BOLETÍN DEL MINISTERIO DE JUSTICIA

Año LXVIII Núm. 2163 Febrero de 2014

ESTUDIO DOCTRINAL

INCORPORACIÓN AL PROCESO DEL MATERIAL INFORMÁTICO INTERVENIDO DURANTE LA INVESTIGACIÓN PENAL

ANTONIO EVARISTO GUDÍN RODRÍGUEZ-MAGARIÑOS

GOBIERNO DE ESPAÑA
MINISTERIO DE JUSTICIA

ISSN: 1989-4767
NIPO: 051-14-001-0
www.mjusticia.es/bmj

INCORPORACIÓN AL PROCESO DEL MATERIAL INFORMÁTICO INTERVENIDO DURANTE LA INVESTIGACIÓN PENAL*

ANTONIO EVARISTO GUDÍN RODRÍGUEZ-MAGARIÑOS
Secretario Judicial del Juzgado Central de Instrucción nº 6 de la Audiencia Nacional. Doctor en Derecho.

Resumen

El reconocimiento judicial de los soportes electrónicos presenta grandes dificultades para concretar su contenido, tanto por la inestabilidad de la información existente en los mismos como consecuencia de la enorme cantidad de información que es tratada. Estas dificultades han dado lugar a un debate extraordinariamente complejo entre quienes se muestran partidarios de su tratamiento como medios de prueba autosuficiente frente a quienes postulan someter aquellos a las reglas de la sana crítica, tal como se prescribe en nuestra actual LEC. En el presente estudio se aborda la condición propia de la información electrónicamente almacenada, así como las distintas maneras en que dicha información puede quedar identificada y aportarse al proceso en condiciones que aseguren la fiabilidad de la información y el principio de tutela judicial efectiva.

Abstract

The discovery of the electronically stored information faces the major difficulty of selecting their contents, as a result both of the enormous information instability and of the huge amount of information contained in these media. These difficulties have led to an extraordinarily complex discussion, among those who are in favour of its treatment as self-sufficient evidences and those who are dealt with those issues according to the general rules of the burden of proof laid down in the Spanish procedural rules. In this paper, it will be analyzed the nature of the stored electronically information, as well as the different ways on this information must be identified and provided to the Court and all of this in order to ensure its reliability and to the respect to the Principle of the Due Process in Law.

Palabras claves

Volcado informático, desprecinto, clonación,

Key words

Stored electronically information, legal evidence

* Fecha de recepción: 12-12-2013. Fecha de aceptación: 31-1-2014.

SUMARIO

1- DOCUMENTOS ELECTRÓNICOS Y SOPORTES ELECTRÓNICOS

Conforme a su sentido etimológico derivado de su raíz latina, «*docere*», documento es aquel objeto material que por si solo tiene la virtualidad de mostrar o dar a conocer una determinada información.[1] Exige por tanto que un conjunto de información quede incorporada de forma inescindible en algún tipo de soporte, sea papel, pergamino, piedra, madera, etc. Esta inescindibilidad entre continente y contenido es su nota esencial, hasta el punto que cuando la información originalmente contenida en un material ha sido alterada o sustituida por otra, solemos entender que se ha producido una falsificación. Esto es así, porque al proceder de este modo se rompe la correspondencia entre continente y contenido y por ende la identidad de la información, perdiendo el documento la funcionalidad que le es propia.

En principio, en el documento en papel cualquier alteración es fácilmente perceptible, en cuanto que, una vez impresa en el papel, la tinta queda fijada de modo indeleble al soporte, resultando imposible materialmente separar uno de otro. Lo cierto, sin embargo, es que aún tratándose de soporte papel, siempre existió la posibilidad de realización de documentos por otros medios que no presentaban ese carácter inescindible. En el documento realizado con lápiz es posible borrar el contenido. En éste, ciertamente cabe la realización de una pericial que nos permitiese reconstruir lo borrado, pero resultaría imposible determinar si ha habido ulteriores adiciones o modificaciones en el documento y cuál fue su contenido original. Así, si borramos un digito del documento varias veces y lo sustituimos por otro, quizás podamos identificar su autor y en algún caso reconstruir las trazas de alguno de los mensajes originales, sin embargo este medio de prueba no resultaría definitivo, pues nunca sabríamos cual es el dígito que se propuso el autor originariamente escribir al hacer el documento. [2]

La transformación que ha supuesto la aparición de la era digital y la desaparición del soporte papel, impone también **identificar de forma diferenciada** la información contenida en un soporte electrónico, entendido este como el medio en el que aquella será preservada. En principio el solo soporte electrónico permite recibir y tratar la información, como también, en mayor o menor medida, la identificación de su origen y de las alteraciones que se hayan producido en el mismo, sin embargo en puridad no cabe identificar un contenido propio, pues éste va cambiando conforme a las necesidades del sistema donde se encuentra inmerso.

---

[1] Núñez Lagos define el documento como una cosa mueble corporal que enseña algo, corporeidad y docencia son sus notas, (Núñez Lagos, R. "La fe pública", Revista internacional del Notariado, 1958, tomo 43, p. 305-342). Por su parte Prieto Castro entiende por documento el objeto en que consta una expresión por escrito. Otros autores ciertamente atienden además al hecho de que el material donde se documenta la información sea susceptible de ser llevado ante el juez (Guasp) o simplemente que el material pueda asimilarse al papel (Almagro Nosete). Modernamente el concepto de documento atiende a la posibilidad de reconstruir la realidad a través de un medio material determinado, así Suzanne Briet define el documento «*Tout indice concret ou symbolique, conservé ou enregistré, aux fins de représenter, de reconstituer ou de prouver un phénomène ou physique ou intellectuel»* (Briet, S. *Qu'est-ce que la documentation,* Edit, Paris, 1951. p. 7). Sin embargo, si la funcionalidad propia del documento atiende a este carácter representativo de la realidad, su identidad como medio jurídicamente eficiente debe atender al medio mismo considerado y no a la función que se predica del mismo. Así para Levy, M. David, los documentos surgen por la necesidad humana de crear estabilidad en un medio cambiante, estableciendo marcas reconocibles, susceptibles de identificar la información y de replicarse, esto es, de permitir la distribución de un conjunto ilimitado de copias todas las cuales son capaces de preservar su forma y en consecuencia de trasladar su contenido de forma estable en el tiempo. Levy, M. David, "In ECHT '94: Proceedings of the 1994" *ACM European conference on Hypermedia technology,* 1994, pp. 24-31.

[2] Levy pone el ejemplo del caso del Ulysses de Joyce para poner de manifiesto lo relativo de la estabilidad de la información. La novela como es conocido fue escrita durante siete años, durante este tiempo Joyce añadió más de 100.000 palabras y fue finalmente pasada por impresores que no hablaban inglés. Hubo al menos ocho ediciones incluyendo la edición crítica de 1988 las cuales estuvieron sujetas siempre a una importante controversia. Es difícil saber cuál llegó a ser la edición definitiva para su autor, y desde luego no parece seguro afirmar que pudiera haber llegado a fijarse un texto definitivo. Ciertamente para la mayoría de los lectores el Ulyses es tenido como una obra definitiva, como una estable entidad, sin embargo para los investigadores, mirando críticamente el resultado alcanzado, cabe hablar más bien de un fluido de manuscritos y ediciones que son igualmente eficaces y de interés para conocer la personalidad de la obra. Según Levy fijación y fluidez son conceptos dependerán de la perspectiva del observador. Levy, M. David, "In ECHT '94: Proceedings of the 1994" *ACM European conference on Hypermedia technology,* 1994, p 27.

Para que el soporte electrónico tenga el carácter de un verdadero documento es necesario que la información quede fijada de forma estable, de modo tal que no se haga posible su alteración, de modo que sea posible identificar la información y su tratamiento autónomo. Son estos datos identidad y tratamiento jurídico diferenciado los establecidos por nuestro legislador para determinar la condición de un documento electrónico. En tal sentido el artículo 3 de la Ley 56/2007 de 28 de diciembre de medidas de impulso a la sociedad de la información señala *que tan sólo deberá considerarse tal (documento electrónico) a aquél que fuese susceptible de contener información de cualquier naturaleza, que permita archivar su contenido en un soporte electrónico según un formato determinado, susceptible de identificación y de tratamiento diferenciado*.

Se exige por tanto que a través de medios físicos o técnicos se pueda identificar la información contenida en un soporte electrónico, véase mediante el volcado de su información a un medio indeleble, el empleo de programas bloqueadores o a través de programas que permitan encriptar la información mediante la firma electrónica. Cuando el conjunto de la información no es identificable temporal y espacialmente cabe hablar simplemente de un conjunto de datos (información electrónicamente almacenada conforme a la terminología anglosajona), pero sin que a estos pueda darse un tratamiento jurídico diferenciado. [3] El documento electrónico al constituir un medio de prueba en si mismo considerado, exige la identidad de la información comprendida en el mismo, la determinación de su fecha y la identificación de su autor, sin embargo, la concreción de estos extremos admite como en cualquier otro documento en papel diversos grados de intensidad. Así, la ley de firma electrónica junto al documento electrónico al que anteriormente nos hemos referido distingue el documento electrónico firmado electrónicamente (aquel que permita identificar el contenido con un autor conocido) y como sistema aún más perfecto el documento firmado mediante firma electrónica avanzada (aquel en el que la firma electrónica avanzada está basada en un certificado reconocido y ha sido generada mediante un dispositivo seguro de creación de firma). [4] Estos documentos en

[3] No por ello, ambas especies, documento electrónico y soporte electrónico, dejan de tener su virtualidad propia en orden al almacenamiento de información. Cierto sector de la doctrina de forma irreflexiva a nuestro juicio, Gómez Soares, Sanchis Crespo, Mira Ros y otros, se han postulado en favor de dicha identificación por estimar que la contraria responde un perjuicio atávico frente a los inexorables avances tecnológicos, no siendo sino una reticencia del viejo modelo procesal fundamentado en el soporte papel. Sea como fuere la tendencia en nuestra legislación es la de equiparar unos y otros, así el artículo 230.2 de la LOPJ, equipara unos y otros siempre que quede garantizada la autenticidad, integridad y el cumplimiento de los demás requisitos procesales. Por su parte, el artículo 7 bis de la Ley del Notariado en la regulación dada al mismo por la Ley de Medidas Fiscales, administrativas y de Orden social de 27 de diciembre de 2001, asimila el documento electrónico entre los medios de prueba documentales: *"Los instrumentos públicos a que se refiere el artículo 17 de esta Ley, no perderán dicho carácter por el sólo hecho de estar redactados en soporte electrónico con la firma electrónica avanzada del notario y, en su caso, de los otorgantes o intervinientes, obtenida la de aquel de conformidad con la Ley reguladora del uso de firma electrónica por parte de notarios y demás normas complementarias".* También, en este sentido se muestra la redacción inicial de la Ley de Firma Electrónica que identifica al documento electrónico con el documento con firma electrónica. El propio código penal en su art. 26 da a entender que el documento es cosa distinta al soporte que le sustenta. Sin embargo, esta virtual equiparación de los documentos electrónicos con los documentos tradicionales no se corresponde exactamente con la regulación de los medios de prueba contenidos en las leyes procesales. Así el art. 299.2 de la LEC, acoge aquéllos fuera de la relación de los medios de prueba propiamente dichos, significando como tales 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. A primera vista, podría parecer que los documentos electrónicos quedan excluidos del epígrafe correspondiente a la documental, estando asimilados a los medios o soportes de dicha documental con un tratamiento semejante al de las cosas objeto de reconocimiento judicial.

[4] Pese a la tendencia legislativa de vincular el documento electrónico a la firma electrónica no cabe asociar necesariamente el concepto de documento electrónico al de firma electrónica. Tal pretensión resulta exorbitante en la medida que la firma electrónica, si bien es el instrumento más completo para fijar el contenido de la información contenida en un soporte electrónico, no puede pretender la exclusión de otros medios mecánicos o electrónicos que impidan la alteración del contenido de los soportes informáticos. De este modo, si inicialmente, la Ley 59/2003 de 19 de diciembre vinculó el concepto de documento electrónico a la firma electrónica, con posterioridad a aquella, la ley 56/2007, 28 de diciembre de Medidas de Impulso a la sociedad de la información, al otorgar una nueva redacción al artículo 3 de la Ley de Firma Electrónica (en adelante LFE), vino a modificar la definición de documento electrónico para alinearla en mayor medida con los conceptos utilizados en otras

cuanto tales pueden gozar como todo documento de la condición de documentos públicos[5] y en su caso documentos judiciales.[6]

Sin embargo, la información electrónica a que se accede desde la investigación penal carece normalmente de esta condición, exigiendo su individualización e identificación para acceder al proceso y poder ser examinada. Para la realización de este examen de modo que pueda identificarse su contenido y contrastar la indemnidad del documento, se suele emplear sistemas de resumen de su contenido como los sistemas que emplean el algoritmo *HASH*. El *«hash»*, que está en la base de los programas de firma electrónica avanzada, es una función que permite la realización de un resumen de la información contenida en una cadena de dígitos, y posibilita con ello identificar probabilísticamente un gran conjunto de información con otro subconjunto menor que participaría de la misma función algorítimica. La relación matemática o algoritmo es siempre la misma de modo que cualquier alteración del conjunto afecta al subconjunto y viceversa. La ventaja de la identificación de la información electrónicamente almacenada en un soporte informático a través del *hashing* es doble: en primer lugar permite identificar el contenido efectivo de la información, posibilitando así el acceso indiscriminado a su contenido sin riesgo para el documento original, y de otra parte, da a la información obtenida el tratamiento de verdadero documento, esto es, produce su virtualidad por si misma sin necesidad de una valoración jurídica ulterior. En tal sentido el *hashing* viene a hacer la función que el cotejo visual entre original y copia en los documentos tradicionales.

A diferencia del documento electrónico, lo característico de los **soportes electrónicos** es el carácter esencialmente mudable de la información contenida en los mismos. Ciertamente cabe plasmar la información contenida en aquel en un momento dado mediante el volcado a un medio indeleble, pero entonces el soporte electrónico adquiere una nueva condición cual es la de documento propiamente dicho. Pese a estas dificultades, el soporte electrónico no carece en absoluto de valor, siendo el medio normal de análisis de los soportes informáticos cuando el flujo de información es masivo o cuando los hechos investigados no tienen la relevación bastante como para documentarlos en forma. En tal caso, la virtualidad de dicho medio de prueba vendrá determinada por el contexto en que fuese encontrado y la seguridad de la cadena de custodia. Es por esto por lo que, el artículo 384.3 de la Ley de Enjuiciamiento Civil, remite para su valoración a las reglas de la sana crítica y no de la prueba tasada propia de los documentos. Para algunos autores, esta previsión determina hacer de peor condición al documento en soporte electrónico respecto del documento en soporte papel tradicional al cual se le aplican las reglas de prueba legal.[7] En mi opinión y conforme a la distinción entre

normas españolas de carácter general y en los países de nuestro mismo entorno según expresa el Preámbulo de la propia Ley. La propia Ley 18/2011 ha venido a reconocer la insuficiencia de los sistemas de firma electrónica al reconocer junto a los sistemas de firma electrónica avanzada el empleo de otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen.

[5] La Ley 56/2007 de 28 de diciembre identifica el documento público electrónico, como aquel que por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso (art. 3.6.a. de la Ley 56/2007 de 28 de diciembre).

[6] Las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el propio interesado o por las oficinas judiciales, manténgase o no el formato original, tendrán inmediatamente la consideración de copias auténticas con la eficacia prevista en las leyes procesales, siempre que el documento electrónico original se encuentre en poder de la oficina judicial donde haya sido originado o incorporado y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan comprobar la coincidencia con dicho documento. Si se alterase el formato original, deberá incluirse en los metadatos la condición de copia. (Art. 27.1 de la Ley 18/2011 de 5 de julio reguladora de las tecnologías de la comunicación y la comunicación en el ámbito de la Administración de justicia).

[7] Para Gomes Soares si un soporte informático sustituye a un documento tradicional, el reconocimiento del mismo por la parte a quien perjudique, debe constituir un supuesto de prueba tasada, pues si no fuese así, sería tanto como penalizar con la prueba libre la utilización de los avances informáticos, y premiar con la prueba legal el mantenimiento de las formas tradicionales. Gomes Soares, Fernanda Sabah, "La prueba en la contratación electrónica de consumo", Revista Internacional

documento y soporte electrónico que hemos apuntado, tal previsión es plenamente coherente, siendo consecuencia del carácter incompleto del soporte electrónico como medio de prueba atendida la falta de determinación definitiva de sus contenidos.[8]

Un estadio más en la inestabilidad de la información electrónicamente almacenada se produce cuando la información identificada de forma diferenciada por su autor se incorpora directamente al proceso comunicativo a través de un sistema de vínculos compartidos. En tales casos no es posible identificar aquella dentro de un soporte determinado quedando al arbitrio de otros usuarios que pueden a su vez acceder y proceder al ulterior tratamiento de los vínculos. Tal es el caso de los **sistemas informáticos fijados a través de hipertexto**, en los cuales, por medio de una serie de intercambios de información actualizada a través de hipervínculos y nódulos, el contenido queda al albur de los intercambios entre los distintos usuarios del sistema. Un buen ejemplo de cuanto se está diciendo sería el caso de la página web en que incluyamos una fotografía a través de una dirección IP, lo normal es que el hipervínculo nos presente la fotografía originalmente querida, pero que pasa cuando la fotografía es cambiada por el usuario que ha creado el vínculo de origen, hasta que punto somos ajenos a esta nueva versión del documento. Cabría pensar que la información de la que somos responsables únicamente sería la querida, pensada y publicada originariamente y en tal sentido podría ser identificada y discriminada respecto de aquellos datos no queridos y que se han visto afectados por la actualización del sistema. Pero que ocurre cuando estos hipervínculos carecen de estabilidad alguna de modo que el documento resultante no sea sino la contribución de una colectividad anónima de individuos, y sobre todo, que ocurre cuando el hipervínculo se encuentra mutuamente consensuado o la información es consecuencia de sistemas de mutuo intercambio como es el caso de los sistemas peer-to-peer (P2P), en que medida somos responsables de los cambios producidos. Este es a nuestro juicio el punto final de toda esta evolución. Llegados a este punto la información se abstrae completamente del soporte desapareciendo aquella correlación con un material sensible que durante cientos de años había sido el único modo de obtener su tratamiento jurídico diferenciado. Al proceder así, no existiendo referencia sensible, la identificación de la información de un documento vendrá amparada únicamente en la intención de fijar de forma más o menos estable sus contenidos.[9]

En el presente trabajo abordaremos el modo de incorporar al proceso la información electrónicamente almacenada —documentos electrónicos, soportes electrónicos e

sobre estudios de Derecho Procesal y Arbitraje, nº 3, 2009. En igual sentido Sanchis Crespo, Carolina (1999): *La prueba por soportes informáticos,* Valencia, Tirant lo Blanch, 1999, p. 41

[8] La regulación de la LEC se centra en la regulación de los efectos informáticos como soportes informáticos desconociendo la categoría del documento electrónico, para cuya equiparación ha de acudirse a normas extrañas al texto procesal. La ausencia de preceptos procesales en el Anteproyecto de la LEC que regulen estos aspectos fundamentado en el *numerus apertus* de fuentes de prueba, que se reconocida en el artículo 354 del borrador, hoy art. 351.3 de la Ley. Tal vacío fue advertido CGPJ, que en informe al Anteproyecto solicitó la revisión del texto para acomodar esta concepción a una época en la que transcripción al papel de pensamientos, ideas informes… está siendo progresivamente sustituida por la generalización de las herramientas informáticas, el soporte electrónico y los medios audiovisuales». Sea como fuere a lo largo de su articulado se deja sentir la tendencia a la tendencia a la equiparación de unos y otros, así el artículo 265.1, que hace extensiva la obligación de la aportación de la documental a los medios e instrumentos a que se refiere el ap. 2º del artículo 299. En igual sentido el art. 812.1,1ª respecto del procedimiento monitorio que admite como fundamento para su admisión a trámite la aportación de documentos, cualquiera que sea su forma y clase o el soporte físico en que se encuentren, que aparezcan firmados por el deudor o con su sello, impronta o marca o cualquier otra señala, física o electrónica proveniente del deudor.

[9] Bolter y otros autores consideran que el hipertexto son jardines con senderos que se bifurcan, tomando la cita de la conocida frase de Borges, estimando que dos lectores no tienen necesariamente por que seguir el mismo camino, ni necesitan seguir ambos caminos a la vez. En tal sentido argumenta que el lector, mediante su elección activa puede elegir los elementos a través de los cuales construir su lectura. El concluye que este mundo de multiplicidad, múltiples caminos, múltiples posibilidades, múltiples voces, múltiples lecturas y múltiples lectores que participan como escritores en el acto de la lectura, hacen del carácter definitivo de un documento una mera ilusión. La cuestión sin embargo no ha de ser tratada tanto desde el punto de vista del receptor en que efectivamente puede existir una mayor o menor incertidumbre, como el propósito que anima al individuo a compartir la información o el posibilismo que quiera dar a la misma al permitir su acceso a ciertos contenidos. Bolter, J. D., *Writing Space: The Computer, Hypertext, and the History of Writing*. Hills&le, New Jersey: Lawrence Erlbaum Associates, 1991, p.139.

hipertexto—, desde el punto de vista de la identificación de su origen y su tratamiento jurídico diferenciado, partiendo para esta tarea de su tratamiento documental como medio que establece el grado más alto de fijación de sus contenidos y siguiendo por aquellos otros, que carentes de la estabilidad necesaria, exigen medios técnicos o periciales para su tratamiento jurídico diferenciado.

2- CONSECUENCIAS DE LA DISTINCIÓN ENTRE LOS DISTINTOS TIPOS DE ALMACENAMIENTO DE LA INFORMACIÓN ELECTRÓNICA.

De todo lo cual y resumiendo lo dicho cabe deducir una distinta eficacia en orden a su incorporación al proceso de unos y otros:

- **En cuanto a su autosuficiencia**. A diferencia del soporte electrónico el documento electrónico hace prueba por sí mismo.[10] El soporte electrónico y el hipertexto, por el contrario, sólo merece la calificación de pieza de convicción, y como tal su apreciación como medio de prueba está sujeta a las reglas de la sana crítica (véase art. 299.2 LEC).

- **En cuanto a su integridad.** Tratándose de soportes electrónicos cada una de las distintas unidades de almacenamiento informático, en su multiplicidad de versiones, puede ser considerada bien como un solo cuerpo, la totalidad de la información del soporte electrónico en sus distintos momentos temporales. Por el contrario el documento electrónico no atiende al soporte material sino a la información contenida en el mismo y al método para reconocer un conjunto de información estable, cuya concreta identidad dependerá de la eficacia que pretendamos dar a la información contenida en aquellos al salir del entorno en que se encuentra.

- **En cuanto a su identidad.** Por último, cabe distinguir una distinta función en orden a su acceso al proceso. Respecto del soporte su eficacia en el proceso dependerá de la fidelidad de la cadena de custodia. ¿Cómo se consigue esto si es de esencia a estos su continua mutabilidad? Para ello, habremos de atender al modo de exteriorización de su contenido, bien documentando la extracción de los datos o la realización de imágenes de su contenido que permitan la realización de los posteriores análisis periciales, bien contrastando la información con otros soportes informáticos que estén en conexión con aquel o bien, en último término, autenticando total o parcialmente la

[10] Esta confusión entre el alcance del soporte electrónico y el documento electrónico es bastante común. Así en el ámbito de la Administración Pública pese a la grandilocuencia con la que se suele presentar la importancia de dichos documentos su eficacia es bastante limitada. Así la Ley 11/2007, de 22 de junio, sobre el Acceso Electrónico de los Ciudadanos a los Servicios Públicos, pese al reconocimiento explicito del documento electrónico, a través de las diversas alusiones a *"procedimientos administrativos gestionados en su totalidad electrónicamente"* (art. 37), a su iniciación *"a solicitud del interesado por medios electrónicos"* (art. 35.1) y una *"instrucción por medios electrónicos"* (art. 36), incluso a la *"terminación de los procedimientos por medios electrónicos"* o la *"resolución de un procedimiento utilizando medios electrónicos"* (art. 38), lo cierto es, que de forma más discreta, establece algunas reservas frente a la digitalización del procedimiento administrativo, como la previsión del posible requerimiento de cotejo con sus originales de las copias digitalizadas aportadas al procedimiento (art. 35.2) y, sobre todo, por la salvedad (formulada por el art. 38.2) de que *"podrán adoptarse las resoluciones en forma automatizada en aquellos procedimientos en los que así esté previsto"*. Como señala MIRA ROS, a la hora de la verdad, el acto administrativo por antonomasia que es la resolución administrativa, por regla general, no cabe en formato electrónico sino existe una expresa previsión en tal sentido. Ese mismo escepticismo legal frente a la digitalización administrativa asoma también detrás de la obligación de mantener, en todo caso, las llamadas *"oficinas de atención presencial"*, art. 7,2,a. de la Ley 11/2007 de 22 de junio, (MIRA ROS, Corazón. "¿Una justicia por ordenador?" Revista del Notariado, Marzo-Abril 2010, n º 30).

información mediante la firma digital, lo que transmutará su naturaleza en un verdadero documento electrónico.[11]

El caso es que no siempre es posible, ni necesario proceder al examen de la información electrónicamente almacenada con todas las garantías que implica su incorporación al proceso como un elemento documental. En muchos casos, la información contenida en los soportes electrónicos presenta un grado de inestabilidad tal —véase el caso por ejemplo de la contabilidad financiera— que no es posible materialmente proceder a la interrupción de los procesos informáticos haciéndose necesario contrastar dicha información a través de otros medios o adoptar otro tipo de garantías.[12] Es en este punto, donde en los últimos tiempos se ha presentado una importantísima polémica, tanto para determinar la procedencia de uno y otro medio, como para apreciar la diligencia y comportamiento de las partes en torno a la conservación de la información electrónicamente almacenada. Se hace preciso abordar por tanto el tratamiento de este tipo de información desde ambos puntos de vista para entender las limitaciones que en cada caso puede presentar su incorporación al proceso.

3- INCORPORACIÓN DE LOS DOCUMENTOS ELECTRÓNICOS AL PROCESO.

3.a- La integridad del material informático. El cálculo del algoritmo hash.

Como ha quedado señalado el contenido de los soportes informáticos, pese a que pueden mostrar o almacenar información, se distingue del de los propios documentos al carecer del requisito del carácter definitivo propio de aquellos y de la inescendibilidad entre continente y contenido. Una de las características que se atribuye por la conferencia SEDONA a los soportes informáticos es su carácter esencialmente dinámico.[13] Como ha quedado señalado, los efectos informáticos, a diferencia del resto de piezas de convicción, están continuamente modificándose, de modo que mientras que el ordenador esté en funcionamiento, aunque no esté bajo el control de un concreto usuario, se están produciendo procesos informáticos, rutinas, que modifican continuamente sus contenidos. La información así obtenida impide su tratamiento diferenciado al no poderse contextualizar la información hallada en los mismos.

Esto determina la necesidad de que al tiempo de ser incautados se proceda a interrumpir estos procesos y a congelar su contenido impidiendo que siga modificándose la información, preservando así la información de la interferencia de otros usuarios. Para llevar a efecto este cometido, los protocolos procesales generalmente admitidos exigen proceder a interrumpir estos procesos tan pronto como los efectos informáticos sean aprehendidos y a congelar la información procediendo a la realización de una imagen que permita su análisis sin sospecha alguna de que en el curso de la investigación esa información se pueda ver alterada. A través de estas copias se permitirá en lo sucesivo la realización de cuantas periciales y análisis sean necesarias sin que los soportes originales queden afectados. [14]

[11] La intervención de un técnico en derecho que controle como se llevan a efecto estas operaciones, a nuestro modo deber, facilita mucho las cosas frente a otros países en los que faltando la fe pública tienen que someterse a rígidos protocolos para asegurar la cadena de custodia, siendo el motivo más común para solicitar la nulidad de actuaciones.

[12] En este punto es donde es de especial relevancia apreciar el comportamiento y la diligencia de las partes en orden al proceso, cuestión de enorme importancia en el derecho norteamericano cuya fiscalización a través de la diligencia e-discovery tratamos extensamente en otro trabajo, al que nos remitimos. Gudín Rodríguez-Magariños, Antonio Evaristo, "Búsqueda y conservación de los datos informáticos en el Derecho norteamericano E-discovery", *Estudios de Deusto: revista de la Universidad de Deusto*, vol. 58, Nº. 2, 2010, págs. 205-245

[13] *The Sedona Principles. Best practices & principles for adressing Electronic Document Production, annoted versión*, Coordinador Jonathan M. Redgrave, Sedona Conference, 2005, pp. 7 y 8.

[14] En el ámbito del proceso anglosajón es donde existe un mayor desarrollo de estos protocolos para el tratamiento de información electrónicamente almacenada, véase en tal sentido *English Rules Under the Judicature Act (The Annual Practice*, 1937) O. 31, r.r. 14, *et seq*. En el ámbito norteamericano la regulación de estos procesos se contiene en New York Civil Practice Law and Rules, Michigan Court Rules Ann. (Searl, 1933) Rule 41, §2, si bien se admite tanto el acceso directo

Para la realización de este examen comparativo entre el original y las copias, de modo que pueda identificarse su contenido y contrastar la indemnidad del documento, se suele emplear funciones matemáticas que permiten identificar el contenido de los soportes con gran precisión. El "hashing", es una técnica basada en la idea de que es bastante para identificar un conjunto de información la obtención de un resumen matemático de la misma. De este modo a través de una cadena de dígitos se permite identificar probabilísticamente un gran conjunto de información a través de otro subconjunto menor que participaría de la misma función matemática.[15] Dicha relación matemática o algoritmo es siempre la misma de modo que cualquier alteración del conjunto afecta al subconjunto y viceversa, pero sin que el proceso sea reversible, esto es, se puede reconstruir el subconjunto a través del conjunto pero no al revés.[16] Esta técnica es la que está en la base de los sistemas de firma electrónica, suponiendo el hashing de la información un estadio más rudimentario en la práctica de este tipo de diligencias. Ciertamente a través de la firma electrónica las empresas de firma electrónica proceden a automatizar todas estas operaciones, pero debe recordarse que su operativa está pensada más en la generación de los propios documentos que la recepción de información de otros sistemas.[17]

3.b- La diligencia de volcado de la información contenida en soportes informáticos.

Como indicamos al principio, la realización de estas operaciones de clonado o volcado en aquellos países en que la cadena de custodia no está sujeto al control de la fe pública judicial requiere que se realice en determinadas condiciones o garantías, estableciéndose al efectos rígidos controles no sólo para evitar que la información obtenida no sea modificada, sino sobre todo para saber cuál es el origen y el estado en que aquella fue encontrada. En particular en lo relativo a los efectos informáticos, en la mayoría de los ordenamientos jurídicos se proscribe la posibilidad de proceder a realizar cualquier modificación o alteración en aquellos hasta que se procede a la clonación de su contenido. Concretamente, en los países que cuentan con la existencia de un juez de garantías, se establece además la necesidad de que se informe puntualmente de la incautación de cualquier efecto informático, desde el mismo momento que es identificado por la policía, debiendo ésta informar y dar cuenta de su estado en todo momento a dicha autoridad judicial.[18]

En nuestro ordenamiento procesal, la regularidad de la cadena de custodia y la responsabilidad sobre los efectos de convicción se encuentra atribuida al Secretario Judicial (459 LOPJ).

como la realización de copias para análisis en función de las circunstancias del caso, en tal sentido, la regla 34 de las Federal Rules of Civil Procedure, cuyo concreto alcance ha sido matizado por la corriente doctrinal que surge del caso Zubulake v. UBS, 2004.

15 Vid. Gettys, T., "Generating perfect hash function", Dr. Dobb's Journal, Vol. 26. No.2, 2001, pp.151-155.

16 Las propiedades fundamentales del *hashing: a) Reduccionismo o identificación de la información a través de subconjuntos sensiblemente menores y más manejables.* En realidad su funcionamiento no es distinto los dígitos control de las cuentas corrientes, lo determinante del HASH es la posibilidad de poder tratar grandes volúmenes de información, en un tiempo relativamente corto y de forma sensiblemente más manejable; b) *Determinismo:* implica que si dos resultados de una misma función son diferentes, entonces las dos entradas que generaron dichos resultados también lo son; c) *Uniformidad.* Una buena función HASH debe asignar los aportes esperados del modo más uniforme posible. Es decir, todos los valores HASH deben contar aproximadamente con el mismo nivel de probabilidad. La razón de este último requisito es que el resumen de los contenidos basados en el HASH debería aumentar proporcionalmente a medida que el número de situaciones de conflicto aumenta. Básicamente, si algunos valores hash son más probables que otros, los algoritmos de búsqueda deberán buscar un subconjunto más amplio que permita identificar al conjunto inicial; d) *Unidireccionalidad.* A través de la función HASH podremos reconstruir siempre el mismo subconjunto, sin embargo no cabe reconstruir desde el subconjunto resumen el conjunto inicial.

17 Véase en este sentido los arts. 27 y 28 de la Ley 18/2011 de 5 de julio reguladora de las tecnologías de la comunicación y la comunicación en el ámbito de la Administración de Justicia.

18 Véase artículos 82 y ss. del Código Procesal Penal de Colombia, desarrollo de las previsiones contenidas en el artículo 250.3 de la Constitución Nacional de Colombia que establece que se deben asegurar los elementos materiales de probatorios garantizando la cadena de custodia mientras se ejerce su contradicción.

Es a este funcionario al que corresponde valorar y dejar constancia sobre el modo en que se han incorporado a las actuaciones tales efectos al señalar que *los secretarios judiciales responderán de los bienes y efectos afectos a los expedientes judiciales, así como de las piezas de convicción en las causas penales*. Sin embargo, pese a la importante función que ejerce este, parece que no existe todavía conciencia en nuestro acervo jurídico de las consecuencias materiales que determina alterar cadena de custodia en los efectos informáticos y la necesidad de catalogación del momento y lugar en que estos han sido hallados. Así las sentencias del Tribunal Supremo, no han acertado a determinar el concreto alcance de estas diligencias. La sentencia del Tribunal Supremo Sala 2ª, de 15 de noviembre de 1999, (Martín Pallín, La ley 2501/2000), establece de manera literal: «*En lo que se refiere a lo que se denomina "volcaje de datos", su práctica se llevó a cabo con todas las garantías exigidas por la ley. En primer lugar, la entrada y registro se realizó de forma correcta y con la intervención del secretario judicial que cumplió estrictamente con las previsiones procesales y ocupó los tres ordenadores, los disquetes y el ordenador personal. Lo que no se puede pretender es que el fedatario público esté presente durante todo el proceso, extremadamente complejo e incomprensible para un profano, que supone el análisis y desentrañamiento de los datos incorporados a un sistema informático. Ninguna garantía podría añadirse con la presencia del funcionario judicial al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia».* Dicha sentencia, además argumenta, que cualquier manipulación sobre la evidencia digital o incorrección en el informe pericial que quiera ser comprobada por las partes pudo ser efectuada mediante un contraperitaje por terceros especialistas ajenos a las fuerzas de seguridad. Lo que desconoce la sentencia es que efectuado el análisis pericial los datos de dichos soportes informáticos pueden perder la consideración de tales al haberse modificado substancialmente la información en los mismos contenida. En realidad la sentencia citada se dicta en un momento en el que el estado de la ciencia y de la doctrina técnico jurídica no había concretado el alcance de las cautelas que debieran de adoptarse en la realización de estas diligencias.

Más cercana en el tiempo es la sentencia de la Sala 2ª del Tribunal Supremo de 20 de octubre de 2008, (Andrés Ibáñez, La ley 68710/2008) en la que nuevamente el tribunal incide en la misma línea argumental, señalando, que *la entrada y registro en el domicilio del que ahora recurre habilitaba a la policía para la incautación, entre otras cosas, del material informático que allí pudiera encontrarse; y fue con esta cobertura como por providencia del día 23 del mismo mes se ordenó el análisis de la información de los ordenadores que ya estaba a disposición del juzgado. Es cierto, que esta última actividad no fue practicada ante el secretario judicial, sino por los técnicos policiales en su propia sede. Pero también lo es que, como razona la Audiencia, esa presencia que se reclama habría sido, de facto, tan inútil -y, por tanto, innecesaria- como la que pudiera darse en el desarrollo de cualquier otra de las muchas imaginables en cuya técnica el fedatario judicial no fuera experto. Por eso, no habría nada que objetar a la intervención de los ordenadores y tampoco al modo en que fueron examinados*. Estos mismos argumentos se reiteran en la sentencia de 22 de mayo de 2009 (Berdugo Gómez de la Torre, La ley 67225/2009).

Las sentencias indicadas parten del tratamiento de los soportes informáticos como efectos judiciales sujetos a juicio pericial. A mi entender, sin embargo, son bastantes las razones que aconsejan proceder a la clonación de los soportes periciales y documentar los mismos dentro del proceso como verdaderos documentos electrónicos, pudiéndose destacar las siguientes:

- Al objeto de valorar adecuadamente las **circunstancias de la incautación de los soportes**. La diligencia de clonación permite fijar el contenido existente en la fecha más próxima a la incautación, permitiendo asimismo la apreciación de la proximidad de los sucesos, por lo que no se trata tanto del análisis de los datos como, cuando y en qué condiciones fueron encontrados dichos datos y que virtualidad cabe predicarse de los mismos.

- Por razón del **principio contradictorio**. Permite realizar ulteriores copias que permitan su análisis por todas las partes intervinientes en el proceso. El artículo 479, señala que *si los peritos tuvieran necesidad de destruir los objetos que analicen, deberá conservarse a ser posible, parte de ellos a disposición del juez para que en caso necesario pueda hacerse nuevo análisis.* Ciertamente estas dificultades pueden evitarse mediante el empleo de bloqueadores de escritura pero el remedio es parcial, pues su empleo parte de una presunción que se debería hacer extensiva a todos los peritos y la posibilidad de pérdida de información resulta un riesgo que queda fuera del control del Tribunal.

- Por razón de su integración material del soporte documental en **ulteriores procesos.** La diligencia de clonación permite realizar ulteriores copias con los requisitos de integridad suficiente para hacer fe en otros procedimientos. Véase en este sentido el artículo 28 de la *Ley 18*/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

- Por razón de su **eficacia probatoria**. Sólo la información contenida en documentos electrónicos puede hacer prueba plena en juicio, estando sujeta la contenida en el resto de los soportes a la regla de la sana crítica.

Ciertamente como hemos anticipado anteriormente no siempre es posible, ni conveniente proceder al clonado de toda la información electrónicamente almacenada, pero siempre que se pueda llevar a efecto la identificación de aquella como medio de prueba de cargo, la identificación de su contenido se muestra como una garantía estrictamente necesaria para que aquella pueda desenvolverse con plenitud de efectos.

3.c- La diligencia de desprecinto y clonado.

La operación de clonado pretende tres efectos: la realización de un volcado parcial o total de la información, la identificación de dicha información mediante la técnica del “hashing” y la obtención de una copia exacta de la información extraída de los soportes electrónicos. Tal operación no supone una medida intromisiva, sino únicamente garantizadora de la identidad de la información, suponiendo una exigencia mínima impuesta por los protocolos de actuación policial en todos los pases de nuestro entorno cultural.[19] En tal sentido entendemos que no es necesario requerir la autorización judicial para la realización del simple cálculo algorítmico que identifique el contenido de dichos soportes. Tal diligencia no sería sino una descripción de la externalidad del objeto incautado pero no altera, ni queda afectada la información sensible que el mismo pueda contener. Otra cosa es el tiempo y las circunstancias en que se procede a la identificación del contenido del material informático y la exposición que en este tiempo aquél pueda haber llegado a estar expuesto. Tal circunstancia explica que para evitar cualquier tipo de recelos, la práctica forense haya arbitrado la necesidad de proceder a precintar los soportes informáticos incautados y sólo cuando quede autorizado judicialmente el acceso a dicha información, proceder a un tiempo a la realización de ambas diligencias inmediatamente a continuación del desprecinto judicial. La función de esta diligencia es doble constatar el tiempo en que se ha producido el proceso de clonación e identificar su contenido. Lo primero se verificará determinando las circunstancias en que fue aprehendido, las medidas establecidas para preservar el acceso a los puertos del sistema, señalando en su caso el tiempo en que ha quedado expuesto a la alteración de su contenido, o constatando que la clonación se ha producido inmediatamente a la incautación o desprecinto de los efectos. La identificación del contenido se llevará a efecto mediante la constatación del algoritmo *“hash”,* significando en el acto la cifra numérica resultante.

[19] Véase a modo de ejemplo Good Practice Guide for Computer-Based Electronic Evidence oficial release versión: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

En este sentido, resulta muy ilustrativa la sentencia de la Audiencia Provincial de Cáceres de 20 de octubre de 2008, (Tena Aragón, La ley 221063/2008), la cual declaró la nulidad de la diligencia policial de desprecinto y clonado verificada sin la debida autorización judicial, cuando además, no concurría ninguna razón perentoria para efectuar ese volcado sin impetrar la debida autorización. A juicio de la Sala *«Con ello se produce una vulneración de los arts. 18.3, 18.4 y 18.1 de la Constitución Española, y así se ha expuesto en STS donde se viene siempre interpretando la necesidad de esa autorización judicial, bien expresamente a estos efectos, bien reseñando que esa autorización va ínsita en la de entrada y registro donde conste que se proceda a la incautación del material informático y sistemas informáticos que pudieran encontrarse (STS que se cita en el acto de la vista de 15-11-99 y la más reciente de 14-5-2008, postura jurisprudencial seguida por las Audiencias Provinciales, como la de Madrid, Sección 16 en sentencia de 18-4-2006 y Barcelona, Sección 9, auto de 4-11-2004). De tal forma, que en aquellas jurisdicciones donde no suele ser habitual contar con autorizaciones de entrada y registro porque no son necesarias para hacerse con el material informático, ese acceso al contenido del mismo se declara nulo e inexistente, porque el resultado obtenido supone una invasión a ese derecho a la intimidad, que sólo debe cesar ante una resolución judicial en la que se valoren los principios de proporcionalidad y necesariedad; así podemos citar las STSJ /Sala Social) del País Vasco de 6-11-07, 24-4-2006, 12-9-2006, 21-12-2004; la AN (Sala de lo Contencioso Administrativo, Sección 7º) sentencia de 12-3-2007, sentencia de 18-1-2007 (Sección 2ª). En estas resoluciones se especifica que solo un desprecio absoluto de los derechos a la intimidad y al secreto en las comunicaciones, amparado en la consideración de que aquellos derechos no pueden por definición afectarse a causa del control de un sistema que es propiedad del empleador, podría viabilizar tales conductas. Y desde luego, esa no es la premisa mayor de la que debe partirse, dado que la necesaria integración del ciudadano dentro de la empresa, a fin de obtener medios para su subsistencia, no significa renuncia a los derechos que le significan como tal, siendo éste un punto de partida inaplazable para todos los pronunciamientos encargados de tratar los enfrentamientos entre poderes directivos (libertad de empresa) y derechos fundamentales ya desde la STC 88/1985 (LA LEY 461-TC/1985)».*

3.d- El desprecinto de los efectos informáticos.

Como ha quedado indicado, el volcado de los efectos informáticos y la posterior obtención de una imagen forense de los mismos exige la máxima inmediatez entre el momento de su incautación y el volcado de la información por lo que lo más aconsejable es que el volcado del material informático se lleve a efecto en el mismo momento de su incautación siempre que tal diligencia este autorizada judicialmente. Cuando no sea posible llevarla a efecto en el acto se exige una nueva diligencia, diligencia que no es sino una continuación de la anterior, en el que los efectos, debidamente precintados con las necesarias cautelas para preservar la identidad e integridad de su contenido, son desprecintados con todas las garantías ante la autoridad judicial. Durante este tiempo los soportes informáticos deben ser tratados como efectos judiciales, quedando sujetos por tanto a las garantías establecidas legalmente al objeto de preservar la cadena de custodia.

En tal sentido, la LOPJ confía en el art. 459 de la LOPJ al secretario la obligación del depósito de los bienes y objetos afectos a los expedientes judiciales, así como de las piezas de convicción en las causas penales. Esta función que los secretarios judiciales ejercen bajo la garantía de la fe pública permite que los efectos encontrados durante la investigación queden preservados de cualquier eventual intromisión hasta que por la autoridad judicial se autoriza el acceso a su contenido, siendo por tanto una garantía más que nuestro ordenamiento jurídico otorga a los justiciables al permitir la judicialización y fiscalización de la cadena de custodia por el responsable de la fe pública judicial. Se garantiza así al justiciable la integridad de aquellos, evitando cualquier posible duda que supondría la contaminación de los efectos aprehendidos si aquellos permanecieran en poder de la fuerza investigadora o del propio juzgador.

Esta diligencia exige la presencia del interesado o cuando menos darle la posibilidad de poder estar presente al sólo objeto de que este pueda conocer las circunstancias de la aprehensión

y manifestar lo que tenga por conveniente sobre la identidad de los mismos y los posibles desperfectos que pudieran haberse causado como consecuencia de su traslado a la sede judicial.

3.e- Modo de llevarse a efecto las operaciones de volcado.

La diligencia de volcado de la información no tiene otra finalidad que la realización de una copia, copia que como cualquier otra que pueda hacerse en formato papel, requiere no sólo la duplicación de la información contenida en el mismo, sino también el cotejo con su original para determinar su autenticidad. Tal diligencia para cumplir su función requiere al efecto, como cualquier otra que pueda expedir el secretario, las siguientes premisas:

- La **preservación del contenido**. Para ello es requisito de garantía bastante el empleo de bloqueadores de escritura que impidan modificar el contenido de la información original.

- La **identificación del contenido** mediante el cálculo del algoritmo hash o cualquier mecanismo que permita identificar su contenido.

- El clonado o **realización de una imagen exacta**, (bit a bit) de toda la información extraída que es la que será objeto de examen por el equipo policial.

- Constatación de la **fecha, circunstancias e intervinientes que participan en la realización de la diligencia,** lo cual quedará documentado por el secretario judicial si se quiere dar a la diligencia la condición de verdadera prueba plena en juicio.

4- EXAMEN DE LOS SOPORTES ELECTRÓNICOS.

4.a- Acceso in situ, pantallazos y volcado de la información a soportes indelebles.

La forma más simple y primaria de acceder al contenido de los soportes informáticos es el acceso visual a su contenido aparente. En principio el acceso a los soportes informáticos no debería ser distinto al de cualquier otro efecto judicial. Lo que distingue el acceso a los efectos informáticos es que de su mero examen externo a primera vista no cabe saber qué tipo de información se contiene en los mismos y que garantías deban de adoptarse para proceder a su acceso. Téngase presente que dado el volumen de la información que puede verse afectada y la existencia de varios niveles subliminales de información el acceso inopinado a dicha información pueda conculcar diversos derechos fundamentales.

Junto a la habilitación inicial que posibilita el acceso a este ámbito reservado de la privacidad se hace también estrictamente necesario preservar otra serie de derechos que pueden trastocar la diligencia, particularmente la presencia del interesado que debe visualizar y conocer todas las operaciones que se lleven a efecto y en su caso consentir en facilitar los datos y claves necesarias para que esta se pueda llevar a efecto. En tal caso el consentimiento que se preste debiera darse luego de habérsele instruido de su derecho a no hacerlo y de ser asesorado por letrado de sus consecuencias. La documentación de lo actuado se puede llevar a efecto bien trascribiendo los mensajes de texto o bien mediante realización de pantallazos que permitan

transmutar la información contenida a un soporte indeleble como la impresión de aquellos en papel.

En principio, atendido el objeto de la diligencia, la inspección de los soportes informáticos va indisolublemente unida a la diligencia de reconocimiento judicial. La regulación de este tipo de diligencias en nuestro derecho en los artículos 326 y siguientes de LECRIM partía de una regulación bastante simplista en el que la intervención del juez era central.

Lo cierto es que la tendencia en nuestro ordenamiento es que el juez, quien carece muchas veces de conocimientos técnicos adecuados, suele proceder a delegar estas actuaciones en peritos o expertos policiales. Así se previene respecto de las huellas o vestigios biológicos tras la nueva redacción del párrafo 3º del artículo 326 introducido por la L.O. 15/2003, de 25 de noviembre, conclusiones que se han venido extrapolando a otros ámbitos al amparo de las previsiones contenidas para el reconocimiento pericial.

Por otra parte, la jurisprudencia ha venido posibilitando el acceso a materiales informáticos sin necesidad de una expresa autorización judicial. En tal sentido, ha admitido que la habilitación policial para acceder a la información sensible contenida en los soportes electrónicos se entiende implícita en el auto acordando la entrada y registro. Así la STS de 14 de mayo de 2008, (Andrés Ibáñez, La ley 68710/2008), en la que se significa que la orden de entrada y registro habilita a la policía para la incautación entre otras cosas del material informático que pudiera encontrarse y la STS 27 de junio de 2002 (Ramos Gancedo, La ley 7146/2002) que admitió como lícita la lectura de un mensaje grabado en un móvil porque se encontraba bajo la cobertura de la autorización judicial como si de otro papel o documento que fuese encontrado en el curso de la incautación de la entrada y registro. La STC 70/2002, de 3 de abril, (Garrido Falla, La ley 3534/2002) va más lejos al admitir una habilitación policial implícita en supuestos de flagrancia delictiva y siempre que existan razones de urgencia, necesidad o inmediatez, debiendo en otro caso existir una habilitación previa, no siendo posible una análisis *ex post facto* en función de lo aprehendido, sino ex ante, en consideración a la concurrencia de circunstancias excepcionales, entre las que se encontrará en los dispositivos electrónicos la posibilidad de su borrado, porque de lo contrario la actuación policial al inmiscuirse en la intimidad ajena debería limitarse a la confiscación y el envío del soporte físico en que se conserva adoptando las cautelas necesarias para garantizar y evitar que desaparezca o técnicamente se borre desde otro punto.

El carácter sensible de la información contenida y la imposibilidad de retener aquella hace que de algún modo resulte necesario documentar lo acontecido por el secretario judicial al objeto no sólo de dar carácter fehaciente a la información intervenida, sino también y muy principalmente la de documentar el modo en que se ha llevado efecto y poder valorar si se han preservado o no los derechos de los justiciable.[20]

[20] Así, para Rives Seva el Secretario no sólo da fe sino que garantiza que la intromisión en la inviolabilidad del domicilio se realiza dentro de los límites marcados por el contenido de la resolución. En esta dirección se orientó el Acuerdo de la Junta de Magistrados de la Sala 2ª del TS de 5-11-91 y en tal sentido, la STS de 16 de diciembre de 1991, que declara que la *"irregularidad de la diligencia por la ausencia del Secretario se traduce en su operatividad probatoria, no sólo en la pérdida del valor documental público de dicha acta, sino ella, porque tal acto resulta nulo por falta de los requisitos legales y determinante de indefensión y cuanto se derive de tal diligencia se convierte en nulo".* Por tal razón, resulta muy complejo la subsanación a posteriori de la diligencia, pues se hace imposible reconstruir cual fue y cual debiera haber sido la actuación policial sin la intervención de quien por ley está obligado a velar por la tutelar y documentar la injerencia de los derechos del justiciable. En este sentido cabe citar las STS de 3 de diciembre de 1991 y 23 de abril de 1993. Las dudas e incertidumbre surgidas en el tiempo en que la intervención del secretario no era preceptiva como consecuencia de la reforma del artículo 569.4º por la L.O. 10/92 de 30 de abril, de Medidas Urgentes de Reforma Procesal ponen de manifiesto que la intervención de aquel trascendía del plano de la mera documentación, Durante el tiempo de su vigencia diversos pronunciamientos jurisprudenciales, SSTS de 19 de octubre de 1993 y de 7 de abril de 1994, declararon la nulidad de la diligencia de entrada y registro practicada sin la presencia del secretario judicial, no sólo como requisito para constituir prueba de cargo, sino como garantía añadida a la intromisión domiciliaria. (veáse RIVES SEVA, Antonio Pablo, *La diligencia de entrada y registro domiciliario*, Bosch. Barcelona, 2004, p. 105 y ss)

4.b- Examen cruzado de los datos entre dos soportes informáticos. Los metadatos de los archivos informáticos

Otra forma plausible de comprobar la autenticidad de la información contenida en los soportes informáticos es el de examen comparado de los metadatos contenidos en los archivos informáticos. La conferencia de SEDONA define *los metadatos como la información empleada por el administrador del sistema que refleja datos relativos a la generación, manipulación, transmisión y almacenamiento de los documentos o archivos dentro del sistema informático.* [21]

Para entender la importancia de los metadatos es esencial comprender la forma de incorporación al sistema informático de la información contenida en los archivos y registros informáticos y la forma en que esta queda vinculada al resto del sistema. Tal vinculación que en principio no queda exteriorizada permite identificar la información tanto para vincularla a otros archivos o fuentes de registro como para realizar búsquedas. Esta idea es esencial para el tratamiento electrónico de la información, pues exige preservar los datos más relevantes que permitan su indexación para incorporarlos a las bases de datos del sistema del que dependen. **Esto dota a la información indexada de bastante mayor estabilidad que el resto de los registros del sistema, impidiendo su alteración por parte de cualquier usuario que cuente con los permisos de los titulares o la cualificación necesaria para alterar su contenido.** Téngase presente que la estabilidad del propio programa informático puede depender del tratamiento que se dé a los metadatos.

Los metadatos representan hoy por hoy el punto más interesante para el examen pericial de la información electrónicamente almacenada al permitir interrelacionar la información contenida en los archivos. La configuración jurídica de los metadatos ha sido objeto recientemente de especial preocupación por parte del legislador. El R.D. 1671/2009 de 6 de noviembre por el que se desarrolla la Ley 11/2007 de acceso de los ciudadanos a los servicios públicos, es el primero que trata extensamente esta cuestión. El artículo 47 del Decreto define los metadatos, señalando: *"Se entiende como metadato, a los efectos de este Real Decreto, cualquier tipo de información en forma electrónica asociada a los documentos electrónicos, de carácter instrumental e independiente de su contenido, destinada al conocimiento inmediato y automatizable de alguna de sus características, con la finalidad de garantizar la disponibilidad, el acceso, la conservación y la interoperabilidad del propio documento"*. Por su parte la Ley 18/2011 de las tecnologías de la información en la Administración de justicia distingue el metadato de los metadatos en la gestión de documentos. Los metadatos vienen caracterizados por su carácter meramente instrumental, esto es cualquier dato que define y describe otros datos, mientras que los metadatos de gestión son aquellos metadatos que permiten la identificación de los documentos.[22]

Lo relevante de los metadatos es que al incorporarse en muchos casos a registros públicos o dependientes de un tercero ajeno al sistema permiten contextualizar de un modo fiable los documentos electrónicos. Véase en este sentido, la posibilidad de corroborar la información contable a través de los metadatos existentes en los sistemas de facturación, aspecto en el que el documento electrónico empieza a estar bastante extendido y que ya tiene un grueso cuerpo normativo o también la posibilidad de contrastar la certeza de los correos electrónicos mediante el examen cruzado de las IPs de los remitentes.

[21] Literalmente *«information useful for system administration as it reflects data regarding the generation, handling, transfer, and storage of the document or file within the computer system».* Véase en particular comentario al principle 12*, The Sedona Principles (second edition), adressing electronic document production, 2007, p. 16*

[22] La ley define los metadatos en la gestión de documentos como aquella «información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan»

Sin embargo, la autenticidad de los datos obtenidos, no sólo queda prefijada a través de su incorporación a fuentes de registro públicas, admitiendo diferentes tipos de corroboración:

- Mediante el examen comparado de la información contenida con otros soportes informáticos aprehendidos o que sean conocidos. Véase el caso antes citado de las direcciones IPs que quedan registradas en dos o más terminales que permiten mediante su examen cruzado identificar al autor de los mensajes cuando se acredita su uso exclusivo por alguno de los implicados.[23]

- Corroboración de los metadatos en fuentes de registro no conocidas o de difícil acceso.

- Metadatos incorporados a bases de datos privadas o públicas que tengan por objeto identificar a las personas.

- Metadatos incorporadas a índices de registro ordinales que impidan una alteración del orden del metadato sin la alteración de todo el índice del registro.

4.c- Periciales informáticas sobre soportes electrónicos.

Cuando la información electrónicamente almacenada no ha sido clonada con los medios y garantías adecuados, encontrándose incorporada a un soporte informático, parece evidente que la única forma de análisis es a través de peritos imparciales extraños a la función investigadora. El informe pericial se regula en la Ley de Enjuiciamiento Criminal en los artículos 456 y siguientes desarrollándose en principio ante el juez en forma contradictoria y sin perjuicio de reproducir en el plenario lo actuado en el caso de impugnación. Sin embargo, éste examen contradictorio previsto en la LECRIM, no siempre es posible, e incluso en determinados supuestos, como es el caso de laboratorios oficiales del art. 788.2, debido al funcionamiento propio del laboratorio, ni tan siquiera se prevé la intervención de las partes. Este tipo de prácticas se han venido generalizando y han tomado carta de naturaleza en virtud del acuerdo del pleno del Tribunal Supremo de 25 de mayo de 2005.[24]

En tales casos, los propios peritos adoptando las medidas y garantías adecuadas para preservar el contenido de la información pueden proceder a la extracción de la información más relevante atendiendo a los criterios de búsqueda facilitados por el equipo investigador (si bien a la hora de la realización de estas búsquedas debieran ser oídas el resto de las partes, pues en otro supuesto nos encontraríamos ante una prueba unilateralmente preconsituida).[25]

[23] Sobre este particular véase la reciente del Tribunal Supremo de 3 de diciembre de 2012, (Varela Castro, La ley *195398/2012)*, la cual marca un importante hito en relación a las condiciones del Alto Tribunal para enervar la garantía constitucional a la presunción de inocencia en el ámbito electrónico. La sala 2ª del Tribunal acoge la realidad de que, en el ámbito electrónico, la anonimización mediante suplantación de IP es de accesible para cualquier internauta.

[24] En virtud del mismo, la mera impugnación de los análisis sobre drogas elaborados por centros oficiales, no impide la valoración del resultado de aquellos como prueba de cargo, cuando haya sido introducido en el juicio oral como prueba documental, siempre que se cumplan las condiciones previstas en el art. 788.2 LECrim. En todo caso la proposición de pruebas periciales se sujetará a las reglas generales sobre pertinencia y necesidad.

[25] Se incide en esta cuestión especialmente en el caso Schreiber v. Schreiber, 2010 WL 2735672 (N.Y. Sup. Ct. June 25, 2010) en el mismo se dispusieron determinada cautelas en orden a la realización de las averiguaciones pertinentes en los soportes clonados. En concreto se dispuso que con carácter previo a la realización de cualquier tipo de búsqueda las partes deberían ser oídas en orden a la fijación de los criterios de búsqueda, para lo cual con carácter previo al análisis forense de los soportes analizados se requirió la aportación de una lista de palabras claves y otros criterios de búsqueda que deberían llevarse a efecto por los peritos técnicos nombrados por el tribunal para la búsqueda de archivos o fragmentos de texto codificado. Tales previsiones lo serían dentro de unos límites

Por otra parte el análisis de los soportes informáticos permite la recuperación de los archivos ocultos, restableciendo los vínculos suprimidos y recabando los metadatos que permitirán reconstruir el origen de la información, la identidad del delincuente y las circunstancias y el tiempo de la creación, modificaciones, y de las distintas versiones del archivo.

La tipología de las pericias a realizar sobre los elementos ocupados depende de las necesidades probatorias de los hechos investigados, según Eloy Velasco pueden constituir su objeto, por ejemplo: 1) las señas IP procedencia del ataque informático, el autor, por su origen, 2) el rastro del dinero o el intercambio (el archivo) el autor por su destino, 3) el intercambio y los intermediarios proxies, botnets…, 4) el origen del virus troyano quien lo introduce de dónde viene a quien envía la información, 5) el análisis de las telecomunicaciones, (interlocutores, fechas, duración, localización), 6) la desaparición del cuerpo del delito y los medios empleados para el borrado, 7) la denegación intencionada del servicio (DDOS). A parte de estas existirán otras adecuadas a la finalidad del delito investigado como el informe sobre la autenticidad o imitación de la firma electrónica.[26]

Se suele encomendar estas pericias a los departamentos policiales especializados en la realización de este tipo de pericias existiendo una estructura distinta según de qué cuerpo policial se trate. Cabe que estas pericias se realizan por unidades de investigación especializadas en la persecución al margen de la investigación como el servicio de pericias informática de la Comisaría General de Polícía Científica y en el caso de la Guardia Civil la Brigada de Investigación Tecnológica. Dentro de los grupos policiales dedicados a la investigación del delito existen a su vez equipos especializados en la investigación de delitos de esta clase, como grupo de ciberterrorismo de la Jefatura General de Información.

5- CONCLUSIONES

Dicho todo lo cual, la gran pregunta en relación al tratamiento de la información electrónicamente almacenada es determinar, cual es la línea a seguir para el análisis de los soportes informáticos. A juicio de quien suscribe estas líneas el tratamiento de la información telemática dependerá de diversas factores: de la finalidad procesal pretendida por el medio de prueba empleado, (a saber reconocimiento judicial, examen pericial o documental), del volumen y de la accesibilidad de los datos y por último de los criterios que deban de arbitrarse para la discriminación de la información que por afectar a datos especialmente sensibles se hagan precisos para el pleno desenvolvimiento del proceso:

a) Ante la ausencia previsiones legales en la Ley de Enjuiciamiento Criminal, el tratamiento jurídico de la información electrónicamente almacenada, que no se halle incorporada a un documento electrónico, debe ser la propia de cualquier otro efecto de convicción. Cabe como hemos visto, plasmar parcial o totalmente la información contenida en aquel en un momento dado mediante el volcado a un medio indeleble, en tal caso el soporte electrónico perderá la virtualidad que le es propia para convertirse en un documento propiamente dicho. Lo cierto es que sin llegar a tomar este carácter, en ocasiones, especialmente cuando el flujo de datos es incesante o simplemente cuando la diligencia carece de la relevancia bastante para proceder a su documentación, es posible proceder al reconocimiento directo de los propios soportes sin más consideraciones. En tales supuestos, la información contenida en dichos soportes no pierde su virtualidad propia como medio de prueba, si bien su eficacia vendrá determinada por el contexto en que fuese encontrada y la seguridad de la cadena de custodia. Se entiende así que la Ley de Enjuiciamiento civil, en su artículo 384.3, otorgue a estos una condición propia, remitiendo para su valoración a las reglas de la sana crítica y no a la de la prueba tasada propia

adecuados a la transcendencia del medio de prueba propuesto y de un marco temporal de búsqueda en que los archivos fueron modificados o creados. Se excluía así búsquedas de carácter genérico que no respondiesen a unos indicios ciertos, sino que atendiese al tipo de formato del archivo.

[26] Velasco Núñez, Eloy, *Delitos cometidos a través de internet,* Editorial La Ley, 2009, p. 237.

de los documentos propiamente dichos. Fuera de los supuestos de reconocimiento directo de los soportes electrónicos, el modo normal de tratamiento de la información electrónicamente almacenada es su análisis pericial. No se puede olvidar sin embargo que esta forma de extracción de información es una técnica imperfecta, sujeta a la sana crítica y susceptible de nuevos contraanálisis que pongan en tela de juicio sus conclusiones. Este es un dato muy importante, por cuanto aún cuando en nuestro derecho se encuentra bastante restringido el principio contradictorio ante informes de este tipo,[27] la posibilidad de realización de una contrapericia es una exigencia mínima para discutir las conclusiones periciales alcanzadas.

c) La catalogación de la información contenida en los soportes informáticos a través de una diligencia judicial que fije definitivamente la información contenida en aquellos, otorga al soporte informático la consideración de verdadero documento y por tanto prueba en sí misma considerada, proporcionando mayores posibilidades en orden al tratamiento de la información y permitiendo en mayor medida la contradicción y el logro del resto de los fines procesales. Ciertamente se ha dicho que la realización del clonado puede suponer una pérdida de energías procesales, complicando excesivamente el procedimiento el caso es que como ha quedado indicado es una diligencia estrictamente necesaria en determinados supuestos:

- Delitos en el marco del crimen organizado.

- Procesos en el que los datos contenidos sean la principal prueba de cargo.

- Procesos que tengan gran trascendencia o implicaciones en el extranjero al objeto de preservar la prueba realizada con un máximo de garantías.

- Procesos que contengan datos especialmente sensibles al objeto de facilitar la discriminación de los contenidos.

d) La evolución exponencial de la información contenida en los soportes informáticos hace cada vez más difícil la solicitud de información a los equipos de pericias informáticas, que se encuentran colapsados. Se observa en los últimos tiempos cierto retraso en la realización de estas pericias y tampoco parece que funcionarios con un grado de especialización tan grande como es el que tienen los funcionarios adscritos a estos equipos puedan dar a vasto con diligencias que en definitiva tienen un carácter mecánico. Se hace indispensable por tanto que con carácter previo al análisis de cualquier tipo de información seleccionar o filtrar la información contenida en los soportes informáticos y únicamente será después cuando haya de verificarse las operaciones periciales, búsqueda de metadatos, recuperación de archivos ocultos o cualesquiera otras, sean los que propiamente debería ser objeto de análisis pericial. Desde esta perspectiva, el clonado de la información permitirá la extracción de la información y su incorporación al proceso como documentación propiamente dicha, documentación que como tal puede ser tratada por el equipo investigador e incorporada al proceso sin las prevenciones y cautelas de su análisis pericial (posibilidad de contraanálisis, contradicción y garantía de imparcialidad de los peritos). Para ello sólo exige contar con los medios de clonación adecuados cuya manipulación no exige especiales conocimientos, pudiendo a partir de este momento los propios equipos investigadores desarrollar su función con todas las garantías de imparcialidad al existir una copia a salvo que permita contrastar sus conclusiones.

e) Como ha quedado indicado lo que distingue el acceso a la información electrónicamente almacenada de otro tipo de efectos es que de su mero examen externo no cabe saber qué tipo de información se contiene en los mismos y que garantías deban de adoptarse para proceder a su acceso. Téngase presente que dado el volumen de la información que puede verse afectada y la existencia de varios niveles subliminales de datos informáticos no accesibles sin contar que especiales conocimientos técnicos, cabe que el acceso inopinado a dicha información

[27] Véase, tratamiento jurisprudencia del art. 788.2 LECRIM, véase por todas la STS 2ª, de 3 de febrero de 2009 y en particular el Acuerdo del Pleno no jurisdiccional de aquella Sala de 25.5.2005.

pueda conculcar diversos derechos fundamentales. Así, aparte de la preservación de los derechos sobre el tratamiento de datos de carácter personal, existen otros derechos como el secreto de las comunicaciones, el secreto profesional o la libertad de expresión que pueden verse seriamente implicados.[28] Parece evidente que una actuación dirigida a reconstruir este proceso que permita atribuir a su autor una información obtenida en un soporte informático exige unas garantías especiales que permitan adecuar tal tipo de diligencias a la inmediación judicial y al principio contradictorio. En tal sentido, son muchas las resoluciones, que cuando el volumen de la información que se recibe del sistema supera las posibilidades humanas de control, acuden de forma irreflexiva a las previsiones de los artículos 579.1 y 580-588 para establecer filtros en orden a seleccionar la información relevante del proceso y la exclusión de aquella otra información de carácter intranscendente.[29] Tal normativa decimonónica no se adapta ni de cerca a la función encomendada, haciéndose cada día más necesario una regulación específica sobre estas cuestiones. En el derecho norteamericano, esta cuestión de la selección de información relevante es bien conocida desde hace tiempo a través de la doctrina surgida como consecuencia del caso Zubulake y las restricciones al acceso a grandes volúmenes de información, en el que las diligencia de las partes en orden a procurar información, los criterios de selección de información y el ámbito temporal de averiguación son esenciales para que el proceso pueda desenvolverse con todas las garantías.[30]

6- ADENDA: REGISTRO DE LOS EFECTOS INFORMÁTICOS EN LOS ANTEPROYECTOS DE LA LEY DE ENJUICIAMIENTO CRIMINAL.

Tanto el Anteproyecto de Ley de Enjuiciamiento Criminal presentado por el Gobierno socialista en 2011 como la Propuesta de Código Procesal Penal presentada por el Ministerio de Justicia en 2012 abordan con gran minuciosidad todo lo referente al análisis de los efectos informáticos, dedicando el primero de esto texto un largo precepto el artículo 347 al estudio del registro e incautación de los datos y archivos informáticos, precepto cuyas principales ideas han sido recogidas en la Propuesta.

Las principales novedades vienen determinadas por la atribución al Ministerio Fiscal de una competencia exclusiva para la instrucción de la causa, a salvo las autorizaciones puntuales en que sea preceptivo recabar la intervención del Juez de Garantías para preservar los derechos del justiciable. Los aspectos más relevantes de dicha ordenación son los siguientes:

- Título habilitante. En este caso, la sola autorización del ministerio fiscal resulta insuficiente haciéndose precisa la intervención del juez de garantías, en el entendimiento que los datos obrantes en dichos efectos informáticos pueden tener información sensible de carácter personal.

---

[28] Según Delgado Martín el acceso a los sistemas informáticos puede afectar a los siguientes derechos fundamentales derecho a la intimidad personal (art. 18.1 CE), derecho al secreto de las comunicaciones (art. 18.3 CE), derecho a la autodeterminación informativa en el ámbito de la protección de datos personales (art. 18.4!CE) e incluso al derecho a la inviolabilidad domiciliaria (art. 18.2CE) en aquellos supuestos en los que el dispositivo electrónico es hallado en el seno de una entrada y registro en domicilio. Diario La Ley, nº 8202, Sección Doctrina, 29 Nov, Año XXXIV, Editorial La Ley.

[29] Véase a modo de ejemplo STS, de 13 de enero de 1999, Marañón Chavarri, La Ley 1802/1999.

[30] Recientemente, ha tenido gran trascendencia en el derecho norteamericano el caso Schreiber v. Schreiber, en el que se valora especialmente el modo en que las partes pueden intervenir en orden a la búsqueda de información. En el caso indicado se dispuso que con carácter previo al análisis forense de los soportes analizados se requiriese a las partes para la aportación de una lista de palabras claves y otros criterios de búsqueda que deberían llevarse a efecto por los peritos técnicos nombrados por el tribunal para la búsqueda de archivos o fragmentos de texto codificado. Tales previsiones lo serían dentro de unos límites adecuados a la transcendencia del medio de prueba propuesto y de un marco temporal de búsqueda en que los archivos fueron modificados o creados. Se excluía así búsquedas de carácter genérico que no respondiesen a unos indicios ciertos, sino que atendiese al tipo de formato del archivo. Schreiber v. Schreiber, 2010 WL 2735672 (N.Y. Sup. Ct. June 25, 2010)

- Examen y aprehensión de los datos. El examen y estudio de los datos queda a discreción de lo que señale el juez de garantías, pero deberán emplearse instrumentos o herramientas adecuadas que garanticen la autenticidad e integridad de la información obtenida. En tal sentido el anteproyecto no aborda la condición que deban tener quienes accedan a dicha información, cuestión a nuestro juicio muy relevante para poder determinar el tipo de herramienta forense que deba de emplearse para el examen de la información. En todo caso las personas que accedan a la información deben quedar identificadas en el auto y se prevé la posibilidad de ordenar a las personas que tengan acceso a las claves, que disponga

- Preservación de los datos. Para la preservación de los datos se prevé que el auto que acuerdo el acceso a los efectos informáticos disponga la realización y conservación de copias de los datos informáticos, la preservación de la integridad de los datos almacenados, así como la inaccesibilidad o supresión de dichos datos informáticos del sistema informático al que se ha tenido acceso.

- Impugnaciones. Se restringe la posibilidad de impugnaciones estableciéndose una presunción de integridad de los datos a salvo que se comprueben indicios de manipulación.

Lo más destacable de la reforma es el apartado 5º del artículo 347 relativo a la realización de copias, «*Salvo que constituyan el objeto o instrumento del delito o existan otras razones lo justifiquen se evitará la incautación de los soportes físicos que contengan los datos o archivos informáticos objeto de indagación y registro, limitándose a la obtención de una copia de los mismos en condiciones que garanticen la autenticidad e integridad de los datos».* Tal previsión, que como veremos se recoge literalmente en la propuesta de 2013, supone un cambio considerable en la medida que hace de la diligencia de clonación el eje del nuevo sistema, solución que como hemos venido indicando es la única forma de preservar la información electrónica y dotar esta del carácter de prueba plena como hemos querido apuntar a lo largo de este trabajo.

La propuesta de texto articulado de Ley de Enjuiciamiento Criminal elaborada por la Comisión Institucional creada por Acuerdo del Consejo de Ministros de 2 de marzo de 2012, si bien resulta muy parca en relación a las cuestiones de la cadena de custodia, recoge en relación a esta materia básicamente las ideas que venían siendo apuntadas en el texto precedente.

Pese a ello, el tratamiento sistemático de la cuestión difiere notablemente del texto precedente, al distinguir según se trate de intervención con ocasión de un registro domiciliario (art. 347) o no (art. 348), pudiendo en el primero de los casos establecerse a prevención. También se recoge la posibilidad de acceso a este tipo de información a través de accesos remotos. La novedad más relevante es la previsión contenida en el artículo 348 en relación a la autorización judicial para el acceso a este tipo de información, en tal caso se habilita un gran margen de discrecionalidad por parte del juez de garantías para fijar los términos y el alcance del registro de estos soportes. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial.

De forma semejante al texto precedente de 2011, se previene que salvo que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen, se evitará la incautación de los soportes físicos que contengan los datos o archivos informáticos, cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos que sean objeto de investigación.

Como queda indicado se prevé igualmente la instalación en los equipos investigados de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que la medida resulte proporcionada para la investigación de un delito de especial gravedad y sea además idónea y necesaria para el esclarecimiento del hecho investigado, la averiguación de su autor o la localización de su paradero. Si bien se parte del carácter secreto de tales diligencias, no existen previsiones en orden a la desinstalación del software previamente instalado, así como las medidas que deban adoptarse para la preservación de la indemnidad de los equipos.

Tales previsiones se ven sin embargo limitadas notablemente, al excluir expresamente este tipo de acceso remoto, en los casos de que los equipos se encuentren almacenados en un sistema informático o en una parte del mismo situado fuera del territorio sobre el que se extienda la jurisdicción española. En estos casos, se instarán las medidas de cooperación judicial internacional que al día de la fecha resultan manifiestamente insuficientes para obtener una respuesta ágil para el tratamiento de estas cuestiones.

BIBLIOGRAFÍA

Alemany Eguidazu, Jesús, "La prueba de la autenticidad electrónica con la LEC 2000", Diario La Ley, Sección doctrina, ref. D-51, tomo 3, Editorial Ley, 2001, Las Rozas.

Anguiano Jiménez, José Mª, "La Teoría de la Media Electrónica", Diario la Ley, Boletín 8708, de 8 de mayo de 2013.

Bolter, J. David, *Writing Space: The Computer, Hypertext, and the History of Writing*. Hills&le, New Jersey: Lawrence Erlbaum Associates, 1991.

Briet, Suzane. Qu'est-ce que la documentation, Edit, Paris, 1951. p. 7.

Delgado Martín, Joaquín, "La prueba electrónica en el proceso penal", Diario La Ley, Nº 8167, Sección Doctrina, 10 Oct. 2013, Año XXXIV, Editorial LA LEY 7336/2013.

Delgado Martín, Joaquín, "Los derechos fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos", Diario La Ley, nº 8202, Sección Doctrina, 29 Nov. 2013/01/06 año XXXIV.

Devy, M. Levy, "In ECHT '94: Proceedings of the 1994" *ACM European conference on Hypermedia technology,* 1994, pp. 24-31.

Gettys, T., "Generating perfect hash function", Dr. Dobb's Journal, Vol. 26. No.2, 2001.

Gudín Rodríguez-Magariños, Antonio Evaristo, "La diligencia de cotejo de los documentos electrónicos" Revista General de Derecho Procesal, nº 22, 2010.

Gudín Rodríguez-Magariños, Antonio Evaristo, "El cómputo de los plazos en la presentación de escritos por medios electrónicos" Diario La Ley, n 7699, 2011.

Gudín Rodríguez-Magariños, Antonio Evaristo, "La búsqueda y conservación de los datos informáticos en el Derecho norteamericano E-discovery" Estudios de Deusto: revista de la Universidad de Deusto, ISSN 0423-4847, Vol. 58, nº. 2, págs. 205-245.

Gudín Rodríguez-Magariños, Faustino, *La administración de justicia Digitalizada,* Ediciones Experiencia S.L., 2008.

Hernández Guerrero, Francisco, «Medios informáticos y proceso penal», Estudios jurídicos del Ministerio Fiscal IV, 1999.

Mira Ros, Corazón, "La Digitalización de los Archivos Judiciales", Revista General de Derecho Procesal, 2009.

Mira Ros, Corazón, *El expediente judicial electrónico.* Dykinson, 2010.

Mira Ros, Corazón, "La prueba documental electrónica: algunas concesiones a la seguridad jurídica preventiva" Oralidad y escritura en un proceso civil eficiente: [Coloquio de la Asociación Internacional de Derecho Procesal] / Federico Carpi(ed. lit.), Manuel Pascual Ortells Ramos (ed. lit.), Vol. 2, 2008 (Comunicaciones = Presentations), pp. 105-114.

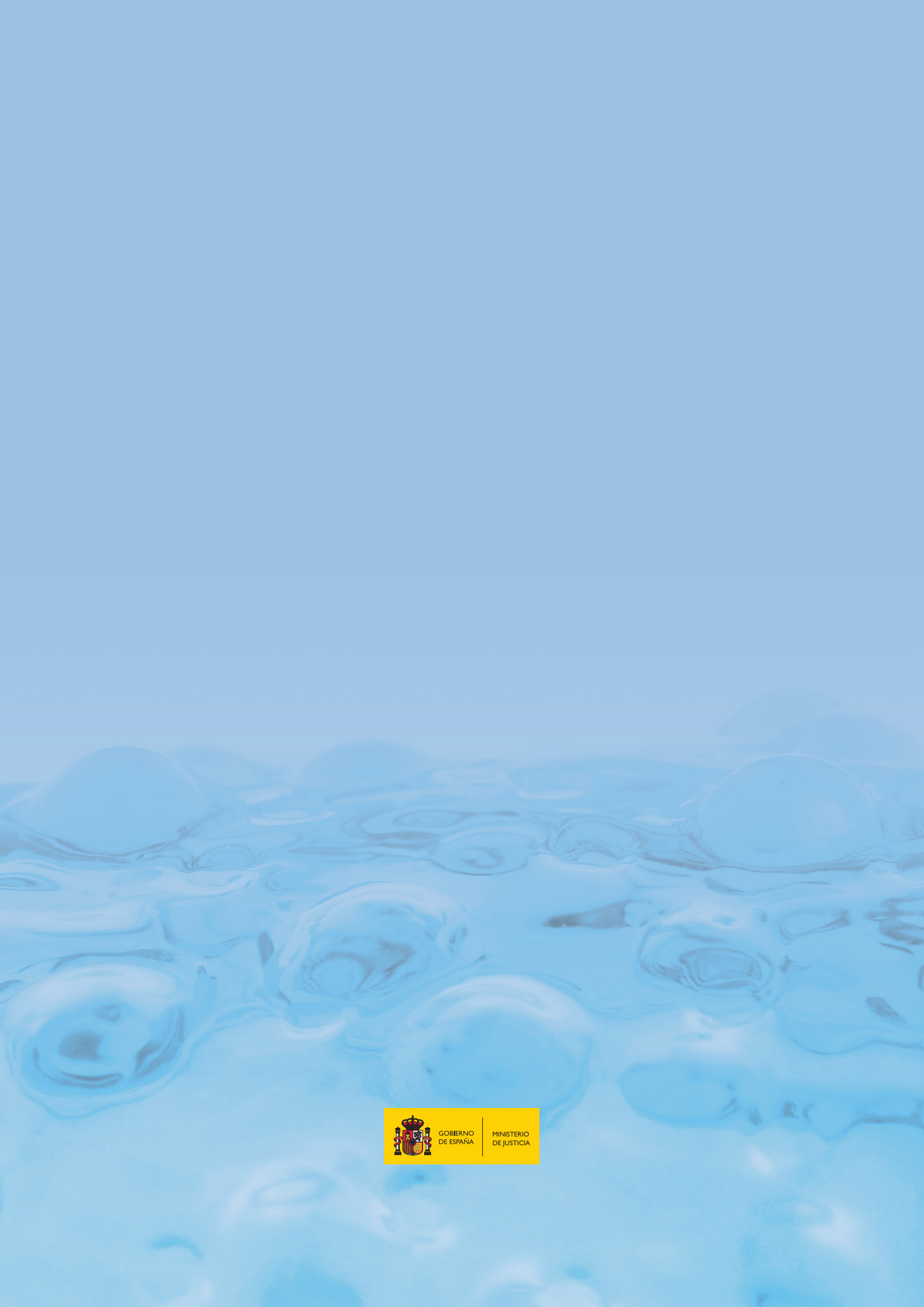
Marchena Gómez, Manuel, "Dimensión jurídico penal del Correo Electrónico", Diario La Ley, núm. 6475, Sección Doctrina, 4 de mayo de 2006, Ref. D-114.

Richard González, Manuel, "La cadena de custodia en el Derecho procesal Español", Diario La Ley, Nº 8187, Sección Tribuna, 8 Nov. 2013, Año XXXIV, Editorial La ley.

Rodríguez Lainz, José Luis, *La intervención judicial en los datos de tráfico de sistemas de telecomunicaciones y de comunicaciones electrónicas,* Editorial Bosch, Barcelona, 2003, pp. 14-32.

Sanchis Crespo, Carolina, *La prueba por soportes informáticos*, Tirant lo Blanch, Valencia, 1999.

Velasco Núñez, Eloy, *Delitos cometidos a través de Internet, aspectos procesales,* La Ley actualidad, 2010; VVAA, *The Sedona Principles. Best practices & principles for adressing Electronic Document Production* ,annoted versión, Coordinador Jonathan M. Redgrave, 2005, pp. 7 y 8.


GOBIERNO
DE ESPAÑA
MINISTERIO
DE JUSTICIA