamos en que las máquinas están programadas para funcionar como deben? ¿Quién asegura y da validez a todo esto?

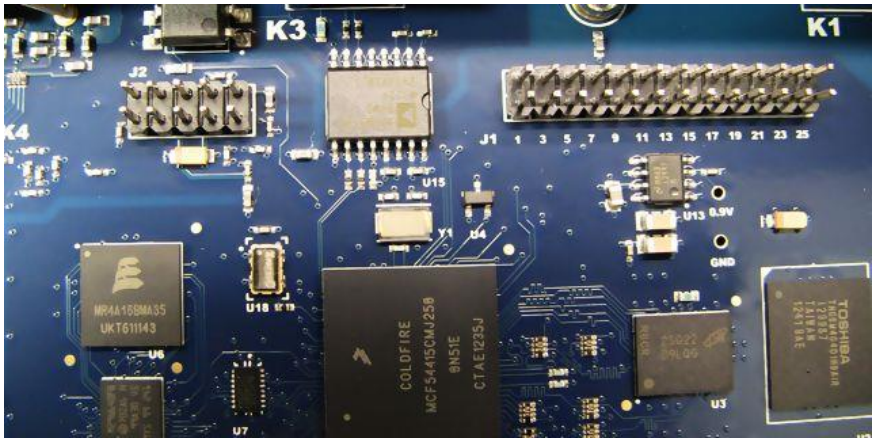
Se conocen claros ejemplos de manipulaciones de teléfonos, donde el emisor no es realmente el emisor; de aparatos GPS que mandan coordenadas de una ubicación por donde jamás pasaron; de correos electrónicos enviados por

emisores que jamás tuvieron email; de fotografías que muestran una escena que nunca sucedió; de vídeos que muestran una secuencia de imágenes que nunca tuvieron lugar… Manipulaciones, manipulaciones y más manipulaciones.

En un proceso judicial, aportar cualquiera de estas supuestas evidencias digitales como prueba aclaratoria es intrascendente. Resulta evidente. Ya sucede en muchos tribunales que **basta que la parte contraria demuestre que cualquier fichero digital es manipulable y que pueda estarlo** para echar abajo cualquier prueba documental de algo digital.

Si una prueba se basa en lo que dictamina una máquina, ¿quién certifica que esa máquina no estaba ya manipulada cuando realizó su dictamen? Si una aplicación informática genera un informe sobre la veracidad de un fichero, ¿quién certifica que esa aplicación no ha sido también manipulada por quien la desarrolló o quien dice que ese fichero que debe verificarse no es el original y ya se encuentra manipulado? ¿Quién controla qué está o no está manipulado? Y si hay un controlador, ¿quién dice que dicho controlador no pueda estar también manipulado?

En efecto, todo esto es de locos. Pero lo que está claro es que la sociedad demanda, cada vez más, soluciones y mediaciones a problemas judiciales en escenarios totalmente tecnológicos o digitales: insultos, amenazas, difamaciones en redes sociales; suplantación de identidad digital; delitos tecnológicos, etc. No queda más remedio que disponer de mecanismos certificados que ayuden a encontrar una solución a este nuevo escenario legal que aumenta cada año, al igual que aumenta la tecnología.



Cualquier dispositivo electrónico o digital puede ser manipulado. Por lo tanto, deja de ser "evidente".

Considero que habrá casos en los que demostrar según qué actos sea imposible y demasiado costoso. Reciente es el caso de la **negación del fabricante Apple de ceder al FBI el acceso a uno de sus dispositivos** en una investigación. Yo me pregunto, ¿sería aceptada la petición de un juez español a Facebook, Twitter o Google a que certificaran el contenido, la fecha y la hora de cualquier actividad de una persona que les fuera solicitada? Sinceramente, creo que dicha solicitud se perdería en el olvido. Recordemos que los servidores de estos gigantes de Internet se encuentran en países donde la legislación es diferente y no se aplica de la misma manera.

Lo mismo ocurre con WhastApp o con cualquier otra aplicación de mensajería instantánea. Por lo tanto, **la carga de prueba recae sobre quien presenta la conversación o publicación como prueba documental**, donde la presentación en papel ya no es suficiente ni evidente. Aquí se abre una posible vía que consiste en solicitar una prueba pericial, que, dado su alto coste y su extensa y compleja realización, así como la demora de su ejecución, es evidente que la hacen casi inviable.

Respecto a los peritos informáticos tengo que decir que cuentan con todo mi respeto y apoyo, pues soy conocedor de lo duro que es llegar a desempeñar dicha profesión (muchos años de estudio de diferentes carreras y especialidades). Me gustaría conocer cómo trabajan, qué herramientas usan y que procedimientos emplean para realizar sus comprobaciones y dar validez a lo que investigan y descubren. Pongo un ejemplo e invito a peritos informáticos a aportar su opinión o comentario. Quiero leer vuestros comentarios y, sobre todo, vuestros blogs, trabajos y proyectos.

Si un perito informático tiene que dar validez, por ejemplo, a los **metadatos de una fotografía digital**: ¿el software que utiliza para extraer los metadatos tiene una certificación de que funciona correctamente y no pueda manipular los datos extraídos? Ese software, ¿detecta si la foto a comprobar es la original o, suponiendo que sea la original, si los metadatos que posee dicha foto ya han sido manipulados con anterioridad? ¿Y si la cámara desde donde se realizó la fotografía ya estaba manipulada? ¿Es detectable todo esto? ¿Qué porcentaje de validez o certificación sobre un elemento puede alcanzarse? ¿Se puede dictaminar que un fichero digital es tal como se creó al 100%?

Entonces, ¿existe alguna solución? En mi humilde opinión, para suplir la necesidad surgida de evidenciar lo aparentemente evidente y la única forma de

validar y certificar acciones de este tipo es a través de un tercero de confianza oficial acreditado, quien se encargue de poner los medios y mecanismos necesarios para salvaguardar la autenticidad de cualquier fichero digital. ¿Cómo hacerlo? Enviando el fichero creado en el mismo instante de su creación al certificador, quien lo custodiará de forma segura en un estado inalterable.

Hoy en día, **en España existen 25 Prestadores de Servicios de Certificación supervisados y acreditados por el Ministerio de Industria, Energía y Turismo del Gobierno de España**. No quiero pensar en la inversión tecnológica que han tenido que realizar para ello, sobre todo en cuanto a material tecnológico (servidores, instalaciones seguras, certificados, ordenadores, informáticos, etc…). Aunque también es cierto que existen otras entidades capacitadas en certificar digitalmente cualquier elemento que pueda ser considerado como prueba, por ejemplo, peritos, notarios, la policía o la misma guardia civil.

Pero lo que sí es cierto es que ellos son los únicos que pueden certificar y dar validez a cualquier fichero digital que les llegue mediante los mecanismos creados para tal fin. Por lo tanto, en un proceso judicial, son los únicos que pueden asegurar la autenticidad o no de cualquier prueba digital, que pasará a ser una **evidencia digital**.

Como vemos, evidenciar lo que parece evidente no es tan fácil cuando nos movemos en el mundo digital, un mundo propenso a ser manipulado. Todavía queda mucho camino que recorrer. La tecnología avanza muy deprisa y la sociedad se adapta casi al mismo ritmo. Pero no así el sector jurídico.

En un estado de derecho, es necesario cubrir todos los escenarios posibles para poder defender los derechos de los ciudadanos en cualquier ámbito y circunstancia. A día de hoy, lamentablemente, esto queda todavía muy lejos.

Con estas líneas, doy por finalizada mi contribución a este desafío legal, invitando a todos los participantes en el mismo a aportar su opinión y comentario respecto a este artículo que acaba de leer. Creemos debate.

Óscar DOMÍNGUEZ MERINO

Fuente original:
http://www.oscar-dominguez.com/blog/informatica/la-necesidad-evidenciar-lo-evidente/

PARTE IV:
Prestadores de Servicios de Confianza

14

Los servicios de confianza y la prueba electrónica

Nacho Alamillo Domingo*

@NachoAlamillo

El **Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014**, relativo a la **identificación electrónica y los servicios de confianza** para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (en adelante, "**Reglamento eIDAS**") establece, a tenor de lo dispuesto en su artículo 1, apartados b) y c), **normas para los servicios de confianza**, en particular para las **transacciones electrónicas**, así como un marco jurídico para las **firmas electrónicas**, los **sellos electrónicos**, los **sellos de tiempo electrónicos**, los **documentos electrónicos**, los **servicios de entrega electrónica certificada** y los **servicios de certificados para la autenticación de sitios web.**

Para el **Reglamento eIDAS**, un **servicio de confianza** es "el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en: a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o b) la creación, verificación y validación de certificados para la autenticación de sitios web, o c) la

* Abogado experto en identidad digital, firma electrónica, administración electrónica y Derecho de las TIC. Actualmente es General Manager en Astrea La Infopista Jurídica S.L. y CISO & Innovation Manager de eLogalty. Vicepresidente de MiFirma.com. Ha escrito varias publicaciones como se puede comprobar en su perfil de LinkedIn.

preservación de firmas, sellos o certificados electrónicos relativos a estos servicios" (artículo 3 (16) del Reglamento eIDAS).

Algunos de estos servicios ya habían sido **regulados de forma previa** por la 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 (en adelante, "DFE"), y que el Reglamento eIDAS deroga a todos los efectos a partir de 1 de julio de 2016, desplazando también las normas nacionales que se opongan o resulten incompatibles con el citado Reglamento eIDAS; en España, la Ley 59/2003, de 19 de diciembre (en adelante, "LFE"), que deberá adecuarse urgentemente.

En concreto, la DFE crea un marco jurídico para la firma electrónica y para determinados servicios de certificación con el fin de garantizar el correcto funcionamiento del mercado interior; indicándose en el considerando (3) del Reglamento eIDAS que la Directiva *se refiere a las firmas electrónicas, sin ofrecer un marco global transfronterizo e intersectorial para garantizar unas transacciones electrónicas seguras, fiables y de fácil uso. El presente Reglamento refuerza y amplía el acervo que representa dicha Directiva.*

Aunque la Directiva no contiene una definición de **servicio de certificación**, lo caracteriza cuando indica que un *proveedor de servicios de certificación es la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica*, en una concepción muy amplia.

Quizá la Directiva ha tomado esta denominación, que en algunos casos ha resultado confusa, porque la **firma electrónica reconocida**, que es la que recibe mayor efecto jurídico, se debe basar de forma necesaria en un **certificado electrónico reconocido**. Desde luego, la prestación de servicios como el sellado de la fecha y hora de una firma electrónica, o la generación, validación o custodia de una firma electrónica no parece tener nada que ver con los certificados electrónicos, por lo que su inclusión en este concepto resulta extraña, y más cuando la Directiva no establece obligaciones para dichos servicios.

En cambio, la denominación de **servicio de confianza** contenida en el Reglamento eIDAS constituye una *evolución* y, al tiempo, **ampliación semántica** sobre la denominación de **servicio de certificación**, y se fundamenta en el hecho de que estos servicios permiten aportar confianza a los

procesos de negocio en los que se emplean, en gran medida gracias a los efectos jurídicos que se asocian a dichos servicios.

Muestra de ello es que la exposición de motivos del **Reglamento eIDAS** manifieste que *el presente Reglamento se propone reforzar la confianza en las transacciones electrónicas en el mercado interior proporcionando una base común para lograr interacciones electrónicas seguras entre los ciudadanos, las empresas y las administraciones públicas e incrementando, en consecuencia, la eficacia de los servicios en línea públicos y privados, los negocios electrónicos y el comercio electrónico en la Unión* (Considerando (2) del Reglamento eIDAS), para lo cual se precisa ir más allá de la regulación de firma electrónica, la cual no ofrecía "un marco global transfronterizo e intersectorial para garantizar unas transacciones electrónicas seguras, fiables y de fácil uso" (Considerando (3) del Reglamento eIDAS).

El artículo 3 (16) del **Reglamento eIDAS** no contiene, propiamente, una definición o concepto de servicio de confianza, sino más bien una enumeración de servicios de la sociedad de la información que, precisamente por ser incluidos en dicha lista cerrada, se consideran "**de confianza**". Podríamos conceptualizar los servicios de confianza como aquellas tecnologías en las que se puede confiar, por lo que modifican la percepción del usuario con respecto a la vulnerabilidad de un proceso al que se incorporan. Para ello, el usuario debe poder reconocer un servicio de confianza, de hecho, como suficientemente confiable.

Para ello, la aproximación del **Reglamento eIDAS** es la creación de un nivel reforzado de servicios de confianza, lo cual no deja de llamar la atención, en el sentido de que realmente la confianza en dichos servicios parece nacer el hecho de que los mismos se encuentran regulados, más que de sus propias características técnicas. Y en este sentido, el artículo 3 (17) del Reglamento eIDAS nos aporta la noción de un "servicio de confianza cualificado", que define como "un servicio de confianza que cumple los requisitos aplicables previstos en el presente Reglamento", distinción relevante porque permite establecer, con carácter general, dos niveles de servicios "de confianza":

· El ***nivel ordinario*** *de servicio de confianza*, que no se encuentra prácticamente regulado, y que no recibe ningún reconocimiento legal en particular; y en cuyo caso, el usuario debe construir su propio estado interno de confianza respecto al servicio; por ejemplo, puede reconocer una contraseña de su entidad

financiera como suficientemente segura, pero no un servicio de almacenamiento de documentos en la Nube.

El ***nivel cualificado*** *de servicio de confianza*, que sí se encuentra altamente regulado, y que recibe un reconocimiento particular de efectos legales, lo cual debería suponer un incentivo a su adopción (aunque en realidad, la dificultad de demostrar que un servicio es realmente cualificado puede llegar a eliminar todo el incentivo que ofrece el "reconocimiento" legal del servicio cualificado, lo cual se intenta solventar mediante la imposición de la evaluación de la conformidad del servicio).

En este caso, este *reconocimiento legal explícito* es el que permite al usuario reconocer el servicio como confiable, por lo que podemos asumir que estos servicios se desarrollarán antes y en mayor volumen que los que no gocen de esta condición; aunque podría tratarse de una apuesta arriesgada, dada la experiencia previa de la firma electrónica reconocida, que ha tenido una escasa adopción, por inhibidores de diversos tipos. En efecto, hay que reconocer que el mayor uso de la firma electrónica basada en certificado electrónico se observa en los escenarios donde la Administración ha impuesto este mecanismo (como en el ámbito tributario) o bien ha ofrecido un incentivo extra para su uso (para habilitar usos privados como la factura electrónica, por ejemplo).

Es preciso también comentar que el **Reglamento eIDAS** contiene una lista cerrada de servicios de confianza, al objeto de delimitar el alcance de la regulación uniforme europea, pero que los Estados miembros pueden definir otros servicios de confianza, así como mantener (o introducir) disposiciones nacionales, acordes con el Derecho de la Unión, relativas a los servicios de confianza, siempre que tales servicios no estén plenamente armonizados por el presente Reglamento, consideraciones que muestran el objetivo central de la regulación, que no es otro que garantizar la libre circulación de estos servicios en el mercado interior, mediante un conjunto mínimo de normas armonizadas (cfr. el Considerando (24) del **Reglamento eIDAS**), algo que desde luego no sucede en la actualidad, al menos en términos prácticos.

Los *servicios de confianza* presentan una relación evidente con la prueba electrónica, como reconoce el Considerando (22) del Reglamento eIDAS cuando indica que *para contribuir al uso transfronterizo general de los servicios de confianza, debe ser posible utilizarlos como prueba en procedimientos judiciales en todos los*

Estados miembros, pero también que *corresponde al Derecho nacional definir los efectos jurídicos de los servicios de confianza, salvo disposición contraria del presente Reglamento*.

En este sentido, el **Reglamento eIDAS** establece lo siguiente:

· En relación con la **firma electrónica**, el artículo 25.2 determina que "una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita", mientras que el epígrafe 1 del mismo artículo ordena que "no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada". En todos los casos, en aplicación de los principios de equivalencia funcionalidad, una firma electrónica puede ser equivalente a una firma manuscrita, diferenciándose la firma electrónica cualificada de las demás porque la misma es directamente equivalente a la firma manuscrita, por mandato legal, mientras que en las restantes firmas electrónicas eventualmente se deberá probar su idoneidad, en función del caso concreto.

En relación con la nueva institución del **sello electrónico**, que el **Reglamento eIDAS** construye como analogía de la firma electrónica pero reservada en exclusiva a las personas jurídicas, el artículo 35.2 determina que "un sello electrónico cualificado disfrutará de la presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado". De nuevo, el epígrafe 1 del mismo artículo ordena que "no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos del sello electrónico cualificado".

Nótese como, **a diferencia de la firma electrónica cualificada**, cuyo efecto realmente es sólo *ser equivalente a* una **firma escrita** (sean sus efectos los que sean en cada legislación), en cambio para el **sello** se definen exactamente los efectos jurídicos concretos, entre los que, por cierto, no parece incluirse la idoneidad para la producción de declaraciones de voluntad, algo que, de ser interpretado en términos excesivamente estrictos, podría limitar enormemente su uso más allá de la remisión de documentación a terceros. No debería ser el caso, dado que el Considerando (59) del Reglamento eIDAS indica que "los sellos electrónicos deben servir como prueba de que un documento electrónico ha sido expedido por una persona jurídica, aportando certeza sobre el origen y la integridad del documento", y además, a diferencia de la firma electrónica, el

Reglamento eIDAS considera que, además de autenticar el documento expedido por la persona jurídica, los sellos electrónicos pueden utilizarse para autenticar cualquier activo digital de la persona jurídica, por ejemplo, programas informáticos o servidores (Considerando (65) del Reglamento eIDAS).

El reto, por tanto, aparece por la **posible inaplicabilidad** del principio de equivalencia funcional; en efecto, en tanto en cuanto no siempre existen normas sobre el uso de los sellos físicos de personas jurídicas, se generarán dudas razonables acerca de la posibilidad de emplear su correlato electrónico, como por ejemplo en la contratación. Se trata de toda una oportunidad de innovación jurídica, tanto en las relaciones *inter privatos*, donde se podrá estipular lo que se considere oportuno, cuanto en la regulación aplicable a determinadas categorías de negocios jurídicos privados, cuanto en los procedimientos administrativos y judiciales.

Dado que en la **autenticación de fuentes de prueba electrónica** – sea ésta documental o pericial – mediante **sello electrónico** no requiere de la actuación directa del apoderado de la persona jurídica, cabe esperar una fuerte adopción del sello electrónico, por lo que, con una cierta ironía, el Considerando (58) del Reglamento eIDAS parece instituir un principio de no discriminación del apoderado, cuando indica que "cuando una transacción exija un sello electrónico cualificado de una persona jurídica, debe ser igualmente aceptable una firma electrónica cualificada del representante autorizado de la persona jurídica".

· En relación con la **nueva institución del sello de tiempo electrónico**, que no está regulado en la DFE ni en la LFE, el artículo 41.2 determina que *los sellos cualificados de tiempo electrónicos disfrutarán de una presunción de exactitud de la fecha y hora que indican y de la integridad de los datos a los que la fecha y hora estén vinculada*s, mientras que el epígrafe 1 del propio artículo ordena que *no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello de tiempo electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos de sello cualificado de tiempo electrónico*. Se trata de un servicio que aporta un gran valor a los procesos de negocio con relevancia probatoria, así como a las técnicas de generación de registros de actividad (*logs*) y a la denominada **cadena de custodia**, por lo que entendemos que está llamado a jugar un papel fundamental en la prueba electrónica no documental y, especialmente, en la pericia informática.

Finalmente, en relación con la nueva institución de la **entrega electrónica certificada**, que englobaría las frecuentemente denominadas notificaciones privadas electrónicas, el artículo 44.2 determina que *los datos enviados y recibidos mediante un servicio cualificado de entrega electrónica certificada disfrutarán de la presunción de la integridad de los datos, el envío de dichos datos por el remitente identificado, la recepción por el destinatario identificado y la exactitud de la fecha y hora de envío y recepción de los datos que indica el servicio cualificado de entrega electrónica certificada*, mientras que el epígrafe 1 del mismo artículo ordena que *a los datos enviados y recibidos mediante un servicio de entrega electrónica certificada no se les denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales por el mero hecho de que estén en formato electrónico o no cumplan los requisitos de servicio cualificado de entrega electrónica certificad*a.

Para los restantes servicios de confianza, el **Reglamento eIDAS** *no establece efectos jurídicos ni menos aún presunciones*, incluso aunque los mismo sean *cualificados*. En todos los casos, hay que decir que el Reglamento eIDAS no altera las reglas de la carga de la prueba, que corresponde determinar al legislador nacional, por lo que sigue siendo preciso demostrar que una firma electrónica de persona física, sello electrónico de persona jurídica, sello de tiempo electrónico o cualquier otro servicio de confianza realmente es cualificado, como condición previa para que se produzcan los efectos legalmente previstos (equivalencia con la firma manuscrita o presunción de autenticidad correspondiente).

En este sentido, la innovación principal del **Reglamento eIDAS** es un **modelo regulatorio de fuerte control previo por el supervisor**, así como la obligación de certificar la seguridad técnica de los dispositivos empleados para la creación de la firma o sello electrónico cualificado, de modo que se alivia enormemente la carga de probar que en efecto una firma o sello electrónico, o un sello de tiempo electrónico, son realmente cualificados. A partir de ahí, lógicamente la otra parte tiene todo el derecho a proponer la práctica de prueba en su descargo, algo que puede ser muy necesario, dado que los niveles de seguridad de los servicios cualificados no son sino razonables y, por tanto, susceptibles de fallo – en algunos casos, además, debido al siempre delicado equilibrio entre seguridad y usabilidad, que puede conllevar la generación fraudulento de una prueba, incluso con firma/sello cualificados.

Y como **muestra**, un botón: desde el momento en que las normas técnicas empleadas para la certificación de los dispositivos seguros de creación de firma o sello electrónico permiten que una de las partes (por ejemplo, en una formalización contractual) genere unilateralmente el resumen criptográfico del

documento a firmar y lo remita a la otra parte para la creación de la firma, ¿qué impide un posible fraude? ¿Cómo probará esa parte generadora que no ha hecho trampa? ¿Cómo confiar realmente en un sistema cualificado si el mismo permite – nada menos que por diseño normativo – la posibilidad de engañar a la otra parte, frecuentemente protegida por un estatuto beneficioso como el del consumidor o el trabajador?

En este punto, hay que reconocer que la **interposición del tercero de confianza** – aún definido en el artículo 25 de la Ley 34/2002 – en la generación de la prueba puede ser la **única vía de prueba fuerte** de la que disponemos hoy, incluso cuando empleamos firmas y sellos cualificados; y no digamos cuando empleemos el resto de tipos de firma y sello electrónicos. Eso sí, debe ser digno, porque como le dijo el tío Ben al futuro Spiderman, "un gran poder conlleva una gran responsabilidad".

Nacho ALAMILLO DOMINGO

Fuente original:
http://www.empresaactual.com/servicios-confianza-y-prueba-electronica/

15

Validez y eficacia procesal de la prueba electrónica

Pedro J. Canut Zazurca*

@pjcanutz

Tratándose de un artículo divulgativo, sin aspiraciones científicas elevadas y dado que el público objetivo conoce sobradamente la legislación procesal trataré de obviar, en la medida de lo posible, las referencias normativas comunes.

En primer término, y antes de entrar en aspectos de lege lata, no me parece ocioso recordar el Auto T.S. de marzo 2013, ponente: magistrado Sr. O´Callaghan. En dicho Auto (previo a la publicación del Reglamento UE 910/2014, de 23 de julio) ya se establecían dos premisas respecto de la validez de las notificaciones telemáticas que, entiendo humildemente, pueden extrapolarse al ámbito probatorio.

En el citado Auto se decía que el destinatario de una notificación telemática debía estar en posesión de los medios telemáticos para recibir dicha

* Abogado y miembro del Consejo Asesor del Internet Governance Forum España. Ha sido profesor de la Facultad de Derecho en la Universidad de Zaragoza, especializado en derecho informático y de la contratación electrónica. Fundador y primer presidente de la sección de Derecho de Internet y Nuevas Tecnologías del Real e Ilustre Colegio de Abogados de Zaragoza, y miembro de la Comisión de Nuevas Tecnologías de la citada corporación de Derecho Público. Creador del primer registro global de obras libres por Internet conocido como Espacio de utilidad pública. Actualmente es Director General de Coloriuris, S.L., prestador de Servicios de Confianza para el sector público y privado; acreditación fehaciente de actos y procesos en redes telemáticas.

notificación, y continuaba invocando la figura del Prestador de Servicios de Certificación (regulado en la Ley 59/2003 de firma electrónica) como garante del proceso.

Aunque no es habitual, en esta ocasión el juzgador se adelantó al legislador en sus consideraciones; dado que en julio de 2014 (un año más tarde) los artículos 41 y 43 del Reglamento eIDAS establecían presunción de certeza en los servicios de sellado de tiempo electrónico y entrega electrónica certificada generados por Prestadores Cualificados de Servicios de Confianza (QTSP por sus siglas en inglés), herederos del Prestador de Servicios de Certificación, y de los que **ya hemos hablado** en **otras ocasiones**.

Artículo 41

Efecto jurídico de los sellos de tiempo electrónicos.
1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello de tiempo electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos de sello cualificado de tiempo electrónico.
2. Los sellos cualificados de tiempo electrónicos disfrutarán de una presunción de exactitud de la fecha y hora que indican y de la integridad de los datos a los que la fecha y hora estén vinculadas.
3. Un sello cualificado de tiempo electrónico emitido en un Estado miembro será reconocido como sello cualificado de tiempo electrónico en todos los Estados miembros.

Artículo 43

Efecto jurídico de un servicio de entrega electrónica certificada.
1. A los datos enviados y recibidos mediante un servicio de entrega electrónica certificada no se les denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales por el mero hecho de que estén en formato electrónico o no cumplan los requisitos de servicio cualificado de entrega electrónica certificada.
2. Los datos enviados y recibidos mediante un servicio cualificado de entrega electrónica certificada disfrutarán de la presunción de la integridad de los datos, el envío de dichos datos por el remitente identificado, la recepción por el destinatario identificado y la exactitud de la fecha y hora de envío y recepción de los datos que indica el servicio cualificado de entrega electrónica certificada.

De este modo, y aunque la presunción sea *iuris tantum* y no *iuris et de iure*, y los QTSP no gocen de fe pública (como sí tiene el Notariado, o mejor dicho, los notarios respecto de los hechos percibidos por sus sentidos (artículo 1 del Reglamento notarial) resulta evidente que el legislador comunitario ha optado

por ellos como garantes de los servicios de confianza online en el marco de la Unión Europea.

Lo dicho hasta ahora no significa que el juez ordinario no pueda, conforme al principio de la sana crítica, tener en consideración todas las pruebas que se sometan a su valoración a la hora de dictar Sentencia. De este modo, la prueba pericial o el testimonio de terceros de confianza (en el ámbito exclusivo de la contratación electrónica conforme a lo dispuesto por el artículo 25 LSSICE) sometidas a la contradicción de las partes pueden – y deben – ser otro medio en el que las partes puedan apoyar sus pretensiones; con la diferencia, respecto a la prueba intermediada por QTSP´s, de que la carga de la prueba se rige por los principios generales, y con las excepciones recogidas en las leyes.

Artículo 25

Intervención de terceros de confianza.
1. Las partes podrán pactar que un tercero archive las declaraciones de voluntad que integran los contratos electrónicos y que consigne la fecha y la hora en que dichas comunicaciones han tenido lugar. La intervención de dichos terceros no podrá alterar ni sustituir las funciones que corresponde realizar a las personas facultadas con arreglo a Derecho para dar fe pública.
2. El tercero deberá archivar en soporte informático las declaraciones que hubieran tenido lugar por vía telemática entre las partes por el tiempo estipulado que, en ningún caso, será inferior a cinco años.

En definitiva, la valoración de la prueba – también en el ámbito digital – es prerrogativa del Juzgador y, por mucho que incomode fuera del sector jurídico, en Derecho dos más dos no siempre suman cuatro.

Del mismo modo que un acta notarial de manifestaciones no es prueba plena respecto de la veracidad de los hechos manifestados, no puede pretenderse que la intermediación de terceros de confianza, el informe pericial o el certificado emitido por un QTSP hagan prueba plena de todos los hechos en litigio; y sí y sólo de aquellos sobre los que los terceros, los peritos o los QTSP´s tienen el absoluto control.

Probablemente me explicaré mejor con un ejemplo: Fallo condenatorio por amenazas tomando como base la visualización de un *WathsApp* en el terminal móvil de la víctima. Sin duda el amable lector, con un alto grado de conocimiento tecnológico, se lleve las manos a la cabeza; y también me las llevaría yo si la visualización de una conversación de *WathsApp* fuera el único

elemento probatorio tenido en cuenta a la hora de emitir el Fallo. No obstante si el juzgador, que ha visto y hablado con la víctima de 70 años, llega a la conclusión razonada de que ésta carece de los conocimientos técnicos y/o de la picaresca necesaria para falsear la prueba la cosa cambia.

Por otra parte no es infrecuente el desconocimiento de algunos tecnólogos respecto de las consecuencias que tiene el hecho de falsificar una prueba en juicio; para quien *hace trampas* y para el abogado que a sabiendas presenta y defiende esa prueba. No debemos olvidar que la contraparte puede ejercer su legítimo derecho a presentar prueba en contrario y, en no pocas ocasiones, la prueba falseada para inducir a error al perito, al tercero o – incluso – al QTSP puede convertirse en la prueba de cargo de la falsificación probatoria con las consecuencias para el infractor que prevé el código penal.

Dicho lo cual ¿que la prueba electrónica es más fácilmente falseable que la analógica? Probablemente. ¿Que la prueba pericial y/o el testimonio de un tercero de confianza en materia contractual refuerzan la validez de la prueba electrónica? Sin duda. ¿Que la certificación de un Prestador Cualificado de Servicios de Confianza goza de presunción de certeza? Indiscutible.

Pero también, que del mismo modo que viene ocurriendo a lo largo de los siglos en el mundo analógico, en el ámbito digital hay sitio para la falsedad y el fraude; y la responsabilidad, en estos casos, es única y exclusivamente del autor del mismo. Pretender algo distinto es como pretender que la responsabilidad de que un cuchillo no corte por el lado opuesto al filo es responsabilidad del fabricante de los cuchillos y no del comensal que utilizó mal la herramienta.

He dejado para el final mi opinión respecto a la intervención de notario a la hora de preconstituir prueba digital.

Las actas notariales, y de esto hay quien sabe muchísimo más que yo, pueden ser de muchos tipos, y pueden plasmar diversas manifestaciones. Volveré a los ejemplos; en este caso un acta notarial sobre el contenido de una página web en fecha determinada. Con variantes de estilo un acta de estas características podría decir, por ejemplo:

"Don Jacinto X Y, se persona en mi notaría y me requiere a mí el notario para que acceda al sitio web http://www.elsitioweb.com y levante acta incorporando el contenido de la misma. Yo el notario accedo a la citada dirección de Internet y realizo 10 impresiones de pantalla con el contenido del sitio web, las cuales incorporo a este acta en tantos folios de papel notarial, numerados…"

Cuando Don Jacinto acuda a los Tribunales con su acta notarial que goza de fe pública pueden ocurrir dos cosas:

1ª.- Que el perjudicado por la prueba sepa que es cierta y se allane a la demanda de Don Jacinto.

2ª.- Que el perjudicado por la prueba sepa que NO es cierta y trate de desvirtuar la prueba de Don Jacinto y presente prueba en contrario.

En el segundo supuesto el demandado no lo tiene demasiado difícil a partir de prueba pericial especializada, porque el notario autorizante – que no puede comprobar la veracidad de la información que le muestra su navegador – de lo único que dará fe es de que escribiendo en su navegador la dirección de internet que le ha informado Don Jacinto él ve determinada información, la imprime y la incorpora al acta notarial; pero otra cosa es hablar de veracidad del contenido con exclusión de phising, man in the midle…etc. Porque los seres humanos (y los notarios, hasta donde yo sé, lo son :)) no podemos percibir por nuestros sentidos las transacciones que se producen entre un equipo local y las páginas de Internet.

También puede ocurrir que, quien haya de resolver el litigio entre Don Jacinto y el demandado carezca de los conocimientos informáticos básicos y no confíe en la pericial contradictoria, aferrándose al concepto fe pública como un mantra.

Podría haber quien llegados a este punto pudiera pensar que si Don Jacinto, a pesar del acta notarial, no ve reconocidas sus pretensiones tiene una acción de responsabilidad contra el notario. Nada más lejos de la realidad. El notario ha hecho su trabajo…sólo que su trabajo no era lo que necesitaba Don Jacinto…o sí, si había actuado con *picardía*.

En Derecho dos más dos no siempre suman cuatro. En el ámbito de la prueba digital, como cuando nos referimos a la prueba analógica, los Tribunales entrarán a valorar cualquier prueba válida en Derecho. Es labor de los letrados conocer cuando se precisa cada prueba; sola o en combinación con otros medios probatorios no necesariamente digitales.

Pedro J. CANUT ZAZURCA

Fuente original:
http://www.blogespierre.com/2016/04/12/reto2jcf-validez-y-eficacia-procesal-de-la-prueba-electronica/

16

Nuestro punto de vista sobre la evidencia digital

Yago Jesús Molina*

@YJesus

Estos días se ha puesto en marcha el #Reto2JCF desde el portal @JuristasFuturo para que diferentes personas que participan de una forma u otra en lo que se denomina 'evidencia digital' diesen su punto de vista.

Creo que es una magnífica oportunidad de expresar la forma en la que desde eGarante concebimos ese concepto y tratar de ofrecer un punto de vista que transcurra en paralelo al de Notarios, Abogados y Peritos informáticos.

De entrada, nosotros no pretendemos 'enviar de vacaciones a los notarios', nunca hemos creído que el tipo de servicios que ofrece eGarante se corresponda con la actividad de un notario. Y es algo que dejamos muy claro en nuestra página web, y siempre que alguien nos lanza esa cuestión:

¿Vosotros sois como un notario? NO
¿Vuestra certificación tiene la misma forma jurídica a la de un Notario? NO
Decir lo contrario supondría directamente mentir, y las mentiras tienen las patas muy cortas.

---

* Profesional de la seguridad informática desde el 2001 ha colaborado profesionalmente con los equipos de seguridad en grandes empresas del sector telecomunicaciones, entidades bancarias, organismos del sector defensa, y participado activamente en el despliegue de la PKI del DNI Electrónico. Editor del blog Security By Default, ha desarrollado multitud de herramientas entre las que destacan 'Unhide', herramienta para realizar análisis forenses en sistemas Unix/Windows que forma parte de las principales distribuciones Linux (Debian, Ubuntu, RedHat) O Patriot NG, herramienta anti-Malware para entornos Microsoft. Creador de eGarante, una herramienta web que permite obtener certificados con sello de tiempo de correos electrónicos y de páginas web.

Nosotros entendemos nuestros servicios como la posibilidad de ofrecer pruebas **extremadamente sólidas desde un punto de vista pericial**. De hecho, uno de los primeros pasos que dimos cuando pusimos en marcha el servicio es iniciar contactos y colaboraciones con **ANCITE**, prestigiosa asociación de peritos Española. Y en ese aspecto hemos puesto todo nuestro esfuerzo y capacidad: en poner **todos los medios técnicos (firmas digitales longevas, sellos de tiempo, etc)** para que todas las evidencias generadas por eGarante tuvieran una solidez técnica que las convirtiese en atractivas para Abogados y Peritos. De hecho, muchos de nuestros clientes provienen de ambas ramas profesionales.

Ni eGarante es un notario, ni un notario es siempre la mejor opción cuando nos adentramos en el mundo digital.

Pondré un ejemplo totalmente inventado pero con una base técnica real. Supongamos que alguien encuentra una vulnerabilidad de tipo XSS (Cross-site scripting) en un periódico digital, por ejemplo en 'El País'. Este tipo de vulnerabilidades son bastante curiosas y se basan en la posibilidad de abusar de partes en las que el usuario puede insertar contenido y que luego es usado posteriormente para construir una página web. Normalmente la idea del programador es, por ejemplo, poner un apartado de comentarios en una noticia donde espera que la gente escriba texto 'normal'.

Pero ¿y si alguien mete contenido HTML? Respuesta: **Tenemos un problema**, y si encima añade contenido javascript, entonces esa vulnerabilidad puede ser abusada para crear una nueva página web que nada tenga que ver con la original.

Por poner un ejemplo, hablemos del famoso **Mr Bean en la página web de la presidencia española de la UE**. Muchos medios tacharon ese incidente de 'Hackeo' y vendieron el asunto como si hubiese sucedido una intrusión.

Pero no era así. Se trataba de una vulnerabilidad de tipo XSS que nada tiene que ver con una intrusión.

Siguiendo con el ejemplo anterior, tenemos un periódico digital y ahora vamos a suponer que alguien encuentra una vulnerabilidad de tipo XSS que le permite crear contenido totalmente ajeno al del periódico usando, por ejemplo, el espacio de comentarios que tiene cada noticia. Y como este atacante tiene mucho sentido del humor, crea una página paralela en la que se da por noticia

una supuesta relación sentimental entre Pablo Iglesias y Albert Rivera. Le añade un fotomontaje y la publicita por twitter con un tweet tal que así:

'Asco de periodismo' http://enlace-que-te-lleva-a-elpais-con-contenido-que-no-es-de-elpais

Ese tweet se viraliza y alguien en Podemos decide tomar cartas en el asunto. Va a un notario y le piden que levante acta de lo que hay ahí. El notario, muy versado en transmisión de patrimonio pero bastante lego en informática, levanta un acta demoledora.

Podemos lleva a juicio a El País por intromisión al honor y el juez, que tiene mucha confianza en el Notario, condena al periódico digital ya que la noticia, según la evidencia, existía y es claramente una falacia.

Ahora pensemos en otro escenario diferente. Existe esa acta notarial, pero en paralelo, El País se pone en contacto con nosotros y nos pide que certifiquemos tanto el contenido de la web (el pantallazo) como **el código fuente** de dicha web. En la evidencia digital que El País tiene en su poder, es perfectamente auditable 'donde está la miga' y deja muy a las claras que nadie en la redacción de dicho medio ha tomado partido directamente en la supuesta noticia.

El juez valora el acta del notario, que da fe del contenido, y en paralelo valora la prueba pericial de la que dispone El País que desvela claramente que un usuario malintencionado ha abusado de su web y que en realidad el contenido ofensivo es totalmente ajeno al medio periodístico.

El juez absuelve al periódico e inicia diligencias para localizar a la persona para hacerla responsable tanto del daño a los políticos como al medio digital.

Un final feliz donde todas las partes han cumplido una misión valiosa a la hora de crear evidencias digitales.

Este ejemplo es una materialización de cómo vemos desde eGarante la evidencia digital. Creemos que en el ordenamiento jurídico y en la realidad de la sociedad existen múltiples figuras que coexisten. Todas estas figuras: notarios, abogados, peritos y certificadores tienen una función específica y tiene todo el sentido del mundo que colaboremos entre nosotros para conseguir el objetivo final de todos: ofrecer las máximas garantías sobre lo que ha sucedido en el entorno digital.

Este objetivo me lleva a otro aspecto, que es el grado de certeza que se puede tener sobre un hecho concreto. En este aspecto, el entorno digital genera en

muchas personas una percepción de inseguridad que les lleva a ser mucho más exigentes que en el entorno físico, llegándose a extremos que según los casos no tienen ningún sentido.

¿Cuál es el objetivo de servicios como el nuestro? Básicamente es proveer una herramienta que permita dar un salto cualitativo en la capacidad probatoria respecto de comunicaciones acaecidas por medios digitales, ya sea información publicada en la web, información intercambiada por correo electrónico o documentos intercambiados por medios online. Los servicios como los nuestros aportan valor por sus características intrínsecas:

· Constatan la información de la que ha sido testigo un tercero independiente al hecho que está en cuestión

· Recogen la información tal y cómo se ha visto con un elevado grado de detalle técnico que permite conocer no sólo el contenido en discusión, sino también información técnica asociada al proceso de la comunicación

· La información se capta en el momento de producirse la comunicación, facilitando de manera enorme resolver dudas sobre la cadena de custodia

La información capturada **queda firmada digitalmente** con un **sello de tiempo** asegurando al mismo tiempo el origen temporal de la misma y la integridad ya que, si dicho documento es manipulado, el firmado digital alertará de la pérdida de integridad

¿Cuál es el resultado? Unos documentos que ofrecen una capacidad probatoria extremadamente sólida. Y estos documentos pueden ser un punto de partida perfecto para, en caso de necesidad, practicar una prueba pericial.

No obstante, nuestra experiencia es que el constatar la información de una forma tan sólida, tiene un efecto disuasorio enorme en la parte que quiere, de manera dilatoria, negar la existencia de una comunicación o un hecho acaecido en Internet. Sin la existencia de la participación de un tercero independiente, el eslabón más débil es probar la existencia de una comunicación. Cuando un tercero ha participado y dejado una sólida evidencia de lo ocurrido, resulta prácticamente imposible desmontar dicha prueba. Como consecuencia de ello, la parte incumplidora suele tratar de buscar una vía de conciliación.

Yago JESÚS MOLINA

Fuente original:
https://blog.egarante.com/2016/04/12/nuestro-punto-de-vista-en-el-reto2jcf/

Epílogo

Ruth Sala Ordóñez*

@Ruth_Legal

Fui sorprendida por el #Reto2JCF, era sobre la "Prueba Electrónica", mi especialidad, la materia de mis clases en la Universidad de Barcelona, en las formaciones en los Colegios de Abogados de diferentes partes del país. ¿Por qué no crear ese artículo para sumar en un proyecto común con los mejores profesionales del país?

Me proyecté a esos años iniciáticos en los que compaginaba tercero de carrera con mis horas en un despacho. Se me pedía la creación de un contrato y sobre él, mi jefe, tachaba y redondeaba todo lo que, a su criterio, estaba mal. Lo más fácil es trabajar sobre el trabajo de otros, lo difícil es crearlo. Ante la solicitud de Juristas con Futuro por que enviara mi opinión, decidí que no. Que prefería escuchar qué era lo que los demás compañeros y profesionales, intervinientes en los procesos de captación de evidencias / pruebas electrónicas, tenían para aportar. Así que, mi punto de partida es el trabajo de creatividad y experiencia aportado por los demás profesionales sobre el que tengo la responsabilidad de hacer un epílogo digno de su altura y conocimientos.

Desde mi día a día ante los Tribunales, tuve que buscar solución a la forma de proceder para la aportación de prueba electrónica que tuviera validez jurídica.

---

* Abogada penalista, especialista en delincuencia informática. Directora de Legalconsultors. Actualmente colabora con la Universidad de Barcelona en el Máster de Derecho Digital y con la Universidad de La Salle en el Máster de Márketing Digital. Miembro de la Sección de Derecho de las Tecnologías de la Información y la Comunicación del Colegio de Abogados de Barcelona.

Descubrí que las evidencias pueden ser alteradas y por tanto, generar una duda importante acerca de su autenticidad e integridad. Indagando en las herramientas de que disponíamos los Juristas para preservar esa autenticidad e integridad, di con los que se denominaban Prestadores de Servicios de Certificación y que, mediante un Certificado Electrónico, validado por el Ministerio de Industria español, podían acreditar la autenticidad e integridad de todos, o muchos, de los actos y procesos que se producían a través de la red. Descubrí la existencia de los que se denominaban Terceros de Confianza y que utilizaban, en la venta de sus productos y servicios para garantizar los actos y procesos en la red, los Certificados Electrónicos de aquéllos Prestadores de Servicios de Certificación validados por la Administración. Se abrió un mundo de posibilidades y de diferentes criterios dentro de este "mundillo".

Un artículo en el Blog "Un Informático en el Lado del Mal", pilotado por Chema Alonso, o al menos, figura su nombre como motor del mismo, en el que se reventaba una de las aplicaciones que utilizaba un Operador de Telecomunicaciones, Lleida.net, acerca de la captación de fotografías con certificado del lugar y la identificación del terminal, me generó mucha indignación, lo reconozco. No tanto por el contenido en sí, sino por la sensación de que no había forma posible de que la Prueba Electrónica tuviera garantía de ser auténtica e íntegra. Aquél artículo produjo en Twitter notable revuelo. Meses más tarde, el auténtico autor de aquél artículo se puso en contacto conmigo, brindándome la posibilidad de expresarle, en directo, mi disconformidad por la inseguridad jurídica que crea el hecho de inutilizar aplicaciones que, supuestamente, deberían generar seguridad jurídica.

Aquél artículo fue devastador para la confianza que había adquirido con los Prestadores de Servicios de Certificación en mi día a día profesional. ¿Aceptar el Reto2JCF? Por supuesto... que no! La sensación agridulce aún permanecía en mi memoria después de aquél artículo que "liquidaba" la aplicación del Operador de Telecomunicaciones. Preferí mantenerme en la calma y el silencio, esperando la visión de los profesionales que, desde su especialidad, tenían acerca de ello.

Notarios, la prueba electrónica, su gran reto.

Paco, (**Francisco Rosales**) Notario me adelantó su artículo por mail: **"*Validez y eficacia procesal de las evidencias digitales*"** Sorprendentemente nunca hubiera orientado mi discurso hacia aquéllos parajes

del estudio y la profundidad jurídica en el "por qué". Aquellos textos, propios de largas Tesis especializadas, me quedaban anclados en la época de los estudios en la biblioteca de la Facultad de Derecho. Un carácter impaciente y el trabajo en la trinchera hacen que necesites encontrar la herramienta precisa como si fueras una yonqui del "dame lo que necesito ahora, no me hagas pensar". Francisco Rosales te lleva a los conceptos primigenios del hecho jurídico, acto jurídico y del negocio jurídico. Hace hincapié en la verdadera posibilidad de probar actos jurídicos digitales. Aún a pesar del análisis tan profundo que se hace sobre los conceptos, la realidad es que, el *Artículo 199.2 del Reglamento Notarial* impide que el Notario de fe de hechos que requieran conocimiento periciales. Esta es la conclusión que, descarta por completo el trabajo de los Notarios y evidencia que están perdiendo posibilidades en la acreditación de los Actos, Hechos o Negocios Jurídicos en los que se vea implicado el Código de Programación. ¿Descartamos el discurso? No, por supuesto. Es digno de una Fundamentación Jurídica de Sentencia del Tribunal Supremo, aún por venir con ese enfoque.

En calidad de Notario también, **José Carmelo Llopis**, en su artículo ***"Prueba electrónica y Notariado"*** hace hincapié en la posibilidad de la existencia de una herramienta que pudiera facilitar la captación de prueba electrónica directamente desde el ordenador del Notario. ¿De qué tipo de herramienta hablamos? ¿De una como el etilómetro, por ejemplo? Que cumpliera con las garantías administrativas necesarias para ser considerada "la herramienta" de la autenticidad y la integridad de la prueba electrónica. Pensando la frase, siento que es extremadamente arriesgado pensar en la fiabilidad de una herramienta tecnológica que pudiera hacer una captación de evidencias digitales con las máximas garantías y más cuando ni el propio Notario, por entrar en contradicción con su artículo 199.2 del Reglamento del Notariado, no podría acreditar las potenciales alteraciones que se hubieran podido efectuar sobre la misma herramienta y que podría dar una Prueba Electrónica corrupta, con las nocivas consecuencias jurídico-procesales sobre ello.

Concluyendo sobre el trabajo de los Notarios, podemos entender que, su propio Reglamento impide la acreditación de extremos que, como ellos mismos reconocen, escapan a sus conocimientos por precisar de la intervención de Periciales, en este caso, de carácter informático. Quizás tampoco profundizaría tanto en el Reglamento Notarial puesto que ya, desde

su artículo 1, se hace hincapié en que sólo podrán Dar fe de aquello que puedan percibir a través de sus sentidos.

Ingenieros Informáticos, valoración desde el mismo Código.

Los Ingenieros, realmente prácticos, se centran en desvelarnos otros puntos débiles y que envuelven la Prueba Electrónica y son, entre otros, la cadena de custodia. **José Aurelio García** con su post ***"Cadena de Custodia vs Mismidad"*** se centra en la importancia de la Cadena de Custodia. No existen protocolos legislados que determinen un proceso tasado acerca de cómo se debe proceder a la ejecución de esa captación de prueba electrónica y esa conservación hasta su enjuiciamiento. Se centra en la necesidad de:

- garantizar la indemnidad de la prueba

- evitar las alteraciones, sustituciones, contaminaciones o destrucciones

- la necesidad de que la evidencia que se recolecta del escenario debe ser la misma que se está presentando ante un Tribunal.

Ese debería ser el enfoque acerca de la valoración de la prueba, la ·"mismidad" y la "autenticidad".

Aún a pesar de introducir estos nuevos criterios o necesidades "deja caer" la importancia de estar plenamente convencidos que la prueba informática no ha sido alterada. Plantea un supuesto práctico y la posibilidad de que por la mera introducción de un pendrive en un puerto USB controlado por un determinado Sistema Operativo, se altere la prueba sin remedio. Ese artículo volvió a generar duda sobre si realmente hemos desarrollado la metodología y las herramientas que preservan esa autenticidad de la prueba electrónica captada.

Óscar Domínguez Merino, con su artículo "***La necesidad de evidenciar lo evidente***", inicia su argumentario con un "(…)en lo que a informática se refiere, cualquier elemento es manipulable", sin embargo, termina su desarrollo con un "los Prestadores de Servicios de Certificación son los únicos que pueden certificar y dar validez a cualquier fichero digital" y yo me pregunto, ¿seguro? Vuelvo una y otra vez al artículo de la Aplicación crackeada del Operador de Telecomunicaciones y sigo con la desconfianza de que realmente esos Prestadores de Servicios de Certificación sean "los únicos" que puedan dar validez a la Prueba Electrónica.

La postura de **Yago Jesús**, Ingeniero de eGarante, con su artículo "***Evidencia Digital***" me parece la más elegante y honesta, por cuanto define el proyecto de eGarante como un Tercero de Confianza (tercero que no es parte interesada en un acto o proceso) y describe el "mapa" de los operadores intervinientes en la captación de Evidencias Electrónicas en paralelo junto al de los Notarios, Abogados y Peritos Informáticos. Defiende el papel del Tercero no parte por cuanto, no tiene interés en "lo que sucede", recoge información técnica detallada y garantiza el momento en el que esa transferencia de información se ha producido. Dibuja un escenario de la Prueba Electrónica en el que cada uno de los Profesionales tiene su propio papel.

Concluyo por la parte de los Ingenieros Informáticos la necesidad de que sus propias intervenciones técnicas sean validadas por alguna herramienta que jurídicamente otorgue a la Prueba Electrónica captada de plena validez y autenticidad para el caso de tener que ser presentada como prueba ante los Tribunales.

Abogados y Consultores, el reto de la Prueba Electrónica

Los juristas se dividen en dos grupos diferenciados, los que plantean causas eminentemente prácticas y procesales del día a día de los profesionales del Derecho y los que plantean un estudio profundo acerca de cuáles son las Leyes que validan la autenticidad de la Prueba Electrónica captada mediante herramientas creadas por los Prestadores de Servicios de Certificación e incluso los Terceros de Confianza.

Las abogadas **Sara Molina** y **Marta Sánchez** aportan, desde elementos prácticos del día a día, la necesidad de aportar la prueba de WhatsApp junto con una Pericial Informática y un Acta Notarial que autentique el contenido. Transmiten la necesidad de poner cuantas más "capas" de seguridad mejor a fin de considerar una prueba fácilmente manipulable en algo auténtico e íntegro. Sobre WhatsApp se han escrito ríos de tinta, incluso se ha tomado la Sentencia del Tribunal Supremo 300/2015 como "punta de lanza" para determinar acerca de la necesidad de esas Periciales Informáticas. Baste decir que, a día de la fecha, no entiendo cómo se le ha dado tantísima relevancia a esa Sentencia que muchos de los operadores (Ingenieros incluidos) se la han "hecho suya" como si de una verdad absoluta se tratara. La Sentencia menciona la mayor fuerza que puede dar presentar una Pericial Informática, pero no determina que pueda ser considerada "prueba de cargo" por su simple

existencia. Determina, a lo largo de toda la Sentencia, de la necesidad de proceder a la valoración de una suma de indicios y al denominado "comportamiento procesal de las partes".

David Maeztu, aporta su grano de arena en relación a la prueba del WhatsApp preguntándose si puede acreditarse el contenido de una comunicación en este sentido, concluyendo que si las partes no presentan impugnación, cualquier medio es válido para presentar una prueba, estando sujeta a la determinación de su pertinencia por el Juez y a la valoración bajo los criterios de la sana crítica.

Sobre los aspectos también eminentemente prácticos introducidos en el artículo relacionado con Fitbit, aplicación que valora el estado de salud, tenemos también que decir que resulta una prueba más que curiosa puesto que introduce nuevos elementos en la investigación delictiva y en la captación de Prueba Electrónica. No nos quedemos sólo en lo que se ve, porque dentro de las mismas aplicaciones contenidas en el móvil existe muchísima más información que generará ese perfil del usuario y, por tanto, posiblemente del investigado. ¿Será considerada auténtica esa evidencia electrónica? ¿Puede un Prestador de Servicios de Certificación intervenir en ello para garantizar su autenticidad e integridad? No, no puede, pero servirá como esa "suma indiciaria" que podrá decantar la orientación de un proceso judicial.

Rubén Vázquez con su artículo ***"Geolocalización y práctica probatoria, condenados a encontrarse"***, incide en otra de las posibilidades que nos ofrecen las aplicaciones móviles, e incluso los mismos terminales, la geolocalización. Los usuarios, en ese intercambio diario de información van generando ellos mismos su propia Prueba Electrónica, condenatoria o absolutoria, sin conocimiento alguno. Nos abre los ojos a la posibilidad de proceder a una investigación sobre los hechos a partir de la Geolocalización de terminales y de aplicaciones. Con muy buen criterio, introduce la primera contradicción en esa búsqueda de la herramienta más adecuada para garantizar la autenticidad y la integridad de la prueba electrónica. Cuando, alguno de los Ingenieros concluye acerca de la necesidad de la existencia de los Prestadores de Servicios de Certificación, plasma sobre su artículo la referencia al mismo post de "Un informático en el lado del mal" donde efectivamente se plasma ese crackeo del GPS de un terminal móvil y una aplicación que supuestamente garantiza la captación de imágenes en el lugar exacto en el que han sido

captadas, no detecta el falseamiento que se ha efectuado sobre el GPS del terminal.

Con este artículo, me devuelve al punto de partida y sigo estando en el "punto cero" del Reto2JCF. Si bien concluyen hasta aquí todos los profesionales acerca de la necesidad de encontrar la herramienta jurídica que garantice la Autenticidad y la Integridad, una y otra vez los ejercicios técnico-informáticos a modo de "prueba-error" nos vuelven a esa inseguridad jurídica con la que iniciamos el epílogo.

José María Anguiano, profesional parte del proyecto de Logalty (Tercero de Confianza con servicios de Certificación Electrónica) realiza un estudio y profundización en la necesidad de generar aquellas herramientas necesarias que puedan acreditar la prueba electrónica en la banca digital. Con **Raúl Rojas** nos vamos directamente a casos prácticos en el ámbito laboral, que son numerosos. El intercambio de información de los empleados a través de los diferentes medios electrónicos, van a fundamentar en muchas de las ocasiones los despidos procedentes que se vienen realizando en las empresas. Cuestiona directamente acerca de la autenticidad de la prueba presentada y la sitúa en que la evidencia digital, como podría ser una captura de pantalla, podría ser presentada en forma de:

a) documento privado o documento público

b) con informe pericial que dé acreditación a su contenido incorrupto

c) constatación directa por el propio Juzgado por reconocimiento judicial

Si bien, no tendrá el mismo valor probatorio la prueba presentada de una manera o de otra, no descarta la posibilidad de su aportación en cualquiera de los formatos, dejando siempre a la valoración y la sana crítica de un Juez el valor de la misma.

Aporta **Sergio Carrasco** también, dentro del proceso, la necesidad del abogado de conocer de la importancia de preservar adecuadamente la prueba electrónica y como criterios diferenciadores se pronuncian tanto **Pedro J. Canut** (Gerente de ColorIURIS, Prestador de Servicios de Certificación) como **Nacho Alamillo** (Colaborador de Logalty, Tercero de Confianza) en la defensa de los Servicios de Certificación Electrónica de Actos y Procesos, fundamentando la "natural" validez de sus servicios por la normativa europea que les ampara, en este caso el Reglamento IDAS (Reglamento UE 910/2014

del Parlamento Europeo y del Consejo de 23 de julio de 2014) que establece las normas para los servicios de confianza así como un marco jurídico para las firmas electrónicas y los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega certificada y los servicios certificados para la autenticación de los sitios web.

Con este expositivo relacionado en ambos artículos, se fundamenta la validez jurídica de los Servicios de los Prestadores de Certificación y, en su caso, los Terceros de Confianza que utilicen, de una forma u otra, los "sellos" de los Prestadores.

Volvemos al principio, a la posibilidad, según el artículo del Blog "un informático del lado del mal", de crackear una aplicación de Prestador de Servicios de Certificación. Aún a pesar de que exista la legislación que ampare su existencia dando valor jurídico y autenticidad a sus productos y servicios, lo cierto es que, tal como manifiestan los Ingenieros, la prueba electrónica podrá ser siempre manipulable y, en esa situación, nos metemos de lleno en el artículo de **Ricardo Oliva** acerca de la prueba electrónica envenenada que podría provocar la desestabilización de todo un proceso por haber sido alterada o ilícitamente obtenida.

Conclusión, ¿hay seguridad en la presentación de la prueba electrónica? Parece ser que no está tan claro y mucho menos entre los mismos Operadores Jurídicos intervinientes en el proceso, ni siquiera para los Ingenieros. ¿Qué hacemos entonces en un proceso judicial? Podríamos decir que deberemos estar a esa "suma indiciaria" y a la valoración por la sana crítica del Juez, quién, en mayor o menor medida, deberá resolver los procesos en base a la prueba presentada, sea electrónica o no.

Aún a pesar de las muchas dudas y contradicciones que se abren con este Reto2JCF, seguiré dando la clase de Prueba Electrónica en la Universidad de Barcelona confiando en los servicios de los Prestadores de Servicios de Certificación como una herramienta que da valor y autenticidad a los Actos y Procesos generados en la Red.

Ruth SALA ORDÓÑEZ

QUIÉN ES QUIÉN EN LA PRUEBA ELECTRÓNICA

HECHO DIGITAL
Contenido alojado en una página web en una determinada fecha, una comunicación en un sistema de mensajería instantánea...

NOTARIOS

ACTA NOTARIAL DE PRESENCIA

¿Qué es? Es un recurso jurídico que debe cumplir con ciertos requisitos técnicos e informáticos para ser efectiva en juicio.

Limitaciones de las actas:
- No basta con ver la web o hacer un pantallazo: Lo que muestra la pantalla es sólo el resultado de la interpretación de un código informático.
- Es posible falsificar / manipular / alterar los envíos de aplicaciones de mensajería.
- La actuación notarial no convierte en verdad lo que es falso. El notario puede ser inducido a error (el interesado le presenta un documento falso).
- El notario levanta acta según lo que se presencie o perciba por sus propios sentidos.
- La DGRN (a día de hoy) no ha aprobado las normas técnicas sobre los soportes en que debe realizarse el almacenamiento de documentos electrónicos.

Contenido sugerido de un acta de una página web:
- ✓ El código fuente
- ✓ La ubicación del servidor
- ✓ La ruta de conexión

Objetivos genéricos:
Acreditar, dejar constancia con fe pública de un hecho digital.

Objetivos específicos:
Probar de modo fehaciente el uso ilegítimo de la propiedad intelectual (textos, fotos, vídeos), el tratamiento de nuestra imagen o datos personales sin consentimiento, la comisión de un delito en internet (injurias, calumnias), delitos contra la propiedad industrial y revelación de secretos...

NO PUEDEN:
- Percibir datos electrónicos.
- Verificar el origen de la comunicación.
- Emitir juicios de valor que requieran conocimientos periciales.
- Garantizar que lo que ve ha sido o está siendo manipulado.

PERITOS INFORMÁTICOS

DICTAMEN PERICIAL

¿Qué es? Es un medio de prueba que permite dejar constancia de que lo que se ve ha sido (o no ha sido) o está (o no está) siendo manipulado.

¿Cómo sabe el perito que está frente a lo que se recolectó en su día?

Limitaciones:
- Es fácil alterar las pruebas electrónicas y difícil preservar su inalterabilidad.
- El perito sólo puede certificar el estado de las cosas desde el momento en el que toma contacto con la evidencia.
- Necesario control de la cadena de custodia para dar traslado de la prueba inalterada al ámbito probatorio mismidad de la prueba.

PROCEDIMIENTO PERICIAL — ISO/IEC 27037:2012
No hay un procedimiento legal.
Se rigen por los estándares internacionales en materia de recogida, identificación y secuestro de las evidencias digitales.

Se recomienda CLONAR la evidencia.

IDENTIFICAR EL HASH elemento clave en el análisis pericial informático.

Cadena alfanumérica hexadecimal generada a partir de la aplicación de un algoritmo.

Identificador de un archivo digital.

Objetivo genérico:
Emitir una opinión según las reglas de su experiencia y conocimientos de la cuestión.

Objetivos específicos:
- Garantizar que la evidencia que se recolectó en la escena de la comisión del hecho es la misma que está siendo analizada por el perito o está ante un tribunal.
- Evitar alteraciones, sustituciones, contaminaciones, destrucciones de la prueba.

Determina si ha habido manipulación o no, analizando: dispositivos / software

Describe y constata hechos digitales

"PRINCIPIO DE INTERCAMBIO O DE LOCARD"
Cada contacto deja su rastro

TERCERO DE CONFIANZA

CUSTODIA DOCUMENTOS

¿Qué es? Archiva y guarda una copia de los documentos electrónicos

Limitaciones:
- Sólo custodia.
- La ley no le exige garantías de custodia.
- No es un notario.
- No garantiza la legalidad del documento que custodia.
- No otorgan garantías ni seguridad jurídica con fe pública.
- Necesario el acuerdo de ambas partes, no puede actuar de forma unilateral.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Artículo 25:

Intervención de Terceros de Confianza:
Pacto entre las partes para que un TERCERO archive sus declaraciones de voluntad que integran los contratos electrónicos.

en soporte electrónico

Consignará FECHA Y HORA en que ha tenido lugar la comunicación

por el tiempo que estipulen las partes, pero mínimo 5 años

Objetivo genérico:
Custodiar documentos privados electrónicos.
Guardar copia de las comunicaciones electrónicas hechas entre partes.

Ley 59/2003, de 19 de diciembre, de Firma Electrónica

Prueba de autenticidad de la comunicación.

Objetivos específicos:
GARANTIZAR:
- **Confidencialidad**
- **Integridad**
- **Disponibilidad**

Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD)

SÓLO ARCHIVA DOCUMENTOS EMITIDOS POR VÍA TELEMÁTICA

NO PUEDEN:
- Garantizar la legalidad del documento.
- Garantizar que se ha respetado la cadena de custodia.

PRESTADORES DE SERVICIO DE CERTIFICACION / PRESTADORES CUALIFICADOS DE SERVICIOS DE CONFIANZA

SERVICIOS DE CONFIANZA

¿Qué es? Aquellas tecnologías en las que se puede confiar.
Servicio electrónico prestado habitualmente a cambio de una remuneración:

CREACIÓN | VERIFICACIÓN | VALIDACIÓN | PRESERVACIÓN

- FIRMA ELECTRÓNICA
- SELLO ELECTRÓNICO
- SELLO DE TIEMPO ELECTRÓNICO
- SERVICIO DE ENTREGA ELECTRÓNICA CERTIFICADA
- CERTIFICADO ELECTRÓNICO

Limitaciones:
- Gran inversión en tecnología
- Intrusismo y confusión al usuario
- Publicidad engañosa
- Responsabilidad
- Inmadurez tecnológica de abogados y jueces

Objetivo genérico:
Otorgar validez a los documentos electrónicos.

Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, de FIRMA ELECTRÓNICA

Objetivos específicos:
- Otorgar validez a las notificaciones telemáticas
- Evitar una falsificación de una prueba digital
- Aportar confianza a las interacciones electrónicas
- Poder ser utilizados como prueba en procedimientos judiciales

Reforzar la confianza en las transacciones electrónicas en el mercado interior

REGLAMENTO eIDAS*

* Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

ABOGADOS

PRUEBA JUDICIAL ELECTRÓNICA

IMPUGNACIÓN DE LA PRUEBA

teoría del fruto del árbol envenenado

Limitaciones:
- Medios de defensa legítimos
- Obtención lícita de la prueba
- No servir para dilatar el proceso
- Conocimiento de la cadena de custodia
- Manipulable

¿Qué es? Actividad encaminada a verificar la veracidad o falsedad de un hecho presentada informáticamente y que estaría compuesta por 2 elementos:
- **TANGIBLE**: parte física y visible que depende de un hardware (Smartphone, memoria USB)
- **INTANGIBLE**: representado por un software consistente en los metadatos y archivos electrónicos modulados a través de interfaces informáticas.

PRUEBA LÍCITA: Aquella que se obtiene sin violar derechos y libertades fundamentales

Objetivos genéricos:
Acreditar y probar la concurrencia de un hecho físico o electrónico.

LEY DE ENJUICIAMIENTO CIVIL

CÓDIGO DEONTOLÓGICO DE LA ABOGACÍA

Plena libertad para utilizar los medios de defensa que estime pertinentes.

PRINCIPIOS:
Oralidad
Contradicción
Concentración
Publicidad
Inmediación

PRUEBA DOCUMENTAL

VALORACIÓN POR LAS REGLAS DE LA SANA CRÍTICA

Coordinadores:

RICARDO OLIVA LEÓN

@RicardoOlivaON

Abogado especializado en Derecho tecnológico y Derecho de sociedades. Actualmente ejerce como letrado y socio responsable del área de Derecho tecnológico de Lexmotive Law Group. Abogado colegiado ejerciente en España y Perú. Doctorando en Derecho Privado europeo por la Universidad de Zaragoza y la Universidad de Roma Tres, en régimen de cotutela. Es profesor de Derecho de Internet en el Curso de Derecho Digital impartido en el Centro Universitario Villanueva, y en el Executive Master Business Innovation (Security & Safety / Medical & Health), impartido en la Universidad Antonio de Nebrija y coordinado por el Grupo GEES Spain. Miembro del equipo ganador del 1º Legal Hackathon de España, realizado en Bilbao en mayo de 2015. Fundador y editor de Juristas con Futuro y autor del blog Des-complicando el Lenguaje Jurídico. Acostumbrado a trabajar en equipos multidisciplinares y multiculturales, es un buscador de alianzas y oportunidades. Visita su web profesional **www.elabogadotecnologico.com** y escríbele a ricardo@lexmotive.com. Junto con Sonsoles Valero Barceló ha sido el encargado de coordinar este eBook.

SONSOLES VALERO BARCELÓ

@sonvalero

Abogada del Ilustre Colegio de Abogados de Madrid. Experta Universitaria en Derecho de Consumo por la Universidad de Salamanca. Especialista en protección de consumidores y usuarios, atención al cliente y resolución de conflictos. Colaboradora de la Oficina Municipal de Información al Consumidor del Ayuntamiento de Zaragoza y de la Dirección General de Protección al Consumidor del Gobierno de Aragón. Habituada a la docencia, ha impartido diversos módulos especializados en Atención al Cliente, Consumidor y Usuario. Además, ha elaborado numerosas guías de protección del consumidor y publicaciones divulgativas para diversas Asociaciones de Consumidores y Usuarios e Instituciones Públicas. En la actualidad ejerce como jurista en el gabinete legal CONSUMLEX, del cual es socia directora. Compagina esta actividad con la realización de fotografías jurídicas para el portal Juristas con Futuro y la coordinación de los desafíos legales propuestos bajo el hashtag #RetoJCF, junto con Ricardo Oliva León. Posee buenos conocimientos en diseño digital y gestión de redes sociales. Infatigable y comprometida le ha dado un toque mágico al formato de este eBook (es la autora de la fotografía de la portada). Puedes escribirle a sonsolesv@juristasconfuturo.com

Patrocinan:

¿Quieres convertirte en

Premium Sponsor de Juristas con Futuro?

Ponte en contacto con nosotros por **email** (info@juristasconfuturo.com o roliva@juristasconfuturo.com) o por **teléfono** (+34 69 95 51 887)

Septiembre 2016

En la Sociedad de la Información es cada vez más común que la información contenida en la red resulte imprescindible como prueba para acreditar un hecho, el incumplimiento de un contrato, la vulneración de un derecho fundamental, la comisión de un delito, la producción de un daño, la publicación de un contenido. Surge el reto de conocer herramientas útiles y fiables, así como identificar a profesionales especializados que nos ayuden a demostrar que la información extraída de Internet no ha sido objeto de modificación o manipulación y que su contenido es, precisamente, aquel que queremos certificar como cierto. Se hace indispensable que todo abogado sea capaz de saber cómo afrontar la incorporación de la llamada prueba electrónica en un proceso judicial así como saber reaccionar cuando la parte contraria le opone un medio de prueba digital que pueda perjudicar sus intereses. En este contexto nace el segundo eBook de Juristas con Futuro titulado **"LA PRUEBA ELECTRÓNICA. Validez y eficacia procesal."** que es el resultado del trabajo de 20 profesionales expertos en la materia y que ahora tenemos el orgullo de presentar a la comunidad jurídica y tecnológica.

Síguenos en:

JURISTAS con FUTURO

eBook

juristasconfuturo.com

ISBN 978-84-617-4743-6