LA PRUEBA PERICIAL DIGITAL Y LA CADENA DE CUSTODIA

José Miguel González Reyes
Profesor asociado Administrativo de Derecho
Universidad de La Laguna

Resumen

La irrupción de la denominada revolución digital ha supuesto en todos los órdenes una modificación de los comportamientos sociales planteando a nuestro Derecho nuevos retos que hasta ahora eran desconocidos. El presente trabajo constituye un estudio de los requisitos que han de tener las pruebas derivadas de la comisión de delitos a través de medios informáticos, su licitud y modo de incorporación al proceso penal. En este contexto, viene siendo tradicional en la doctrina y jurisprudencia penal española que para que una prueba se repute lícita, esto es, en última instancia válida, ha de traerse al proceso con una serie de garantías, siendo la más relevante la de poder ser sometida a contradicción, momento en el que la pericia informática, a través de la práctica forense, puede alcanzar un papel en orden a confirmar o denegar la validez de aquéllas para operar como prueba de cargo o descargo en el proceso penal.

Palabras clave: derecho procesal digital, ciberdelito, indefensión, prueba pericial.

PERICIAL EVIDENCE IN CRIMES COMMITTED THROUGH COMPUTER MEDIA AND THE "CHAIN OF CUSTODY"

Abstract

The appearance of the dominant digital revolution has led to a modification of social behaviour in all areas, posing new challenges to the Law that were until now unknown. This work constitutes a study of the requirements for gathering evidence, derived from the commission of crimes through computer media, its legality, and the way in which they are incorporated into criminal proceedings. In this context, it has been traditional in criminal doctrine and jurisprudence that an evidence, to be considered lawful, that is, ultimately valid, it must be brought to the process with a number of procedural guarantees, being the most relevant one the possibility to be subject to contradiction. It is in this light when computer expert, through their forensic practice, can be involved in order to confirm or deny the validity of potential evidence which, in turn, may relate to the charge or discharge of criminal proceedings.

Keywords: digital procederal law, cybercrime, helplessness, pericial evidence.

DOI: https://doi.org/10.25145/j.anfade.2021.38.03
Anales de la Facultad de Derecho, 38; septiembre 2021, pp. 43-79; ISSN: e-2530-8319

1. SOBRE LA NATURALEZA DE LA PRUEBA INFORMÁTICA Y EL MODO DE SU INCORPORACIÓN AL PROCESO PENAL

Lo que se viene entendiendo como prueba informática o evidencia electrónica a día de hoy no ha sido descrito por norma jurídica alguna en España[1]. Si bien, no obstante, sí que se han definido en nuestro ordenamiento interno los conceptos de documento electrónico y firma electrónica[2].

Como quiera que sea, con mejor precisión, en el ámbito europeo (y del que España forma parte), se ha realizado una mejor aproximación a ese concepto por mor de la Decisión 2002/630/JAI del Consejo, de fecha 22 de julio de 2002, relativa a la creación del programa marco para la cooperación policial y judicial en materia penal (AGIS)[3]. En este instrumento jurídico, se define la prueba electrónica como «la información obtenida a partir de un dispositivo electrónico o medio digital, el cual sirve para adquirir convencimiento de la certeza de un hecho». También define los medios de prueba electrónicos como «los soportes técnicos que recogen la prueba electrónica».

La prueba informática o evidencia digital[4] implica su necesaria contextualización en el ámbito de las tecnologías de la comunicación e información. La información que generan las operaciones de informática de carácter delictivo resulta producida, almacenada o transmitida mediante dispositivos o instrumentos digitales. De este modo, con carácter general se viene entendiendo por prueba informática

[1] Para una aproximación al concepto de prueba informática *vid*. Illán Fernández, J.M., *La Prueba Electrónica, Eficacia y Valoración en el Proceso Civil*, Aranzadi, Navarra, 2009; Hernández Guerrero, F.F.; Álvarez de los Ríos, J.L., «Medios informáticos y proceso penal», en Estudios Jurídicos, Ministerio Fiscal IV, CEJAJ, Madrid, 1999; y Sanchís Crespo, C., «La prueba en soporte electrónico», en *Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio* (coord. Gamero Casado y Valero Torrijos), Thomson Reuters-Aranzadi, Navarra, 2012.

[2] Se trata de normas extraprocesales que ofrecen definiciones acerca de medios de prueba concretos, como la que hace la Ley 59/2003, de 19 de diciembre, de Firma Electrónica. En el art 3.5 de esta norma se concreta una definición de documento electrónico como «la información de cualquier naturaleza en forma electrónica, archivada en soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado». Se trata de una definición amplia si bien la firma electrónica en sí no da al documento electrónico carácter de prueba documental en juicio, sino únicamente al documento electrónico firmado electrónicamente. Por su parte, el Reglamento eIDAS 910/2014 lo define como el documento redactado y archivado en soporte electrónico que incorpora datos que están firmados electrónicamente.

[3] En el ámbito europeo, no obstante, destaca la Directiva 2006/24/CE sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, así como la Directiva 2013/40/UE, que establece las normas mínimas a la definición de las infracciones penales y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de la información.

[4] Es importante señalar aquí que el uso en castellano de la palabra «evidencia» como sinónimo de «prueba» o de «indicio» se debe a la influencia de la palabra inglesa *evidence*, que en este idioma hace referencia a toda prueba (circunstancial, testimonial o material) que se alega en un proceso judicial.

o evidencia electrónica la referida a la que contiene cualquier tipo de información almacenada o trasmitida a través de dispositivos informáticos que tiene la virtualidad de poder acreditar los hechos sobre los que versa el proceso[5]. Se trataría, en última instancia, de toda aquella información digital que permita constatar la realidad de un hecho afirmado por las partes y que resulta relevante para el objeto del proceso judicial[6].

En este sentido, las innovaciones tecnológicas en el ámbito delictual se pueden presentar como un medio de prueba autónomo *ex* art. 299.2 de la LEC[7] pudiendo revestir los caracteres de la prueba documental, que será su consideración corriente[8]. Pero también, de prueba pericial; o, incluso, testifical, si se deriva del testimonio de la persona que ha dado noticia del hecho delictivo por inmediación o conocimiento de lo contenido en los elementos informáticos[9].

Sobre el carácter documental o no de la prueba electrónica existe una controvertida discusión en la Doctrina. El punto de partida lo constituye el art. 326.1 de la LEC, que viene a conferir al documento privado el valor de prueba plena en el proceso si no es impugnado por la parte a quien perjudica y que resulta, en general, más favorable del aplicable si careciera de esa consideración[10]. Así, por un lado, nos encontramos con una posición que atribuye a la prueba digital un carácter autó-

[5] Por su parte, el dispositivo digital sería todo sistema informático, incluyendo sistemas de almacenamiento y transmisión de la información por medios digitales. Hay que tener en cuenta que todo dispositivo digital es, a su vez, electrónico, pero que no todo dispositivo electrónico es digital.

[6] *Cfr.*, Bueno de Mata, F., Prueba Electrónica y Proceso 2.0, Tiran lo Blanch, Valencia, 2014, p. 130.

[7] El art. 299 de la LEC establece como medios de prueba de los que se podrá hacer uso en juicio: (1) Interrogatorio de las parte; (2) Documentos públicos; (3) Documentos privados; (4) Dictamen de peritos; (5) Reconocimiento judicial; (6) Interrogatorio de testigos. No obstante, también se admitirán como se establece en su apartado 2: «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».

[8] Véanse, también, los arts. 384.1 y 382.2.3 y 4 de la LEC.

[9] Consciente del impacto de las nuevas tecnologías y sus consecuencias en el mundo jurídico, la STS de 3 de noviembre de 1997, Sala 3.ª, describe en su FJ 10 la trascendencia de este nuevo modo de interactuación cuando expresa: «... Estamos asistiendo, en cierto modo, en algunas facetas de la vida, incluso jurídica, al ocaso de la civilización del papel, de la firma manuscrita y del monopolio de la escritura sobre la realidad documental. El documento, como objeto corporal que refleja una realidad fáctica con trascendencia jurídica, no puede identificarse, ya, en exclusiva, con el papel, como soporte, ni con la escritura, como unidad de significación. El ordenador y los ficheros que en él se almacenan constituyen, hoy día, una nueva forma de entender la materialidad de los títulos valores y, en especial, de los documentos mercantiles».

[10] Frente a ese valor de prueba plena como documento, la consideración de la prueba electrónica como simple instrumento de archivo informático, en los términos del art. 384 de la LEC, restringiría la misma a un valor probatorio conforme a las reglas de la sana crítica del juez.

nomo gozando de naturaleza propia y singular[11]; por otro, a los que de modo análogo entienden que la prueba electrónica equivale a los medios de prueba tradicionales[12].

Más allá de las disquisición doctrinal, el Código Penal da carácter de documento, examinable de oficio por el tribunal (como prevé el art. 726 de la LECrim), a todo soporte material con datos de relevancia jurídica[13]. De aquí, podría intuirse que el documento electrónico surtiría los mismos efectos que el documento en papel a nivel jurisdiccional[14]. Esto es, que habría una equivalencia funcional entre ambas. Idéntico carácter de documento, y, con ello, de prueba admisible en juicio como

---

[11] *Vid*. esta idea en Montón Redondo, A., «Medios de reproducción de la imagen y el sonido» en *La prueba*, *Cuadernos de Derecho Judicial* núm. 7, CGPJ, Madrid, 2000, p. 50 y ss.; y también Álvarez-Cienfuegos Suárez, J.M.ª, «Las obligaciones concertadas por medios informáticos y la documentación», *La Ley. Revista jurídica española de doctrina, jurisprudencia y bibliografía* núm. 4, 1992, p. 1013 y ss.

[12] Dicha previsión cuenta con abundante apoyo jurisprudencial. Así, la sentencia de 3 de octubre de 1997 ha señalado: «En torno al concepto de documento como instrumento casacional con eficacia demostrativa del error judicial cuya censura constituye la esencia del Motivo, las Sentencias de éste Tribunal de 23 de diciembre de 1996, entre otras, centran su extensión en los siguientes términos: A Que exista un documento, lo que equivale: a) Que se trate de un documento en sentido estricto, y ha de entenderse por tal el escrito, en sentido tradicional, o aquella otra cosa que, sin serlo, pueda asimilarse al mismo, por ejemplo, un diskette, un documento de ordenador, un vídeo, una película, etc., con un criterio moderno de interacción de las nuevas realidades tecnológicas, en el sentido en que la palabra documento figura en algunos diccionarios como "cualquier cosa que sirve para ilustrar o comprobar algo" (obsérvese que se trata de una interpretación ajustada a la realidad sociológica, puesto que, al no haber sido objeto de interpretación contextual y auténtica, puede el aplicador del derecho tener en cuenta la evolución social), siempre que el llamado "documento" tenga un soporte material, que es lo que sin duda exige la norma penal. (Por todas, SS.TS. 1.114/94, de 3 de junio, 1.763/1994, de 11 de octubre y 711/1996, de 19 de octubre). En la actualidad dicha fórmula jurisprudencial tiene adecuada correspondencia en la norma contenida en el artículo 26 del nuevo Código penal, según el cual "A los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica"».

[13] El documento electrónico ha sido definido por la doctrina como «toda representación en forma electrónica de hechos jurídicamente relevantes, susceptibles de ser representado en forma humanamente comprensible». *Vid.* Álvarez-Cienfuegos Suárez, J.M.ª, «Los delitos de falsedad y los documentos generados informáticamente. Concepto procesal y material de documento: nuevas técnicas», en *Cuadernos de Derecho judicial*, CGPJ, Madrid, 1993, p. 8.

[14] La LEC ha procedido a dar un tratamiento autónomo a los medios de reproducción de la palabra, el sonido y la imagen, diferenciándolos de la prueba documental. Consecuencia de la consideración de la naturaleza autónoma de tales medios probatorios es el tratamiento diferenciado que recibe en la LEC, a saber: (1) El tratamiento independiente que la LEC da a la prueba documental a la que consagra los artículos 317 a 334 y a los medios de reproducción de la palabra, el sonido y la imagen, regulados en los artículos 382 a 384; (2) El artículo 265 LEC al disponer los documentos, escritos u objetos que han de acompañar a la demanda distingue en el apartado 1.º «los documentos en que las partes funden su derecho» y en el apartado 2.º «los medios e instrumentos a que se refiere el apartado 2 del artículo 299 –medios de reproducción de la palabra, el sonido...– si en ellos se fundaran las pretensiones...»; (3) Los artículos 267 y 268 LEC establecen la forma de presentación de documentos públicos –copia simple y si se impugnara su autenticidad, mediante original, copia o certificación– y de los documentos privados –original o copia autenticada, uniéndose a los autos o dejando testimonio, con devolución de los originales o copias, o designación del archivo,

documental, otorga el art. 24.2 de la *Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico* al soporte electrónico en que conste un contrato celebrado por vía electrónica[15].

Como quiera que sea, con carácter general, para el TS las evidencias digitales no tendrían el carácter de prueba documental (salvo en los documentos y contratos firmados electrónicamente, como se ha dicho); si bien, en ciertas ocasiones, se ha mostrado favorable a ese carácter documental de la evidencia electrónica como describe, *v.gr.,* la STS de 12 de junio de 1999[16]. Otras veces, como ocurre en el ámbito laboral, se le priva de aquel carácter, como también explica la Sala de lo Social en la STS 6216/2011[17].

Debiera, por tanto, acogerse, en cualquier caso, un concepto amplio de documento que abarca tanto los soportes tradicionales (papel) como los nuevos soportes tecnológicos o informáticos (DVD, *pendrive*, etc.) para que la previsión del art. 26 del Código Penal pueda tener virtualidad respecto a cualquier soporte que, en última

---

protocolo o registro donde se encuentren–, no resultando de aplicación a los medios de reproducción de la palabra, el sonido y la imagen.

[15] Además, tal posición se encontraría positivamente respaldada por el tratamiento que el art. 3.8 de la Ley 59/2003 de Firma Electrónica da a los soportes de los documentos electrónicos firmados electrónicamente, ya que esta Ley los dota del carácter de prueba documental en juicio. Si además dicha firma es reconocida, la impugnación del documento se resolverá comprobando que dicha firma cumple todos los requisitos prescritos en esta Ley. Si no es firma reconocida, sino avanzada, la impugnación tendrá el mismo tratamiento que el establecido en el art. 326.2 de la LEC para resolver la impugnación de cualquier documento.

[16] Así, expresa, tras reconocer que, aunque tanto sustantivo como procesal (Código Civil y Ley de Enjuiciamiento Civil), dada la antigüedad de su redacción, tales textos no contemplan como posibles medios probatorios los mecanismos o elementos derivados de los importantes avances y descubrimientos técnicos de los tiempos modernos, como son las cintas magnéticas, vídeos y cualquier otro medio de reproducción hablada o representación visual del pensamiento humano que «los mismos aparecen admitidos por la jurisprudencia de esta Sala (Sentencias de 30 de Noviembre de 1992 y 2 de Diciembre de 1996), debiendo ser catalogados, dentro de la enumeración contenida en los artículos 1215 del Código Civil y 578 de la Ley de Enjuiciamiento Civil, como prueba documental asimilable a los documentos privados, por cuanto que, al igual que con estos ocurre, si la parte a quien perjudiquen no los reconoce como legítimos, habrán de ser sometidos a la correspondiente verificación o comprobación, por medio de la prueba pericial o, incluso, de reconocimiento o inspección personal del juez, y siendo ello así, o sea (volvemos a decir), admitida la conceptuación como prueba documental de tales elementos o medios técnicos reproductores de la palabra o de la imagen, ha de regir para ellos la misma norma procesal que para los documentos, en el sentido de que aquellos que sean los fundamentales en que la parte actora base su derecho, han de ser presentados con la demanda (artículo 504 de la Ley de Enjuiciamiento Civil), con la única excepción de los que se hallen en alguno de los supuestos del artículo 506 de la citada Ley».

[17] Sin embargo, tal entendimiento del concepto de prueba documental no resulta de aplicación al proceso laboral porque, en primer lugar, en el mismo opera como supletoria, en todo lo no expresamente previsto en la LEC, en la que se establece la diferenciación entre prueba documental y prueba por instrumentos de reproducción de la palabra, la imagen o el sonido, como anteriormente se ha consignado. En segundo lugar, en el proceso penal se realiza dicha interpretación amplia del concepto de documento a la luz de lo establecido en el artículo 26 del Código Penal.

instancia, incorpora o expresa datos, hechos o narraciones con la suficiente eficacia probatoria y, en su caso, necesaria relevancia jurídica.

Ahora bien, el hecho de que la LECrim no regule expresamente el régimen jurídico de la incorporación al proceso de la prueba digital[18] no impide que dicha incorporación al proceso esté exonerada de la observación más elemental de la denominada disciplina de prueba y, muy especialmente, de la posibilidad de contradecir por parte del inculpado las supuestas evidencias digitales que pudieran obrar en su contra.

En este contexto, el peritaje informático de parte se constituye en el garante de uno de los derechos fundamentales más importantes en el orden penal como es el de la presunción de inocencia consagrado en el art. 24 de la CE[19].

2. ANÁLISIS SOBRE LOS REQUISITOS JURÍDICOS Y TÉCNICOS PARA LA VIABILIDAD COMO PRUEBA DE CARGO DE LAS EVIDENCIAS INFORMÁTICAS

2.1. Doctrina constitucional y jurisprudencial relativa a las garantías exigibles a la prueba de cargo

El ordenamiento jurídico español ha establecido un conjunto de reglas procesales en orden a la posibilidad de atribuir un hecho delictivo a una persona y que se concretan en el modo en que se lleva a cabo la actividad probatoria, los medios de prueba en sí y la valoración de aquel resultado.

El derecho a utilizar los medios de prueba no tiene carácter absoluto, ya que la CE se refiere a los medios de prueba *pertinentes*, de manera que tal derecho de las partes no desapodera al tribunal de su facultad de admitir las pruebas pertinentes rechazando todas las demás –arts. 659 y 785.1 LECrim–, si bien la jurisprudencia

ANALES DE LA FACULTAD DE DERECHO, 38; 2021, PP. 43-79

[18] Por tanto, en principio, todos los medios probatorios previstos en la ley son aptos para tal finalidad, pudiendo acceder mediante el documento electrónico, o utilizando soporte papel, o a través de otros medios de prueba tradicionales como el interrogatorio de parte, testifical o pericial.

[19] El artículo 24.2 CE consagra el derecho a un proceso con todas las garantías y a la presunción de inocencia; y con arreglo a una consabida doctrina constitucional y jurisprudencial se «exige para destruir la presunción de inocencia una actividad probatoria suficiente que se explicite motivadamente, haya podido ser contradicha por el inculpado y que pueda considerarse de cargo» (STC 62/1994, de 28 de febrero, citando las SSTC 311/1981, 13/1982, 36/1983, 9/1984, 37/1985, 169/1986 y 256/1988). Y, todavía con mayor concreción, en la STS 94/2013, de 14 de febrero, se lee: «el control casacional de la presunción de inocencia se extenderá a la constatación de la existencia de una actividad probatoria sobre todos y cada uno de los elementos del tipo penal, con examen de la denominada disciplina de garantía de la prueba, y del proceso de formación de la prueba, por su obtención de acuerdo a los principios de inmediación, oralidad, contradicción efectiva y publicidad».

ha establecido una serie de requisitos, formales y materiales, para que este motivo pueda prosperar[20].

Como ha puesto de relieve el supremo intérprete de la CE en la STC 120/1999, de 28 de junio: «La protección del derecho a la presunción de inocencia comporta, en primer lugar, la supervisión de que la actividad probatoria se ha practicado con las garantías necesarias para su adecuada valoración y para la preservación del derecho de defensa. En segundo lugar, comprobar que el órgano de enjuiciamiento expone las razones que le han conducido a constatar el relato de hechos probados a partir de la actividad probatoria practicada. En tercer y último lugar, supervisar externamente la razonabilidad del discurso que une la actividad probatoria y el relato fáctico resultante –STC 189/1998–. Así, sólo cabrá constatar una vulneración del derecho a la presunción de inocencia cuando no haya pruebas de cargo válidas, es decir, cuando los órganos judiciales hayan valorado una actividad probatoria lesiva de otros derechos fundamentales o carente de garantías, o cuando no se motive el resultado de dicha valoración, o, finalmente, cuando por ilógico o insuficiente no sea razonable el iter discursivo que conduce de la prueba al hecho probado –SSTC SS 63/1993 y 68/1998–».

Los requisitos formales de lo que en última instancia viene a ser una modalidad de quebrantamiento de forma son entonces[21]:

1.º Que las pruebas han de estar propuestas en tiempo y forma, de conformidad con las reglas específicas para cada clase de proceso.
2.º Que ante la resolución del tribunal, que debe ser fundada, rechazando las pruebas que no considere pertinentes, o denegando la suspensión del juicio ante la imposibilidad de practicar en ese momento las previamente admitidas, quien ha propuesto la prueba debe hacer constar la oportuna protesta[22].

---

[20] El derecho a la prueba no es un derecho absoluto o incondicionado, y no se produce vulneración del derecho constitucional cuando la prueba rechazada, aun siendo pertinente, carece su contenido de la capacidad para alterar el resultado de la resolución final, y ello exige por parte de quien alegue tal vulneración una doble acreditación: de una parte que el recurrente ha de concretar la relación de hechos que se quisieron y no se pudieron probar y las pruebas inadmitidas; de otra, el invocante de la vulneración del derecho a los medios de prueba pertinente deberá argumentar de modo convincente que la resolución final del proceso *a quo* podría haberle sido favorable de haberse aceptado y practicado la prueba objeto de la controversia.

[21] *Vid*., entre otras, las SSTS 545/2014, de 26 de junio de 2014, y 544/2015, de 25 de septiembre de 2015.

[22] En el procedimiento abreviado, el párrafo segundo del art. 785.1 de la LECrim dispone que contra los autos de admisión o inadmisión de pruebas no cabrá recurso alguno, sin perjuicio de que la parte a la que fue denegada pueda reproducir su petición al inicio de las sesiones del juicio oral. Y, en consonancia con ello, el art. 786.2 de la Ley de Enjuiciamiento Criminal expresa que, al inicio del juicio oral, tras la lectura de los escritos de acusación y defensa, el juez o tribunal abrirá un turno de intervenciones para que puedan las partes exponer, entre otras cosas, lo que estimen oportuno sobre el contenido y finalidad de la pruebas propuestas o que se propongan para practicarse en el acto; y resolverá en el mismo acto lo procedente sobre las cuestiones planteadas, sin que, frente a

3.º Que, si se trata de prueba testifical, han de hacerse constar las preguntas que quien la propone pretendía dirigir al testigo, con la finalidad de que, primero el tribunal de enjuiciamiento y después la Sala de casación, en su caso, puedan valorar la trascendencia de la prueba propuesta[23].

2.2. Requisitos de admisibiliad de las evidencias digitales: licitud y fiabilidad

Tradicionalmente, se vienen considerando como requisitos materiales de la prueba que ésta haya de ser pertinente, esto es, relacionada con el objeto del juicio y con las cuestiones sometidas a debate en el mismo. También, ha de ser relevante, de forma que tenga potencialidad para modificar el sentido del fallo, a cuyo efecto el tribunal puede tener en cuenta el resto de las pruebas de que dispone. Y finalmente, la prueba ha de ser necesaria, es decir, tener utilidad para los intereses de defensa de quien la propone, de modo que su omisión le cause indefensión[24].

Lo anterior implica un juicio *ex ante* de licitud y valoración de las pruebas, es decir, saber el tribunal que si desde la obtención de las mismas por los investigadores hasta su incorporación al proceso (y su posible valoración posterior en el plenario) se han cumplido con los estándares legales y jurisprudenciales que permiten garantizar la plenitud, identidad e integridad de las mismas.

La licitud se concreta en la conveniencia inexorable de que de las evidencias digitales se hayan obtenido sin violación o merma de los derechos fundamentales reconocidos en la CE. El juicio de fiabilidad, por su parte, se refiere a la posibilidad de poderse comprobar la autenticidad e integridad de los documentos digitales obtenidos y su no manipulación. Esta fiabilidad se asegura con la denominada cadena

---

la decisión adoptada, quepa recurso alguno, sin perjuicio de la pertinente protesta y de que la cuestión pueda ser reproducida, en su caso, en el recurso frente a la sentencia.

[23] En cualquier caso, la parte que la propone debe preocuparse de que conste la eventual trascendencia de la prueba respecto del fallo de la Sentencia. La omisión de este requisito no impedirá, sin embargo, la estimación del motivo cuando la pertinencia y necesidad de la prueba se desprenda fácilmente de su propia naturaleza y características.

[24] En este contexto, se trae a colación la STS de 18 de marzo de 2009, que señala: «Es obvio que el doble abordaje del derecho a la prueba –como derecho fundamental o como indebida denegación de la prueba– no altera su esencia: la quiebra se produce cuando la denegada es prueba necesaria, y por tanto es causa de indefensión en los términos del art. 24-1.º de la Constitución Española (CE). Por ello es doctrina del Tribunal Constitucional que el derecho a la prueba está delimitado por cuatro consideraciones: a) Que la prueba sea pertinente, pues sólo a ella se refiere el artículo 24.2 CE. b) Que dada su configuración legal, es preciso que la parte la haya propuesto de acuerdo con las previsiones de la ley procesal, es decir en tiempo oportuno y de forma legal. c) Desde la perspectiva del Tribunal sentenciador, que éste la haya desestimado. d) Al tratarse el derecho a la prueba de un derecho medial/procedimental que se acredite que tal denegación ha podido tener una influencia en el fallo de la sentencia, porque podría haberse variado, y es esta aptitud de la prueba denegada en relación al fondo del asunto, lo que da lugar a la indefensión que proscribe la Constitución, indefensión que debe ser material y no simplemente formal».

de custodia, que se describe en el apartado siguiente, pero también con el adecuado análisis racional, y más extenso, al objeto de que la convicción judicial no adolezca del vicio de inveracidad[25].

Si no se cumple con los requisitos del art. 11.2 de la LOPJ, la obtención de las supuestas evidencias digitales de cargo quedará fuera del ámbito de valoración del tribunal juzgador por no contar con méritos suficientes para enervar la necesaria presunción de inocencia que obra siempre a favor del acusado.

2.3. La cadena de custodia

Para que la prueba de cargo (o descargo) obtenida pueda tener relevancia y lograr la convicción favorable a los intereses de parte (y de la que deberá quedar buen reflejo en el informe pericial), se hace necesario garantizar que las evidencias digitales encontradas han sido almacenadas de forma adecuada y sin posibilidad de manipulación; o, como se suele expresar en términos forenses, que se respete la cadena de custodia[26].

En este contexto, se entiende por cadena de custodia el proceso utilizado para documentar la historia cronológica de una prueba, con el objetivo de convencer al tribunal de que es razonablemente probable que la exposición sea auténtica, así como de que nadie ha alterado la prueba[27].

Con carácter general, la denominada cadena de custodia se encuentra en íntima relación con las garantías de la prueba de cargo. A este respecto, en la STS 491/2016, de 8 de junio, se señala:

> La cadena de custodia es el proceso que transcurre desde que los agentes policiales intervienen un efecto del delito que puede servir como prueba de cargo, hasta

[25] Por desgracia, no estamos en un ámbito exento de la posibilidad de que se fabriquen pruebas informáticas manipuladas, montajes ficticios, falsedades o distorsiones fraudulentas del material informático de las supuestas víctimas u obtención con técnicas espurias, incluso por los propios investigadores policiales, como recurrentemente pone de relieve la Doctrina técnica especializada en este campo. *Cfr.* esta idea en Rubio Alamillo, J., «La Informática en la reforma de la Ley de Enjuiciamiento Criminal», diario *La Ley*, núm. 8663, 2015, p. 8, donde se expresa explícitamente que los datos informáticos pueden ser manipulados sin que, en ocasiones, ni siquiera pueda detectarse esa manipulación por peritos informáticos.

[26] La cadena de custodia resulta de suma importancia en lo que a pruebas informáticas se refiere, puesto que determinar una posible alteración de la prueba en una evidencia de este tipo es una cuestión matemática y absolutamente dicotómica, esto es, o la prueba no ha sido alterada o la prueba ha sido alterada.

[27] Sobre una descripción amplia de la cadena de custodia en el ámbito de las evidencias digitales puede verse Figueroa Navarro, M.C y Del Amo Rodríguez, A., «La cadena de custodia de las pruebas y los protocolos de actuación de la Policía Científica. Policía Científica: 100 años de ciencia al servicio de la Justicia». *Material de las Jornadas. Centenario de la Policía Científica Española, Ministerio del Interior*, Madrid, 2011. Y, también, Rubio Alamilo, J., «Conservación de la cadena de custodia de una evidencia informática», diario *La Ley*, núm. 8859, 2016.

que se procede a su análisis, exposición o examen en la instrucción o en el juicio. Proceso que debe garantizar que el efecto que se ocupó es el mismo que se analiza o expone y que no se han producido alteraciones, manipulaciones o sustituciones, intencionadas o descuidadas. Esta Sala no mantiene una concepción formal, sino material de la cadena de custodia. Así ha establecido que la integridad de la cadena de custodia debe garantizar que desde que se recogen los vestigios relacionados con el delito hasta que llegan a concretarse como pruebas en el momento del juicio, aquello que se ha recogido y aquello sobre lo que recaerá la inmediación, publicidad y contradicción de las partes y, en definitiva, el juicio del Tribunal, es lo mismo. En cuanto a los efectos que genera lo que se conoce como ruptura de la cadena de custodia, esta Sala tiene afirmado que repercute sobre la fiabilidad y autenticidad de las pruebas –STS 1029/2013, de 28 de diciembre–. Y también se ha advertido que la ruptura de la cadena de custodia puede tener una indudable influencia en la vulneración de los derechos a un proceso con todas las garantías y a la presunción de inocencia, pues resulta imprescindible descartar la posibilidad de que la falta de control administrativo o jurisdiccional sobre las piezas de convicción del delito pueda generar un equivoco. Lo contrario podría implicar una mas que visible quiebra de los principios que definen el derecho a un proceso justo –SSTS 884/2012, de 8 de noviembre, y 744/2013, de 14 de octubre. Seguimos sin una regulación legal adecuada y moderna de la cadena de custodia, pese a su relevancia para la fiabilidad de las fuentes de prueba. Aplicando nuestra doctrina jurisprudencial STS 308/2013, de 26 de marzo, entre otras–, a falta de un marco legal, ha de estimarse que una infracción menor de la cadena de custodia solo constituye una irregularidad que no determina la exclusión de la prueba del proceso, por lo que debe igualmente ser valorada como prueba de cargo apta para desvirtuar la presunción de inocencia, sin perjuicio de que el defecto apreciado pueda afectar a su poder de convicción o fiabilidad. Por el contrario una infracción mayor o muy relevante de la cadena de custodia debe determinar la invalidez de la prueba, en la medida que su valoración afectaría al derecho a un proceso con las debidas garantías, al no poderse garantizar la autenticidad de la fuente de prueba.

Es el juicio de fiabilidad lo que nos va a permitir aceptar la viabilidad procesal de la supuesta evidencia digital como auténtica (no manipulable), íntegra (conservación del contenido) y confiable (obtenida sin técnicas espurias)[28]. Ello implica sujetarse a los estándares y requisitos técnicos por parte del juzgador para comprobar si, efectivamente, se ha analizado correctamente y de modo «confiable» el proceso de obtención de las evidencias digitales y su copia clonada, así como la fiabilidad del procedimiento de preservación, análisis del material y correspondencia de lo incautado con el presentado al órgano judicial llamado a decidir[29].

[28] Si la prueba no ha sido alterada desde su recolección hasta su estudio forense, la cadena de custodia habría sido conservada, mientras que, por el contrario, si la prueba ha sido alterada, la cadena de custodia habría sido destruida

[29] Con poco detalle, el art. 588 de la LECrim ha descrito alguno de estos requisitos técnicos. En este sentido se echa en falta una regulación más prolija o protocolo reglado sobre el modo de

En otro orden, nuevamente el Tribunal Supremo, a través de su ATS 2197/2012, describe muy gráficamente la importancia del mantenimiento de la cadena de custodia cuando dice que «es a través de la corrección de la cadena de custodia como se satisface la garantía de la mismidad de la prueba», garantizando que aquello sobre lo que recaerá la inmediación, publicidad y contradicción de las partes en el acto del juicio es lo mismo que los vestigios que se recogieron relacionados con el delito[30].

La cadena de custodia documenta la ubicación e identifica a la persona encargada de su custodia durante todo el ciclo de vida de las evidencias. Como describe la STS 1045/2011, de 14 de octubre, desde que se recogen los vestigios relacionados con el delito hasta que llegan a concretarse como pruebas en el juicio (que es sobre lo que recaerá la inmediación, publicidad y contradicción de las partes) se ha de tener la garantía de que lo incautado y lo analizado en el juicio por el Tribunal es lo mismo. Esto es, que se hace necesario tener la seguridad de que lo que se traslada o analiza es exactamente lo mismo en todo momento desde el momento en que se interviene hasta el final del estudio o análisis[31].

De lo descrito arriba, se colige la necesidad de preservar la evidencia digital inmediatamente después de ocurrido el delito y de garantizar a partir de ese momento la cadena de custodia, de forma que no puedan existir dudas sobre la «mismidad» de la que habla el Auto del Tribual Supremo anteriormente mencionado[32].

Lo determinante será que lo hallado debe ser descrito, puesto en depósito y analizado con las debidas garantías, pues, como señala el art. 338 de la LECrim, los instrumentos del delito deben recogerse de tal forma que garanticen su integri-

---

obtención de las evidencias digitales por parte del CGPJ. Y en este sentido, puede verse Rubio Alamillo, J., «La informática en la reforma de la Ley de Enjuiciamiento Criminal», *loc. cit.*, p. 7 y ss.

[30] Así, la sentencia de la Audiencia Provincial de Barcelona 1301/2008, de 29 de enero, describe el proceso de custodia del material informático intervenido durante un registro policial, llevado a cabo por los dos peritos judiciales, concluyendo de ello que «hubo una correcta identificación de elementos incautados y una adecuada custodia judicial», aunque afirmando a continuación de forma sorprendente: «pero es que además considera la Sala acreditado que en este caso no hubo ninguna manipulación», algo que va de suyo si, como se ha dicho, ha existido una adecuada custodia judicial, cosa que en ocasiones no ocurre.

[31] En este sentido, el Tribunal Constitucional en STC 170/2003, de 29 de septiembre, para un supuesto en que los soportes informáticos incautados durante una entrada y registro no fueron correctamente identificados, sellados y precintados, estima que se había «producido una deficiente custodia policial y control de dicho material» y que, por tanto, no podía garantizarse la inexistencia de eventuales manipulaciones o alteraciones del mismo habiéndose producido por la sentencia recurrida la vulneración a un proceso con todas las garantías.

[32] Respecto a las evidencias digitales, la importancia de la misma y la ruptura de la cadena de custodia resulta extraordinariamente relevante. Baste de ejemplo el auto de la Audiencia Provincial de Madrid 18559/2011 al desestimar la validez de una prueba pericial informática sobre un disco duro por haberse interrumpido la cadena de custodia al haber permanecido durante un año en poder del denunciante, previamente a la realización del informe pericial. Es de resaltar que este tipo de eventualidades se pueden solventar con un proceso de contextualización de la evidencia digital, evitando así que se invaliden todas las circunstancias probatorias obtenibles de un hecho que se descubra tiempo después de haber ocurrido.

dad y reenvío al organismo adecuado para su depósito. Y así, en interpretación de la STC 170/2003 de 29 de septiembre (FJ 3), se establece[33]:

> La legislación procesal penal pone un especial cuidado en regular el modo en que ha de procederse en la recogida de las piezas de convicción y su custodia. A esos efectos el art. 338 LECrim establece que los instrumentos, armas y efectos que puedan tener relación con el delito se sellarán, si fuera posible, y se acordará su retención, conservación o envío al organismo adecuado para su depósito, con la finalidad evidente de que, siendo elementos probatorios, se evite cualquier alteración en los mismos. En este caso, queda acreditado y así es reconocido en vía judicial por la Sentencia de instancia, sin que fuera negado por la de apelación, que los soportes informáticos no sólo no fueron identificados para determinar el domicilio en el que fueron intervenidos, sino que tampoco se procedió a su correcto sellado y precintando. A ello debe unirse el hecho objetivo, también destacado en vía judicial, de la existencia de una significativa discordancia numérica entre los CD-Rom intervenidos. Ello acredita que se ha producido una deficiente custodia policial y control judicial de dicho material, que no estaba debidamente precintado y a salvo de eventuales manipulaciones externas tanto de carácter cuantitativo (número de las piezas de convicción halladas en los registros) como cualitativo (contenido de aquellos soportes que admitieran una manipulación por su carácter regrabable o simplemente por su naturaleza virgen en el momento de su incautación, e incluso su sustitución por otros), lo que impide que pueda afirmarse que la incorporación al proceso penal de los soportes informáticos se diera con el cumplimiento de las exigencias necesarias para garantizar una identidad plena e integridad en su contenido con lo intervenido y, consecuentemente, que los resultados de las pruebas periciales se realizaran sobre los mismos soportes intervenidos o que éstos no hubieran podido ser manipulados en cuanto a su contenido.

De este modo, la ausencia de control judicial de las evidencias electrónicas lesiona y vicia la pertinencia de la prueba. Si la prueba informática es traída al proceso sin las debidas garantías de custodia policial y control judicial sobre su identidad e integridad, pudiera lesionar el derecho a un proceso con todas las garantías. No estamos ante una garantía meramente legal, sino ante una que afecta a la validez constitucional de la prueba.

El modo de conseguir el mantenimiento de la cadena de custodia y, por tanto, la virtualidad de la prueba (cargo o descargo) consiste en la realización de un

---

[33] Pues bien, en relación con el cumplimiento de las garantías procesales en la incorporación al procedimiento penal de los soportes informáticos incautados y los informes periciales realizados sobre ellos, los recurrentes parten de un doble presupuesto fáctico. El primero, reconocido como hecho probado en ambas Sentencias, es que los soportes informáticos incautados no fueron clasificados ni relacionados por la Guardia Civil en función de los que habían sido ocupados en cada uno de los domicilios registrados. El segundo, explicitado en la Sentencia de instancia y obviado cualquier consideración o razonamiento sobre ello en la de apelación, es que, por un lado, se examinaron pericialmente un número de CD-Rom superior al que consta que se ocuparon en las diligencias de entrada y registro y, por otro, que el primer perito recibió los soportes informáticos intervenidos en cajas rotas y sin etiquetar.

clonado o copia de los dispositivos y la obtención de la denominada *función hash* o huella digital, cuya complejidad técnica y valor jurídico detallaremos en las páginas siguientes, únicas garantías básicas de inalterabilidad de los dispositivos aprehendidos.

3. ACTUACIÓN FORENSE Y PERICIA INFORMÁTICA

3.1. La previa habilitación judicial

En los supuestos de análisis de evidencias digitales, cual es el objeto del presente estudio, el acceso a la información contenida en estos instrumentos queda sometido a la extensión previa y vinculante de una autorización judicial específica[34].

De este modo, ante una previsible intervención de las Fuerzas y Cuerpos de Seguridad del Estado donde se cree la posible incautación de evidencias digitales, no bastará con la motivación genérica de la resolución judicial que habilite el registro domiciliario, sino que será precisa una autorización y motivación específica en el auto habilitante –del investigado que pudieran tener relación con los hechos investigados– para poder acceder a su contenido.

---

[34] La STC 173/2011, 7 de noviembre, recuerda la importancia de dispensar protección constitucional al cúmulo de información personal derivada del uso de los instrumentos tecnológicos de nueva generación. Allí puede leerse el siguiente razonamiento: «si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) –por lo que sus funciones podrían equipararse a los de una agenda electrónica–, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información».

Esta resolución ha de dispensar una protección al imputado frente al acto de injerencia de los poderes públicos. Son muchos los espacios de exclusión que han de ser garantizados. No todos ellos gozan del mismo nivel de salvaguarda desde la perspectiva constitucional. De ahí la importancia de que la garantía de aquellos derechos se haga efectiva siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal[35].

El acceso deberá realizarse conforme a las condiciones establecidas en la resolución judicial para asegurar la integridad de los datos y las garantías de su preservación. En este sentido, el art. 588 sexies c de la LECrim da cobertura legal a la necesidad de que se fijen judicialmente las condiciones y el alcance del registro sobre tales dispositivos y la realización de copias, debiendo fijarse las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación haciendo posible, en su caso, la práctica de un dictamen pericial[36].

Sea como fuere, lo cierto es que tanto desde la perspectiva del derecho de exclusión del propio entorno virtual como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador o dispositivo electrónico para acceder a su contenido exige un acto jurisdiccional habilitante. Y esa autorización, en principio, no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en la que se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías[37].

El art. 588 series c de la LECrim establece que el juez fijará las condiciones para asegurar la integridad de los datos y las garantías de su preservación, pero en ningún momento especifica en qué modo se debe proceder al acceso de la información para preservar los datos contenidos en los dispositivos intervenidos. Adivina

[35] La posible lesión al derecho fundamental a la intimidad es patente como también describe la STC 121/1998, de 15 de junio, en su FJ 3.

[36] Se hace necesario documentar la elación detallada y exacta (por parte de la fuerza actuante que se hará cargo de los dispositivos electrónicos que constituyen la fuente de prueba) de quién, cuándo y durante cuánto tiempo ha tenido acceso a los dispositivos electrónicos intervenidos, antes de devolverlos al juzgado instructor, que será el custodio definitivo –en realidad el servicio común– de los mismos como efectos del delito.

[37] La doctrina del TC es firme al señalar que el contenido de un ordenador personal forma parte de la intimidad de su propietario y no se puede acceder al mismo sin autorización del titular o de un juez. Referido al caso, el Constitucional desautoriza al Tribunal Supremo y afirma que el llevar un aparato a reparar o el utilizar un programa de intercambio de archivos no puede ser entendido como una autorización para que la policía entre a mirar el contenido de un ordenador. Detrás de esta decisión está una postura muy frecuente en nuestro Tribunal Constitucional: proclamar con fuerza los derechos fundamentales recordando su valor extraordinario como protección a los ciudadanos frente al poder, pero no aplicar esa teoría en los casos que le llegan.

ya el lector que una mala praxis puede dar al traste con todo el juicio de fiabilidad ya descrito[38].

En última instancia habrá que asegurar las garantías que permiten preservar la cadena de custodia de modo que se desvanezca cualquier tipo de duda acerca de la identidad e integridad plena de los dispositivos intervenidos y de las copias que se efectúen. Se ha de posibilitar, por tanto, que se realicen las periciales oportunas que acrediten la imposibilidad de cualquier manipulación no autorizada judicialmente[39]. Lo que se conoce vulgarmente como volcado comprende en realidad dos operaciones, el clonado o copia y la obtención de la correspondiente firma o código *hash.*

---

[38] En este contexto, la STS 342/2903, de 17 de abril, (FJ 8) establece que: «El acceso de los poderes públicos al contenido del ordenador de un imputado, no queda legitimado a través de un acto unilateral de las fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE) [...]. Pero su contenido también puede albergar –de hecho, normalmente albergará– información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones. El correo electrónico y los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas. Es opinión generalizada que los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito que sería propio de la inviolabilidad de las comunicaciones. La comunicación ha visto ya culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya tutela constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones [...]. La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital».

[39] Sobre este aspecto puede verse Martínez Guerrero, A., «Las diligencias de entrada y registro en el procedimiento penal español», *Revista Actualidad Judicial* núm. 3, enero-junio, 2019, p. 45 y ss.

3.2. El clonado

Sobre cómo se realiza tal clonado o copia debe quedar claro que, conforme a la jurisprudencia consolidada del Tribunal Supremo, los volcados constituyen un procedimiento informático y técnico que, en algunas ocasiones, puede ser muy lento, pero siempre ajeno a la ciencia jurídica[40].

El análisis y pericia del material informático no se llevará a cabo sobre los soportes originales, sino sobre las copias que de los mismos se realicen. Para la obtención de la evidencia digital como primera operación se realiza el denominado clonado de datos, consistente en la realización de una copia espejo, bit a bit, de la información digital original[41].

Desde el punto de vista jurídico, el clonado constituye una garantía del juicio de fiabilidad en el registro y análisis de los dispositivos y que permite acreditar la *mismidad* de lo aprehendido, esto es, que lo que se copia es imagen fiel de lo ocupado o intervenido. De este modo, se preserva la fuente original al tiempo que se facilita a los investigadores o peritos trabajar a partir de las copias, ya sin el riesgo de una alteración imprudente o malintencionada. Quedará así garantizada la mismidad del dispositivo intervenido y, ante cualquier duda que pueda plantearse en el proceso sobre alteración de la prueba, se podrán llevar a cabo las operaciones de contraste necesarias entre la copia y el original[42].

Tales copias o clonados se materializarán –en casi todos los supuestos– en los laboratorios informáticos policiales dada la complejidad técnica de estas operaciones y, de ser posible, bajo la custodia o vigilancia del servicio común[43]. Por ello, deberá determinarse en el acta de registro (con fe pública judicial) la identificación y precinto de los dispositivos, así como cuantos datos permitan identificar a su posible titular, claves si las hubiera y demás elementos que aseguren el material probatorio, así como en poder de quién quedan los dispositivos intervenidos.

---

[40] *Vid*. la STS de 26 de septiembre de 2005.

[41] Se trata de obtener la evidencia clara, manifiesta y tan perceptible de una cosa, que nadie puede dudar de ella.

[42] Nuevamente, la STS 3 de noviembre de 1997 expresa: «... al igual que en el caso de los documentos comunes, puede haber documentos electrónicos sin firma, el documento electrónico (y, en especial, el documento electrónico con función de giro mercantil) es firmable, en el sentido de que el requisito de la firma autógrafa o equivalente puede ser sustituida, por el lado de la criptografía, por medio de cifras, signos, códigos, barras, claves u otros atributos alfa-numéricos que permitan asegurar la procedencia y veracidad de su autoría y la autenticidad de su contenido. Por lo tanto, si se dan todas las circunstancias necesarias para acreditar la autenticidad de los ficheros electrónicos o del contenido de los discos de los ordenadores o procesadores y se garantiza, con las pruebas periciales en su caso necesarias, la veracidad de lo documentado y la autoría de la firma electrónica utilizada, el documento mercantil en soporte».

[43] Solo de manera excepcional se podrán realizar *in situ*, pues se trata de una actuación que exige de unos medios técnicos y de amplio lapso que lo hacen incompatible con la agilidad del registro y con el mandato recogido en el artículo 552 de la LECrim.

El clonado forense de discos duros se realiza a fin de certificar y mantener la cadena de custodia de las evidencias digitales contenidas en el dispositivo[44]. Ello es fundamental en cualquier proceso judicial ya que, de no hacerse correctamente, los elementos probatorios quedarían invalidados. Es deber del perito informático certificar la cadena de custodia, esto es, que las evidencias aprehendidas permanecen inalteradas desde el momento en que son intervenidas, pudiendo certificar su originalidad en cualquier momento posterior a la intervención.

La copia del dispositivo incautado se realizará en otro dispositivo de almacenamiento o fichero de imagen obteniendo la firma *hash* de los bits leídos durante el proceso. Con ello, se obtiene una copia exacta de todo el contenido del disco duro, además de certificar la correspondencia de su contenido con el original mediante la coincidencia de las firmas con *hash*[45].

Los investigadores o, en su caso, el perito informático de parte[46] deberá documentar exhaustivamente el proceso de clonado forense del disco duro o dispositivos de que se trate, incluyendo la situación y tipología del dispositivo original intervenido, así como las características del dispositivo donde se va a volcar la información clonada. Para ello, como primera medida resulta determinante –como se ha dicho en el epígrafe anterior– la identificación detallada, con número de serie del dispositivo que se trate y características del mismo, realizada por el letrado de la Administración de Justicia en el acta de la entrada y registro, y de la que deberá darse cuenta en el informe respecto del cual se pretende el clonado.

Todo ello deberá incorporarse en el informe de peritaje informático, de forma detallada e inteligible, a fin de asegurar la cadena de custodia de las evidencias digitales aprehendidas (físicas y lógicas) antes de proceder al estudio de las mismas.

En relación con el procedimiento de obtención de la evidencia digital, el Tribunal Supremo exonera al secretario judicial (actual letrado de la Administra-

[44] Entre las herramientas para el tratamiento técnico pericial de memorias destaca *Volatility*, conjunto de herramientas desarrolladas en *Python*. Permite hacer volcados de memoria de máquinas con sistemas operativos Windows, Linux, Mac OSX e incluso Android trabajando con versiones tanto de 32 como de 64 bits. A partir de los datos se pueden extraer, por ejemplo, tipo de sistema, fecha y hora, puertos abiertos, ficheros cargados por procesos, así como DLL, módulos del *kernel*, direccionamiento de memoria por procesos, claves de registro utilizadas en los procesos, etc. Otros ingenios periciales informáticos lo constituyen las herramientas *Memoryze* y *RedLine*.

[45] Entre las técnicas más utilizadas que se conocen de tratamiento de discos destaca *Dcdd3*, que permite trabajar sobre el disco del equipo que se quiere analizar realizando copias a bajo nivel para proteger el original. Por su parte, se suele preferir para realizar la copia bit a bit o réplicas de imagen de disco la herramienta *Guymager*.

[46] La clonación forense de discos duros o el peritaje de parte puede requerir de un laboratorio de informática forense móvil compuesto por dispositivos electrónicos específicos, así como de *software* concreto para realizar el clonado forense, bit a bit, de los dispositivos a intervenir para el clonado forense de discos duros, pudiendo realizar intervenciones *in situ*, e incluso en dependencias judiciales ante el letrado de la Administración de Justicia.

ción de Justicia) de permanecer durante un proceso de clonado de dispositivos realizado por la policía judicial[47].

3.3. La obtención del *HASH* o huella digital[48]

Las evidencias electrónicas deben seguir un tratamiento específico para preservar y mantener la cadena de custodia, conservación de las evidencias y seguir un proceso de contextualización adecuado para que, en caso de surgir alguna conclusión cuestionable o controvertida, ésta pueda ser analizada de nuevo por los mismos intervinientes u otros distintos, con las garantías de que la evidencia sigue intacta. Esto es, que se permita la contradicción de la prueba a través de su *repetibilidad*[49].

En cuanto se ha realizado el volcado de los datos, se procede a obtener la firma *hash* de los ficheros electrónicos aprehendidos. Dicha firma *hash* es una función basada en un algoritmo resumen de los bits que componen el fichero, cuya aplicación práctica es la de afirmar que dicho fichero no ha sido alterado con posterioridad[50]. Al cambiar un solo bit del fichero digital, la firma *hash* cambia. Si la firma de dos ficheros coincide, significa que ambos son plenamente coincidentes[51].

La integridad del contenido se obtiene comparando las firmas *hash* obtenidas de la información aprehendida y de la formación original, debiendo ser ambas coincidentes. Al firmarse la imagen digitalmente mediante una *función hash* que permite identificar unívocamente el contenido de la imagen forense se posibilita saber, en todo momento, que la información contenida en la copia es idéntica a la original.

---

[47] Así, la STS 256/2008, de 14 de mayo, señala que dicha presencia es inútil e innecesaria dado que el letrado de la Administración de Justicia no es experto técnico en dicha materia, y por ello no se requiere su presencia durante la práctica de la pericial informática. En el mismo sentido resuelve la STS 1599/1999, de 15 de noviembre, cuando dispone que «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».

[48] El término *hash* proviene, aparentemente, de la analogía con el significado en inglés, esto es, picar y mezclar.

[49] Para poder ser calificada de evidencia digital una prueba se requiere la cumplimentación de los siguientes elementos en materia forense: identificación, preservación, recuperación, análisis y presentación de los hechos.

[50] Una *función hash* es una función computable mediante un algoritmo tal que: H: U → M; x → h(x). Tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte en un rango de salida finito, normalmente cadenas de longitud fija. Es decir, la función actúa como una proyección del conjunto U sobre el conjunto M. También se denominan funciones resumen.

[51] Marques Arpa, T. y Serra Ruiz, J., «Cadena de Custodia en el Análisis Forense», en *Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información. Alicante, 2-5 de septiembre de 2014.* Universidad de Alicante, Alicante, 2014, p. 167.

En todo informe técnico pericial debe hacerse constar el denominado *formulario de adquisición de evidencias*, en el que deben quedar recogidas tanto la cadena de custodia como las autorizaciones de acceso a la información. Estos códigos *hash* permitirían, según lo exigido en derecho procesal penal para las evidencias digitales, repetir las pruebas, tantas veces como se considere necesario para eliminar las dudas, y permitir el análisis a la parte contraria con el fin de no incurrir la indefensión de la otra parte[52].

Es fundamental que el informe pericial que lleven a cabo los investigadores de las Fuerzas y Cuerpos de Seguridad del Estado (o en su caso el perito de parte) establezca, además de la metodología técnica usada en el volcado, las huellas digitales o códigos de cada uno de los ficheros informáticos obtenidos del dispositivo electrónico clonado, así como de la fecha del cálculo de la misma.

La *función hash* permite además que terceros distintos de quienes hayan obtenido la copia digital puedan someterla a contraste. Lo contrario impediría la eficacia de la prueba por ser de imposible contradicción[53].

---

[52] La Sentencia de la Audiencia Provincial de Málaga 1/2011 es una buena fuente de detalles acerca de procedimientos de custodia de las evidencias digitales y uso en sede judicial de tan singular concepto técnico en orden a fundamentar la convicción del tribunal juzgador. Así, se señala que declaraciones de los agentes policiales, tales como «se extrajeron los discos de cuatro ordenadores, se sellaron y se precintaron –por ello no se hizo huella digital–» o que «los CDs empleados eran de una sola escritura y como las copias de los discos se sellaron, no hizo falta hacer el *Hash* o huella digital».

[53] Así, la célebre Sentencia del *Caso Anonymus* dictada por el Juzgado de lo Penal núm. 3 de Gijón, de 6 de julio de 2016 (FJ 5.ª), y que condujo a la absolución de los acusados estableció que «... Pese a que el TS tiene declarado –entre otras en sentencias de 7 de julio de 2010 y 26 de abril de 2016– no basta la mera sospecha sino la evidencia de la ruptura de la cadena de custodia, en el presente supuesto la confusión y contradicción apreciadas acerca de la adopción de garantías suficientes para preservar la identidad e integridad de los efectos incautados a los tres acusados y sobre la posible manipulación o contaminación de los mismos, exceden como se decía anteriormente de la mera sospecha y vienen a evidenciar la ruptura de la cadena de custodia y asimismo exceden de la mera irregularidad o infracción menor a que se refiere la jurisprudencia más reciente y valorados los datos relativos a los efectos incautados y las medidas adoptadas respecto de los mismos en relación con los datos relacionados acerca de los volcados de datos, las manifestaciones efectuadas por el secretario judicial con ocasión del primer volcado en clara contradicción con las de los testigos y peritos que elaboraron los informes de errores y solicitaron y practicaron un nuevo volcado, los defectos de forma apreciados con ocasión de la citación de los investigados, las contradicciones acerca de los efectos examinados en relación con el anterior volcado incluso relativas al número de efectos examinados, y las afirmaciones relativas a que no se examinan determinados dispositivos por carecer de interés, etc que no fueron debidamente aclarados en el plenario por los testigos y peritos, se considera que debe acogerse la cuestión invocada por las defensas por estimar que se produjo la vulneración del derecho a un proceso con las debidas garantías y en consecuencia del derecho de defensa y el derecho a la tutela judicial efectiva consagrada en el art. 24 de la C.E. en contra de lo que sostiene el Ministerio Fiscal y en consecuencia prescindir de la prueba relativa a los efectos incautados a los acusados y la prueba de análisis de los mismos que de ella trae causa».

3.4. La formación de la imagen digital como evidencia electrónica

Fruto de la combinación de los dos procedimientos anteriores, resulta de vital importancia la obtención de la imagen como instrumento de acreditación de la obtención de las evidencias digitales.

El término informático «imagen» se refiere al contenido de la información de un dispositivo electrónico, a su vez, contenido, como copia, en otro. Es decir, que cuando se emplea en los informes periciales la expresión «*imagen de un dispositivo electrónico*» (*v.gr.*, disco duro o USB) se está indicando que se ha creado un archivo que contiene la estructura y los contenidos del dispositivo original[54]. El original y la copia serán idénticos en el momento justo en que se hace la imagen. En resumen, las imágenes forenses son una copia exacta y no manipulable de los datos contenidos en los equipos informáticos originales[55].

De esta forma, obteniendo una imagen forense podemos garantizar la integridad de la información que se presenta, constituyendo la forma más eficaz y fiable de preservar y presentar la información digital.

4. EL INFORME PERICIAL

4.1. Doctrina general sobre la utilización de este medio de prueba. Su necesario carácter de prueba anticipada en el ámbito digital

La LEC en su artículo 335.1 define el dictamen pericial como «una actividad procesal mediante la que una persona o institución especialmente cualificada suministra al Juez argumentos o razones para la formación de su convencimiento acerca de ciertos datos controvertidos, cuya percepción o comprensión escapa a las aptitudes comunes judiciales». Por su parte, en el orden penal, la LECrim regula lo relativo al informe pericial en el Capítulo VII del Título V, dentro del Libro II correspondiente al Sumario (artículos 456 a 485), y en la Sección 3.ª del Capítulo III, dentro del Título 3.º del Libro III referente al Juicio Oral (artículos 723 a 725).

[54] Un archivo es un conjunto de bits que son almacenados en un dispositivo. La imagen forense constituye, entonces, una copia íntegra de todos los sectores que componen un volumen físico o soporte digital (copia byte a byte) de toda la información contenida en un soporte digital. De esta forma, obteniendo una imagen forense podemos garantizar que tenemos una copia con el 100% de la información original.

[55] Como herramienta suele utilizarse *ForLEx*, que constituye distribución Linux orientada a aplicaciones de informática forense. Incluye FTK Imager, que permite crear imágenes de los sistemas para su posterior análisis forense. Permite agregar más herramientas a las que ya presenta por defecto. Por su parte, *Autopsy* es un conjunto de aplicaciones muy útiles para el análisis forense que permite un análisis de la línea de tiempo para ayudar a identificar la actividad. Permite búsquedas de palabras sobre todo el equipo, analiza el registro del sistema operativo Windows y extrae datos EXIF de las imágenes.

La buena práctica judicial, y como extensión del juicio de fiabilidad, haría que la autoridad judicial dicte auto ordenando realizar la pericial informática correspondiente a los grupos especializados de información de los investigadores judiciales o a designar perito o experto de confianza. Por otra parte, en los supuestos de que la parte acusada[56] (o el propio tribunal a la luz de los informes presentados por los investigadores o acusador particular) albergue dudas de la fiabilidad del material probatorio, podrá acordarse la práctica de la pericial informática para descartar éstas y determinar si los archivos informáticos han sido alterados y manipulados o no[57].

La constitucionalización del derecho a la prueba digital comporta la exigencia de efectuar una lectura de las normas procesales tendente a permitir la máxima actividad probatoria por mor del principio *favor probatione*[58]. Dada la complejidad técnica de los tratamientos arriba descritos, lo normal será que la pericia informática sobre la evidencia digital no pueda practicarse en el día señalado para la vista oral concurriendo a la defensa del informe correspondiente. Ahora bien, al no ser reproducible en el juicio oral, debería estar presente el letrado de la Administración de Justicia para que la misma tenga plena validez probatoria *ex* arts. 476 y 477 de la LECrim quedando configurada, por tanto, como prueba anticipada.

[56] No cabe, como señala la STS 587/2003, de 16 de abril, imponer a la defensa carga alguna en el sentido de justificar su impugnación del análisis efectuado.

[57] De la importancia del informe pericial informático da buena cuenta la STS 2047/2015 de 19 de mayo de 2015, cuando estableció la necesidad de llevar a cabo un informe pericial informático que acredite la identidad de los interlocutores, así como la integridad de la conversación mantenida a través de una red social, para que dicha conversación sea aceptada como prueba válida en un procedimiento judicial y establece: «la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas» y basa esta preocupación en la facilidad de manipulación de los archivos digitales mediante los que se materializa ese «intercambio de ideas», amparándose en el anonimato y en la facilidad de creación de cuentas con identidades fingidas que habitualmente permiten las plataformas de redes sociales, haciendo posible de esta manera «aparentar una comunicación en la que un único usuario se relaciona consigo mismo». Por ello, en caso de impugnación, se desplaza la carga de la prueba hacia quien pretende aprovechar la idoneidad probatoria de dichas conversaciones cuando éstas son aportadas al proceso mediante archivos de impresión. La sentencia concluye estableciendo de forma terminante que «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».

[58] En estos términos se pronuncia la STC 10/2009, de 12 de enero, que considera que la legislación procesal criminal debe ser interpretada «sin desconocimiento ni obstáculos» al derecho fundamental a la prueba; y la STC 1/1992, de 13 de enero, al afirmar que «la garantía del art. 24.2 del derecho a la defensa, consiste en que las pruebas pertinentes propuestas sean admitidas y practicadas por el Juez o Tribunal y al haber sido constitucionalizado impone una nueva perspectiva y una sensibilidad mayor en relación con las normas procesales atinentes a ello, de suerte que deban los Tribunales de justicia proveer a la satisfacción de tal derecho, sin desconocerlo ni obstaculizarlo».

4.2. El peritaje forense informático

Para lograr que la prueba electrónica tenga una mayor fuerza de convicción sobre el tribunal, resulta necesario presentar la evidencia digital que se va a utilizar como medio de prueba dentro del contexto en el que se ha generado e introducido en el proceso con las garantías ya descritas. Así, el art. 384.2 de la LEC prevé la conveniencia de que la parte que quiera proponer este tipo de medios de prueba aporte un dictamen pericial, así como cualquier medio de prueba instrumental que considere conveniente para incrementar el poder de convicción de dicha prueba sobre el tribunal[59].

En cualquier caso, la prueba pericial informática será indispensable para los supuestos en que se impugne la veracidad de la prueba digital aportada –tal y como dispone la STS 224/2017, de 8 de marzo–, así como cuando se requiera el acceso a la información contenida en un dispositivo y la misma haya sido encriptada o eliminada o, simplemente, cuando el acceso a dicha información sea difícil y se requiera por ello conocimientos técnicos.

Aunque en principio la prueba pericial informática pudiera parecer una prueba pericial más, dado que no tiene un tratamiento procesal diferenciado con respecto a las otras, lo cierto es que ostenta un carácter especial[60]. Tal singularidad deriva de las características particulares de las fuentes de prueba digitales, especialmente su volatilidad y su facilidad de replicación y alteración, que las distingue del resto de fuentes de prueba utilizadas en otro tipo de pericias y, en particular, de las fuentes de prueba documentales. La prueba pericial alcanza, entonces, por sí, caracteres, extremadamente relevantes, que se tornan decisivos cuando se refiere a aspectos técnicos y especialmente complejos como es el ámbito informático[61].

Para obtener tales razones y argumentos, el perito informático usa una rama de la informática denominada *informática forense*, definida en la literatura anglosajona (*Computer Forensics*) como «la colección de técnicas y herramientas para encontrar evidencias en un ordenador»[62].

---

[59] En este contexto, Bueno de Mata, F., Prueba Electrónica y Proceso 2.0, *op. cit*., p. 130, define a las mismas como «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».

[60] Todas las vicisitudes derivadas del momento y la forma de aportación del dictamen pericial al proceso, su valoración por el juez, las obligaciones y las condiciones del perito, su posible tacha o recusación se rigen por las mismas reglas que el resto peritajes. Sobre esta cuestión véase ampliamente Figueroa Navarro, M., Dolz Lago, M.J. y Valmaña Ochaita, S., «La prueba pericial científica», en *Coleccion de Ciencias Jurídicas y Forenses*, Madrid, 2012.

[61] Gimeno Sendra, V., *Derecho procesal civil. El proceso de declaración. Parte General*, Colex, Madrid, 2010, p. 473.

[62] La informática forense es una ciencia, de reciente aparición, que se encarga de asegurar, identificar, preservar, analizar y presentar un conjunto de datos que pueden constituir pruebas digi-

En el ámbito de la informática forense, campo propio de actuación del peritaje de las nuevas tecnologías, se especifican una serie de procedimientos de cara a garantizar que la evidencia electrónica se adquiere, se conserva y se trata de manera que se cumplan los preceptos de inalterabilidad, conservación y posibilidad de repetición de los resultados[63].

De este modo, para que la prueba o evidencia digital pueda alcanzar relevancia en sede judicial, se requiere cumplir las siguientes características: *verificable* (se debe poder comprobar la veracidad de las conclusiones extraídas a partir de la realización del análisis); *reproducible* (se deben poder reproducir en todo momento las pruebas realizadas durante el proceso); *documentada* (de manera comprensible y detallada); *independiente* (las conclusiones obtenidas deben ser las mismas, independientemente de la persona que realice el proceso y de la metodología utilizada); *auténtica* (debe ser verídica y no haber sufrido manipulación alguna, garantizando y asegurando para ello su total integridad); *completa* (debe representar la prueba desde un punto de vista objetivo y técnico, sin valoraciones personales, ni prejuicios); *creíble* (debe ser comprensible por los órganos judiciales profanos en la materia); y, finalmente, *confiable* (las técnicas utilizadas para su obtención no deben generar ninguna duda sobre su veracidad y autenticidad).

4.3. Objeto de la pericia informática

Con independencia de las diversas clases de peritaje informático existentes, en este estudio vamos a centrarnos en el denominado peritaje forense informático, cuya virtualidad consiste en obtener evidencias de la información digital encontrada en los dispositivos informáticos y confeccionar los medios de prueba correspondientes.

En cuanto al objeto de la pericia informática, ésta viene a concentrarse en el análisis de los equipos intervenidos o dispositivos de almacenamiento en el marco de un procedimiento judicial penal por delito. Una veces para concretar el tipo penal que se persigue (análisis de archivos, enlaces, historiales de búsqueda, *malware* insta-

tales, de tal modo que éstas puedan llegar a ser aceptadas en un proceso judicial. En este contexto, tradicionalmente, se distingue la informática forense *(Computer Forensics)* de lo que se vienen conociendo en este entorno como electrónica digital forense (*Digital Forensics)*, y en íntima relación con el concepto de seguridad informática, y que se refiere al uso de métodos científicamente derivados y comprobados para la preservación, adquisición, validación, identificación, análisis, interpretación, documentación y presentación de evidencias digitales derivadas también de fuentes digitales con el propósito de facilitar o promover la reconstrucción de eventos de carácter criminal o de ayudar a anticiparse a acciones no autorizadas que puedan perturbar operaciones planificadas. Para una aproximación al estudio de la ciencia forense *vid.,* ampliamente, Caloyannides, M.A., *Computer Forensics and Privacy*, Artech House, London, 2001.

[63] Es decir, que se puedan repetir los resultados obtenidos el número de veces que sea necesario, para eliminar cualquier duda respecto a ellos o a los procedimientos empleados para obtenerlos.

lados y ocultos...)[64]. Otras, se pretende conocer la autoría del delito (grado de conocimientos informáticos, *nicks*, procedencia del interlocutor, etc.).

Lo determinante será que las distintas operaciones periciales queden plasmadas en el informe pericial y que necesariamente deberá comprender la descripción del objeto junto con la relación detallada de las operaciones practicadas; y, muy especialmente, las conclusiones de los peritos según las reglas de la ciencia y arte informática o conclusiones[65].

En este contexto, la pericia de autenticidad implica la facultad de tener a disposición tanto el *hard* como el *soft* como patrón de materias de comparación (indubitable), y que permite el contraste o análisis comparativo determinante (o no) de la autenticidad e integridad del elemento cuestionado. Así, las fases y elementos básicos que componen todo análisis forense digital son las siguientes:

1. Identificación del hecho tratado y su entorno.
2. Recopilación de evidencias.
3. Preservación de la evidencia.
4. Análisis de la evidencia.
5. Contextualización de la evidencia.
6. Documentación y presentación de los resultados.

Con toda esta información, el perito informático forense elaborará un informe pericial que se presentará ante el tribunal.

4.4. Normas y estándares para la elaboración de los informes periciales informáticos

Nada dice la LECrim o la LEC sobre las especificaciones o metodología técnica usada en el volcado y demás técnicas usadas para obtener las huellas digitales o códigos *hash* de los ficheros obtenidos en el dispositivo clonado (ya descritas en apartados anteriores) y de las que también se deberá tomar razón, en orden a una

[64] La STS 1102/2007, de 21 de diciembre, ha puesto de manifiesto la importancia de exponer debidamente los principios, leyes científicas y técnicas empleadas por constituir, en realidad, el fundamento necesario del consecuente dictamen pericial, y así expresa: «la necesidad de tomar en consideración, entre otros extremos, la dificultad de la materia sobre la que verse el dictamen, la preparación técnica de los peritos, su especialización, el origen de la elección del perito, su buena fe, las características técnicas del dictamen, la firmeza de los principios y leyes científicas aplicados, los antecedentes del informe (reconocimientos, períodos de observación, pruebas técnicas realizadas, número y calidad de los dictámenes obrantes en los autos, concordancia o disconformidad entre ellos, resultado de la valoración de las otras pruebas practicadas, las propias observaciones del Tribunal, etc.); debiendo éste, finalmente, exponer en su sentencia las razones que le han impulsado a aceptar o no las conclusiones de la pericia».

[65] *Vid*. art. 478 LECrim.

ANALES DE LA FACULTAD DE DERECHO, 38; 2021, PP. 43-79

buena práctica procesal y profesional de acuerdo con la normativa de calidad profesional del sector.

Así, para la realización del análisis forense existen una serie de estándares nacionales e internacionales que recogen unas guías de buenas prácticas que tratan de garantizar, mediante su seguimiento y correcta aplicación, la validez como medios de prueba de las evidencias recogidas en un posterior proceso judicial[66].

En cualquier caso, en el ámbito forense merece destacarse la familia ISO 27000, que contiene una serie de normas estándares de seguridad publicadas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). En concreto, la ISO 27037 proporciona directrices para la identificación, recolección, adquisición y preservación de la prueba digital[67]. Por su parte, las normas UNE 71505 y 71506 tienen como finalidad dar una metodología para la preservación, adquisición, análisis y presentación de pruebas digitales[68].

Otra norma de extraordinaria importancia es la RFC 3227. Este documento, publicado por la Internet Engineering Task Force (IETF), recoge directrices para recopilar y almacenar evidencias sin ponerlas en riesgo[69]. En el mismo, se describen, en primer lugar, unos principios directores a tener en cuenta durante la recopilación de evidencias (y que divide en cuatro apartados)[70]; en segundo lugar, describe las recomendaciones para el procedimiento de recopilación, que debe ser lo más detallado posible, sin ambigüedades y minimizando la toma de decisiones durante la recogida de evidencias[71]; y, finalmente, en relación con el procedimiento

---

[66] Tales criterios, no obstante, no tienen un carácter unánime en la doctrina forense y la normativa de referencia en ausencia de criterio vinculante para a ser una guía de buena práctica profesional.

[67] Esta norma ofrece orientación para tratar situaciones frecuentes durante todo el proceso de tratamiento de las pruebas digitales. Además, define dos roles especialistas: DEFR (*Digital Evidence First Responder*s, expertos en primera intervención de evidencias electrónicas) y DES (*Digital Evidence Specialists*, expertos en gestión de evidencias electrónicas).

[68] Otras guías similares son UNE 71506 (Metodología para el análisis forense de las evidencias electrónicas); *Guidelines for the best practices in the forensic examination of digital technology*; *Electronic Crime Scene Investigation: A Guide for First Responders*; o *Forensic Examination of Digital Evidence: A Guide for Law Enforcement.*

[69] En las mismas, se contienen principios para la recolección de evidencias donde destacan básicamente tres: el orden de volatilidad de los datos, las acciones que deben evitarse y las consideraciones sobre la privacidad.

[70] Orden de volatilidad de las evidencias digitales, debiendo recopilarse en orden de mayor a menor volatilidad. En un sistema típico, se empezaría por los registros o la memoria caché del sistema y se finalizaría por los dispositivos de almacenamiento (CD, DVD, etc.). Se debe evitar para impedir la fácil destrucción de evidencias, como no apagar el equipo hasta terminar la recopilación de evidencias, utilizar programas residentes en dispositivos conocidos y que no modifiquen la fecha de los ficheros o recopilar la información de red previamente a su desconexión.

[71] Se trata de obtener consideraciones legales respecto de las evidencias, que deben ser admisibles en juicio, auténticas, completas, fiables y creíbles para el juez. En relación con las herramientas informáticas a utilizar en la recopilación, y ya en términos más técnicos, se recomienda disponer previamente de un conjunto de herramientas para cada sistema operativo en soportes de solo lectura, incluyendo un programa para el examen de los procesos del sistema (*ps*); programas para examinar el estado del sistema (como *showrev*, *ifconfig, netstat* o *arp*); un programa para hacer copias a nivel de

de archivo, se indica el modo en que cada evidencia debe asegurarse, así como la documentación de su cadena de custodia[72].

Por su parte, en nuestro ámbito nacional nos encontramos con la UNE 197001, que tiene por objeto el establecimiento de los requisitos formales que deben tener los informes y dictámenes periciales, facilitando la lectura y comprensión de los análisis y conclusiones desarrollados por el perito para personal no especializado, incluyendo, por supuesto, el de los organismos judiciales y policiales. La citada norma contiene unas sencillas recomendaciones acerca de que todo informe o dictamen pericial debe disponer de un título que identifique claramente su objeto y debe constar de una estructura básica compuesta por identificación, índice, cuerpo del informe y, cuando corresponda, documentos anexos, así como que, en cada página del dictamen, debe figurar su referencia identificativa, el número de la página y el total de éstas[73].

Del cuerpo del informe pericial, no han de faltar la precisión objeto, alcance, antecedentes, consideraciones preliminares, documentos de referencia, análisis y conclusiones[74].

4.5. Sobre la consideración de perito informático

Los peritos informáticos son los profesionales que se encargan de dar soporte a la hora de presentar pruebas tecnológicas ante un tribunal. Ellos son quienes se encargan de analizar la veracidad de dichos pruebas y de exponerlas de forma clara y sencilla para que puedan ser comprendidas por un juez[75]. La LEC, en su artículo

bit (como *dd* o *SafeBack*); programas para generar huellas digitales y firmas (como *SafeBack, sha1sum* o *pgp*); y programas para generar y examinar imágenes del núcleo del sistema (como *gcore* o *gdb*).

[72] Responde a las preguntas de «Cómo se encontró y fue tratada la evidencia; Dónde, cuándo y quién la descubrió y recogió, Dónde, cuándo y quién la trató o examinó; Quién, durante qué periodo y cómo la ha custodiado y, en caso de cambio de custodia, cuándo y cómo se ha llevado a cabo».

[73] La información de identificación del dictamen debe incluir título del informe y su código o referencia de identificación; nombre del Organismo al que se dirige el informe pericial y, en su caso, número de expediente o procedimiento; nombre y apellidos del perito, titulación o destreza específica y, en su caso, colegio o entidad a la que pertenece, DNI, domicilio profesional, teléfono, fax, correo electrónico y cualquier otro dato profesional que pudiera existir, salvo que no sea legalmente procedente; nombre, apellidos y DNI del solicitante del informe pericial, si es en nombre propio o en representación de tercero, con sus datos, y cualquier otro identificador legalmente procedente.

[74] Todo ello, sin perjuicio de la declaración del perito acerca de posibles vicisitudes sobre tachas y juramento.

[75] En este sentido, indica la STS de 26 de septiembre de 2005 que no parece discutible que el perito es un auxiliar experto que suministra al juez conocimientos especializados de carácter científico o técnico, de los que él no dispone, y que son necesarios para formar criterio sobre el *thema probandum*; así, en el proceso, es pericia la que se emite a partir de saberes que no son jurídicos y que tampoco corresponden al bagaje cultural del ciudadano medio no especialista; consecuentemente, no pueden darse por supuestos y deben ser aportados al juicio, para que su pertinencia al caso y su concreta relevancia para la decisión sean valoradas contradictoriamente.

340.1, especifica que «los peritos deberán poseer el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de éste. Si se tratare de materias que no estén comprendidas en títulos profesionales oficiales, habrán de ser nombrados entre personas entendidas en aquellas materias»[76].

En el ámbito de las tecnologías informáticas y digitales, esta exigencia legal se concreta en que el perito ostente la condición de ingeniero o ingeniero técnico en informática, existiendo colegios profesionales de ingenieros o ingenieros técnicos en informática para mayor garantía de los dictámenes emitidos[77].

Con independencia de las consideraciones legales, los ingenieros e ingenieros técnicos en informática serían a nivel técnico los únicos profesionales cualificados para la realización de peritajes informáticos dado que el estudio de la ingeniería informática cubre todas y cada una de las áreas de esa disciplina incluyendo, por supuesto, la ciencia forense.

En este contexto, se hace necesario llamar la atención sobre el escaso nivel de conocimientos informáticos que, en ocasiones, ponen de manifiesto los agentes actuantes en las intervenciones policiales por no contar con personal cualificado sobre esta compleja materia. O, en peor escenario, cuando, aun contando con personal y e infraestructura adecuada, los primeros agentes intervinientes no han sabido preservar o recolectar las evidencias digitales de forma conveniente para su correcto análisis posterior en los laboratorios tecnológicos forenses. Los cursos de formación sobre peritaje informático no suponen una titulación oficial ni permiten, por tanto, ostentar la cualidad de perito informático titulado u oficial, no debiéndose admitir como prueba pericial válida por nuestros tribunales[78].

Prevé también la LEC, en su artículo 340.2, que «podrá asimismo solicitarse dictamen de Academias e instituciones culturales y científicas que se ocupen del estudio de las materias correspondientes al objeto de la pericia. También podrán emitir dictamen sobre cuestiones específicas las personas jurídicas legalmente habilitadas para ello».

[76] Con respecto a la identificación del perito informático, ésta, de ser necesario que se produzca, será siempre mediante la presentación del carné o certificado expedido por su colegio profesional, en el que constarán su nombre y sus apellidos, su número de DNI y su número de colegiado, sin ser necesarias chapas, placas u otro tipo de certificaciones.

[77] El colegio es el único órgano profesional que puede garantizar, según el ordenamiento jurídico español, que el perito está en el ejercicio de sus plenas facultades profesionales y que por tanto no ha sido inhabilitado debido a mala praxis por su colegio profesional.

[78] Entre esos cursos pueden mencionarse por su amplia difusión en el campo policial los siguientes: Perito Judicial Informático en la UNIR; Curso de Ciberseguridad y Peritaje Informático Forense de Euroinnova; o el Curso de Peritaje Informático de Emagister. Estos «pseudoperitos» pueden realizar análisis e investigaciones, pero no podrán presentar los informes ante un juez con tal carácter de perito.

5. LA VALORACIÓN DE LA PRUEBA INFORMÁTICA A LA LUZ DE LA JURISPRUDENCIA DEL TRIBUNAL SUPREMO Y EL CONSITUCIONAL

5.1. Sistema de libre valoración de las evidencias digitales

A la prueba electrónica, con carácter general, le serán aplicables las reglas procesales generales sobre actividad probatoria, medios de prueba y resultado probatorio. De este modo la evidencia se inserta en el procedimiento posibilitando el necesario debate contradictorio una vez superado el juicio de fiabilidad descrito en páginas anteriores[79].

La prueba o evidencia digital se incorporará al proceso a petición de las partes, bien solicitando la unión a los autos del propio dispositivo, bien mediante su solicitud al juez para que reclame la remisión de una prueba o documento electrónico[80]. En torno a la valoración de las pruebas en el ámbito procesal, se distinguen, tradicionalmente, dos sistemas: la libre valoración y la prueba legal o tasada.

El sistema de libre valoración de la prueba tiene como característica permitir maximizar la función decisoria del juez al encomendarle a éste la determinación del resultado probatorio específico y conjunto de los medios de prueba aportado a un proceso concreto. Por su parte, la prueba tasada reduce al mínimo esta posibilidad al imponerle al juez *ex ante* una forma determinada de establecer el resultado probatorio de uno o diversos medios de prueba. En cualquier caso, la valoración de la prueba no podrá ser arbitraria, sino que deberá ser siempre motivada y fundamentada *ex* arts. 120.3 CE y 247 LOPJ[81].

Como quiera que sea, en la valoración de la prueba informática rige la previsión del art. 741 de la LECrim referente a la «íntima convicción o apreciación en con-

---

[79] La admisibilidad de la prueba es el resultado de un juicio hecho por el juez sobre las condiciones del medio o actividad probatoria propuestos para su admisión en el proceso. Deberá determinarse si tal material probatorio cumple los requisitos de pertinencia, utilidad y legalidad. La prueba que pretenda ser incluida en el proceso ha de reunir necesariamente dichos requisitos, pues su incumplimiento será motivo de inadmisión de la misma. El juez decidirá por medio de auto sobre la admisión o inadmisión de la prueba. En caso de inadmisión, ésta deberá estar motivada. En relación con el recurso a interponer frente al auto de admisión o inadmisión de la prueba, en función del procedimiento en que nos encontremos, existen una serie de precisiones. Así, en el procedimiento ordinario, conforme al art. 659 LECrim, contra el auto que declare la admisión de las pruebas no cabe recurso, y contra el auto que declare la inadmisión cabrá protesta en aras de interponer en su debido tiempo el recurso de casación contra la Sentencia por quebrantamiento de forma y garantías procesales, al haberse propuesto en tiempo y forma una diligencia que se considera pertinente.

[80] 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 que pudiera 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 un carácter efímero y manipulable mayor que el de las otras pruebas

[81] *Vid.* Urbano Castrillo, E., *La valoración de la prueba electrónica*, *op. cit*., p. 55 y ss.

ciencia» del juzgador respecto a la relevancia de la evidencia digital[82]. Y en relación con ello, el art. 726 del mismo texto legal concreta que «El Tribunal examinará por sí mismo los libros, documentos, papeles y demás piezas de convicción que puedan contribuir al esclarecimiento de los hechos o a la más segura investigación de la verdad», términos extensivos predicables de cualquier clase de soporte o evidencia digital[83].

Se impone, entonces, el sistema de libre valoración de la prueba bajo las reglas de la sana crítica. El sistema de prueba legal se aplicará –solo y exclusivamente– en los casos que la Ley así lo disponga de modo expreso, como puede suceder, *v.gr.*, cuando la prueba electrónica se basa en un documento público con firma electrónica avanzada[84], 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[85].

Lo relevante es, en última instancia, que la prueba informática no conforma prueba plena. No obstante, el peso de las pericias informáticas resulta indudablemente potente para los órganos jurisdiccionales por su valor de convicción, dada la complejidad técnica o científica sobre la que versa, haciendo que, en última instancia, su desprecio o ignorancia por parte del tribunal juzgador ponga en riesgo la ecuanimidad de la resolución adoptada y, en consecuencia, la salvaguarda a un proceso con todas las garantías para el acusado.

5.2. Inadmisión de la prueba pericial informática legalmente solicitada

La doctrina sobre el derecho a la prueba, que inspira la jurisprudencia del Tribunal Constitucional acerca de esta materia, se halla recogida, entre otros numerosos precedentes, en la STC 121/2009, 18 de mayo.

---

[82] Señala el art. 741 de la LECrim que «El Tribunal, apreciando, según su conciencia las pruebas practicadas en el juicio, las razones expuestas por la acusación y la defensa y lo manifestado por los mismos procesados, dictará sentencia dentro del término fijado en esta Ley». Por Real Decreto Ley de 8 septiembre 1928 se introdujo un segundo párrafo a esta previsión señalando que «Siempre que el Tribunal haga uso del libre arbitrio que para la calificación del delito o para la imposición de la pena le otorga el Código Penal, deberá consignar si ha tomado en consideración los elementos de juicio que el precepto aplicable de aquél obligue a tener en cuenta».

[83] La legislación procesal española recoge el sistema de la libre valoración de la prueba basado en las reglas de la sana crítica, entendida esta 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».

[84] *Vid.* el 319.1 LEC.

[85] Según el art. 3.6 de la Ley 59/2003, de 19 de diciembre, de firma electrónica: «El documento electrónico será soporte de: a) Documentos públicos, 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. b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica. c) Documentos privados».

De este modo, recuerda el Tribunal Constitucional que el derecho a la utilización de los medios de prueba pertinentes para la defensa es un derecho fundamental de configuración legal en cuya vulneración, para que tenga relevancia constitucional, han de concurrir varias circunstancias: en primer lugar, el recurrente ha de haber respetado las reglas procesales de tiempo, lugar y forma de su proposición[86]; en segundo término, se ha establecido que la denegación o inejecución han de ser imputables al órgano judicial[87]; finalmente, ha de acreditarse que la ausencia del medio de prueba en cuestión se ha traducido en una indefensión material para la parte, lo que significa que la prueba denegada era decisiva en términos de defensa[88].

En el concreto ámbito de las periciales informáticas y su denegación, la STS 160/2016, de 1 de marzo, ha establecido que la denegación indebida de la pericial de parte solicitada inexorablemente conduce, en aplicación de una amplia jurisprudencia consolidada, a la anulación de la sentencia recurrida y la consiguiente necesidad de celebración de un nuevo juicio oral, que haga posible la práctica de la prueba pericial tecnológica. Y así, razona el TS:

> La Audiencia da por probado el acceso al sistema informático –para lo que ha considerado decisivo el informe pericial– y atribuye la autoría del delito de daños informáticos del art. 264.2 del CP al acusado [...]. Pese a la negativa del acusado, los Jueces de instancia le atribuyen el acceso inconsentido a la vista de la utilización de un nombre de usuario Zapatones identificable con la primera inicial y el apellido del recurrente y de la coincidencia temporal entre esa intrusión y el día en que se produjo el despido. Además, porque resultaría absurdo pensar que lo efectuara el propio denunciante causándose perjuicios a sí mismo y como venganza frente al acusado [...] no se trata de restar valor probatorio a una prueba pericial informática por el simple hecho de que haya sido aportada por la acusación particular. Sobre todo cuando, como expresa la sentencia recurrida, la defensa tuvo cumplida oportunidad en el plenario de someter a contradicción los extremos del dictamen. Sin embargo, sea ese dictamen de carácter oficial o tenga su origen en expertos informáticos no adscritos a un centro de esa naturaleza, lo cierto es que la autoría de una intromisión en los sistemas informáticos ajenos exigirá, en buena parte de los casos, algo más que el conocimiento de una dirección IP y un nickname de usuario. Si a ello se añade que el desconocimiento de los términos del acceso al correo corporativo y al programa de edición de vídeos estuvo originado por no haber sido cursada la correspondiente solicitud judicial, los argumentos que respaldan la reivindicación de la defensa adquieren pleno significado.

[86] No podrá considerarse menoscabado este derecho cuando la inadmisión de una prueba se haya producido debidamente en aplicación estricta de normas legales cuya legitimidad constitucional no pueda ponerse en duda.

[87] Por haberse inadmitido, por ejemplo, pruebas relevantes para la resolución final del asunto litigioso sin motivación alguna o mediante una interpretación de la legalidad manifiestamente arbitraria o irrazonable de tal manera que la prueba denegada o impracticada ha de ser decisiva en términos de defensa.

[88] Esto es, que hubiera podido tener una influencia decisiva en la resolución del pleito, potencialmente trascendental para el sentido de la resolución

Las razones de la pertinencia del dictamen pericial que se solicite por las partes, y que pudiera ser rechazado por el tribunal, pueden llegar a comprometer en mucho los derechos fundamentales del acusado. De este modo, si la pericia informática resulta inadmitida o no practicada, y era decisiva en términos de defensa, resultará ya evidente *ab initio*, que ha existido una lesión al ámbito material protegido por el derecho fundamental a utilizar los medios de prueba pertinentes, especialmente, en los casos en que no exista pericial en contra o se contradiga ésta (si existiera) por alguna de parte[89].

5.3. Obligación del tribunal de no ignorar la pericia informática admitida y practicada

Pues bien, como se ha puesto de relieve en las páginas precedentes, las supuestas evidencias digitales, si no han sido traídas a las actuaciones con las debidas garantías que permitan comprobar tanto la realidad del origen de aquéllas como que las mismas coinciden efectivamente con las contenidas en los elementos ocupados, podrían quedar viciadas en el juicio de fiabilidad[90].

Por otra parte, no resulta infrecuente una actuación culposa de los agentes policiales investigadores que han manipulado las evidencias digitales con inobservancia de las cautelas establecidas para la preservación de la cadena de custodia no pudiendo excluirse, tampoco, como por desgracia se ha constatado, que exista una alteración dolosa de éstos con fines de atribuir la autoría de un hecho a persona en quien, en realidad, no concurrían méritos para ello. Ignorar en tal contexto la contrapericial o pericial solicitada por la parte solo puede conducir a resultados proscritos en el ordenamiento jurídico[91].

Precisamente, uno de los aspectos de la doctrina constitucional y jurisprudencial relativa a la presunción de inocencia es la necesidad de valorar la prueba de

---

[89] Así, la STS 160/2016, 1 de marzo, establecía que, más allá de la consistencia del juicio inferencial proclamado por la Audiencia, siendo que el dictamen pericial de parte (y que constituyó la clave probatoria de la condena del acusado) aconsejaba el complemento de otro informe de experto que permitiera concluir, entre otras cuestiones, si la autoría del acceso a un sistema informático puede decidirse en atención a la utilización de un *nickname* coincidente con el apellido del sospechoso. Que resolviera, en fin, si no puede existir otra alternativa razonable.

[90] La STC 123/2006, de 24 de abril , recuerda en cuanto al derecho de presunción de inocencia consagrado en el art. 24.2 CE que «se configura en tanto que regla de juicio y desde la perspectiva constitucional, como el derecho a no ser condenado sin pruebas de cargo válidas, lo que implica que exista una mínima actividad probatoria, realizada con las garantías necesarias, referida a todos los elementos esenciales del delito y que de la misma quepa inferir razonablemente los hechos y la participación del acusado en ellos».

[91] El delito de estafa procesal está regulado en el art. 250.1.7. del Código Penal. El citado precepto dispone que «incurren en la misma los que, en un procedimiento judicial de cualquier clase, manipularen las pruebas en que pretendieran fundar sus alegaciones o emplearen otro fraude procesal análogo, provocando error en el juez o tribunal y llevándole a dictar una resolución que perjudique los intereses económicos de la otra parte o de un tercero».

descargo, y de cuyo control no escapa el juicio sobre la pericia informática[92]. En este sentido, la STC 55/2015, de 16 de marzo, dice: «ciertamente, este Tribunal tiene fijada doctrina a tenor de la cual el principio de libre valoración de la prueba, reconocido en el artículo 741 de la Ley de Enjuiciamiento Criminal, exige para que pueda considerársele ajustado a la Constitución, que se ponderen los distintos elementos que constituyen la actividad probatoria, sin que de esa ponderación pueda excluirse la prueba de descargo realizada en el juicio oral, ya que ello supone desconocer los derechos del inculpado consagrados en el artículo 24.2 de la Norma fundamental».

En esa argumentación, la doctrina del supremo intérprete de la Carta Magna es clara y contundente. Así, la STC 148/2009, de 15 de junio (citando la STC 186/2006, de 19 de junio), explicita con acierto que «... dentro del control que le corresponde realizar a este Tribunal sobre la eventual vulneración de este derecho (derecho fundamental a la presunción de inocencia) se encuentra verificar si se ha dejado de someter a valoración la versión o la prueba de descargo aportada, concretándose que se exige solamente ponderar los distintos elementos probatorios, pero sin que ello implique que esa ponderación se realice de modo pormenorizado, ni que la ponderación se lleve a cabo del modo pretendido por el recurrente, sino solamente que se ofrezca una explicación para su rechazo»[93].

En este contexto, y en el ámbito de las evidencias tecnológicas, la transcendental STS 987/2012, de 3 de diciembre, absuelve al acusado por ignorar la prueba pericial solicitada por vulnerar la garantía constitucional de presunción de inocencia del recurrente, llegando a dictar nueva Sentencia absolutoria, y de la que merece la pena reproducir la siguiente fundamentación jurídica:

> ... Alega el recurrente que el Tribunal de instancia no ha dispuesto de una «mínima actividad probatoria» que desvirtúe aquélla. Y ello en relación al dato esencial de la autoría de los hechos que se le imputa [...]. En definitiva, Reprocha a la sentencia el desprecio de la prueba pericial que acreditaría que, pese a la identificación

[92] No obstante, la Sala Segunda del TS solo excepcionalmente ha admitido la virtualidad de la prueba pericial como fundamentación de la pretensión de modificación del apartado fáctico de una sentencia, impugnada en casación. El primero, cuando existiendo un solo dictamen o varios absolutamente coincidentes y no disponiendo la Audiencia de otras pruebas sobre los mismos elementos fácticos, el tribunal haya estimado el dictamen o dictámenes coincidentes como base única de los hechos declarados probados, pero incorporándolos a dicha declaración de un modo incompleto, fragmentario, mutilado o contradictorio, de forma que se altere relevantemente su sentido originario. El segundo, cuando contando solamente con dicho dictamen o dictámenes coincidentes y no concurriendo otras pruebas sobre el mismo punto fáctico, el tribunal de instancia haya llegado a conclusiones divergentes con las de los citados informes, sin expresar las razones que lo justifiquen o sin una explicación razonable (*vid.* SSTS. 182/2000 de 8 de febrero y 1224/2000 de 8 de julio). En el primer caso se demuestra un error porque asumiendo su informe al incorporar a los hechos las conclusiones del único informe pericial sin explicación que lo justifique se hace de un modo que desvirtúa su contenido probatorio, y en el segundo se evidencia un razonamiento abiertamente contrario a la exigencia de racionalidad del proceso valorativo (STS 2144/2002, de 19 de diciembre).

[93] Y, en este mismo sentido, cabe citar las SSTC 242/2005, de 10 de octubre, 187/2006, de 19 de junio, 148/2009, de 15 de junio, y 172/2011, de 19 de julio.

de la IP desde la que se desplegó la actividad defraudadora, el indicio que permite inferir que fue el acusado el autor resulta poco concluyente y equívoco [...]. Desde luego el informe pericial no acredita por sí solo el error que se denuncia y es objeto de consideración, siquiera insuficiente, en la sentencia. Eso le inhabilita como documento a los efectos del cauce casacional en que es invocado [...]. Para justificar tales conclusiones la sentencia parte del informe policial, confeccionado a partir de la denuncia de quien luego fue coacusado, y que acredita que la orden telemática dirigida a la entidad bancaria se emitió utilizando una IP que había sido adjudicada a un equipo terminal que usaba una línea telefónica de la que era titular el recurrente [...]. La sentencia enfatiza la validez de la indagación policial. Y concluye: el acusado era el usuario del ordenador usado en dicha comunicación. Y, a partir de tal dato básico infiere que él fue el que impartió la orden. En cuanto al informe pericial aportado por la defensa no hace otra consideración que la de recordar que el perito y la policía «en ningún momento examinaron el ordenador del acusado» [...]. Son las afirmaciones inferidas a partir de ahí las refutadas y ello por ilógicas y en exceso abierta. Todo ello a partir de la ostensible insuficiencia del trato retórico dado a la prueba pericial aportada. La sentencia omite todo análisis crítico de tal informe y lo desautoriza partiendo de un dato, tampoco discutido, que, sin embargo, hace poco razonable tal rechazo [...]. En efecto el propio informe advierte que su objetivo y alcance se reduce a poner en evidencia que la inferencia que vincula ser usuario de un ordenador y línea telefónica no lleva necesariamente a la conclusión de que ese usuario sea el autor de toda utilización telemática de esa infraestructura informática [...]. El informe avala sus conclusiones con experiencias que relata y advierte de que ni siquiera tal posibilidad exige una muy cualificada formación en el invasor que incluso dispone de herramientas de ayuda en la misma red. Al respecto facilita un amplio elenco de links en que se puede obtener tutoriales paso a paso para hacerse con el control de otro ordenador.

De este modo, en el ámbito de las evidencias digitales, la no valoración de las periciales informáticas tiene una transcedencia definitiva y a la que no puede dejar de serle aplicada la doctrina general instaurada ya en nuestra jurisprudencia, pues, como recuerda la STS 258/2010, de 12 de marzo: «La ponderación de la prueba de descargo representa un presupuesto sine qua non para la racionalidad del desenlace valorativo». Por tanto, su toma en consideración por el tribunal llamado a resolver es indispensable para que el juicio de autoría pueda formularse con la apoyatura requerida por nuestro sistema constitucional[94].

[94] *Vid.* SSTC 148/2009, de 15 de junio, y 187/2006, de 19 de junio. Y, en el mismo sentido, la STS 252/2008, de 21 de mayo, recuerda que «La STS de 16 de febrero de 2005 absuelve de una condena en la instancia porque la motivación, al no contemplar referencia alguna a la prueba de descargo, no satisfizo de forma adecuada el estándar de justificación que le era exigible».

5.4. Consecuencias de la inobservancia de las garantías previstas para las evidencia digitales

Como dispone el tenor literal del art. 11.1 de la LOPJ, en los procedimientos se respetarán las reglas de la buena fe y «no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales». La prueba obtenida produciendo la vulneración de derechos fundamentales es ilícita. De este modo, 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 está contaminado de ilegalidad y, por lo tanto, no podrá ser utilizado en los tribunales de justicia como medio de prueba válido y eficaz[95].

Cualquier duda sobre la fiabilidad del material probatorio debiera determinar su inadmisibilidad como medio de prueba denegando virtualidad o efectos probatorios a los datos informáticos que compongan la prueba. De este modo, partiendo de la premisa del art. 11.1 LOPJ, y de conformidad con la STS 320/2011, es imprescindible distinguir entre las pruebas originales nulas, las pruebas derivadas de éstas (directa o indirectamente) y las pruebas independientes y autónomas de la prueba nula. Estas últimas «deben estimarse independientes jurídicamente por proceder de fuentes no contaminadas, como serían aquellas pruebas obtenidas fruto de otras vías de investigación tendentes a establecer el hecho en que se produjo la prueba prohibida».

En este contexto, el Tribunal Constitucional, en su Sentencia 66/2009, de 9 de marzo, ha precisado que la valoración en juicio de pruebas que pudieran estar conectadas con otras obtenidas con vulneración de derechos fundamentales sustantivos requiere un análisis a dos niveles: en primer lugar, ha de analizarse si existe o no conexión causal entre ambas pruebas, conexión que constituye el presupuesto para poder hablar de una prueba derivada. Solo si existiera dicha conexión procedería el análisis de la conexión de antijuridicidad (cuya inexistencia legitimaría la posibilidad de valoración de la prueba derivada). De no darse siquiera la conexión causal no sería necesario ni procedente analizar la conexión de antijuridicidad, y ninguna prohibición de valoración de juicio recaería sobre la prueba en cuestión. En definitiva, se considera lícita la valoración de pruebas causalmente conectadas con la vulneración de derechos fundamentales, pero jurídicamente independientes, esto es, las pruebas derivadas o reflejas[96].

Por lo anterior, para que tan nocivos efectos se produzcan es siempre necesario que la admisión a valoración de una prueba conculque también, de alguna forma, la vigencia y efectividad del derecho constitucional infringido por la origi-

[95] Se trae a colación ahora la Doctrina de TS, mantenida, entre otras, en la Sentencia 416/2005, de 31 de marzo, al examinar cuál es la trascendencia mediata a los efectos inhabilitantes de la prueba obtenida con violación del derecho fundamental, en el sentido de superar las diversas interpretaciones y la integración, en los más justos términos, de lo que el mandato legal contiene como severa proscripción del uso de prácticas constitucionalmente reprobables.

[96] *Vid.* la STC. 81/98 de 2 de abril.

naria que, de este modo, le transmite una antijuridicidad que la obligación de tutela de aquel derecho está llamada a proscribir. De no ser así, aunque la segunda prueba haya sido obtenida a causa de la constitucionalmente inaceptable, conservará su valor acreditativo, pues esa vinculación causal se ha producido en virtud de unos resultados fácticos que no pueden excluirse de la realidad y no existen razones de protección del derecho vulnerado que justifiquen unas consecuencias más allá de la inutilización del propio producto de esa vulneración. Y, lo que puede ser todavía más contundente, cualquier prueba que se obtenga, posteriormente, a partir la prueba contaminada tampoco debería poder ser admitida en un proceso judicial.

De este modo, la prueba electrónica, proveniente de un árbol envenenado, pretende erradicar en juicio la utilización de una prueba secundaria que se obtuvo a partir de una prueba primaria, ilegalmente obtenida, por vulnerar derechos fundamentales.

CONCLUSIONES Y PROPUESTAS DE *LEGE FERENDA*

I. Lo que se viene entendiendo por evidencia o prueba electrónica no ha sido descrito por norma jurídica alguna. Ante la ausencia de una definición legal se hace necesario modernizar la legislación procesal para que defina, de forma homogénea y coherente, el tratamiento a dar a dicha prueba.
II. Con carácter general se viene entendiendo por prueba informática o evidencia electrónica la que contiene cualquier tipo de información almacenada o trasmitida a través de dispositivos informáticos que tiene la virtualidad de poder acreditar los hechos sobre los que versa el proceso.
III. En su naturaleza, la prueba informática participa de las características de los medios de prueba comunes con las especialidades propias de tan singular disciplina. De este modo, la evidencia electrónica constituye una información obtenida a partir de un dispositivo electrónico o medio digital (soporte técnico), el cual sirve para adquirir convencimiento de la certeza de un hecho en orden a la destrucción o mantenimiento de la necesaria presunción de inocencia que siempre obra a favor del acusado.
IV. 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 será aquélla que se obtiene sin violar derechos y libertades fundamentales.
V. Se evidencia una controvertida discusión en la Doctrina sobre el carácter de documento electrónico de las evidencias digitales. Debiera, por tanto, acogerse, en una oportuna reforma legislativa, un concepto amplio de documento para que la previsión del art. 26 del Código Penal pueda tener virtualidad respecto a cualquier soporte que, en última instancia, incorpora o expresa datos, hechos o narraciones con la suficiente eficacia probatoria y, en su caso, necesaria relevancia jurídica.
VI. No existe una homogeneidad legislativa en el tratamiento de la prueba electrónica como documento, lo que da lugar a un posicionamiento jurispru-

dencial restrictivo por los tribunales que no se corresponde con la realidad digital del mundo actual y con el impulso al desarrollo de la sociedad de la información.

VII. En la valoración de la prueba informática serán de aplicación las 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.

VIII. El modo de preservación y conservación de la prueba electrónica dentro del proceso judicial no está, tampoco, regulado debidamente en la normativa procesal donde genéricamente se contemplan medidas de conservación. Debiera protocolizarse y normativizarse la actuación judicial tendente a la obtención y preservación de las evidencias digitales o pruebas informáticas.

IX. El Juez siempre puede y debe, dada la complejidad de la materia, 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 contando, en su caso, 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.

X. La cadena de custodia en el ámbito de las evidencias informáticas constituye un proceso transcendental utilizado para documentar la historia cronológica de tales pruebas con el objetivo de convencer al tribunal de que es razonablemente probable que la exposición sea auténtica, así como de que nadie ha alterado la misma. Una metodología de cadena de custodia con lagunas graves puede destruir la certidumbre sobre la prueba que deba servir de soporte probatorio a la demostración de un delito informático o de un ilícito de cualquier tipo.

XI. Se constata la carencia de una metodología con suficiente rigor y que permita garantizar que las evidencias digitales no se han alterado en absoluto desde su recogida hasta su contrastación en el juicio oral. Sería conveniente que por vía normativa o, al menos, jurisprudencial, se recogiera un modelo de referencia con capacidad para responder a las cuatro preguntas, qué, quién, cuándo y dónde, acerca de cada cambio de la evidencia digital a lo largo de la cadena de custodia, desde su recogida hasta su presentación ante el tribunal.

XII. 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 garantizando así, en última instancia, la autenticidad, inalterabilidad e indemnidad de las mismas.

XIII. El modo de conseguir el mantenimiento de la cadena de custodia y, por tanto, la virtualidad de la prueba (cargo o descargo) consiste en la realización de un clonado o copia de los dispositivos y la obtención de la denominada *función hash* o huella digital, únicas garantías técnicas que permiten la

inalterabilidad de los dispositivos aprehendidos asegurando el debate contradictorio sobre las pruebas.

XIV. La prueba electrónica aportada debe analizarse, como cualquier medio probatorio ordinario o convencional, bajo los principios de oralidad, contradicción, concentración, publicidad e inmediación.

XV. 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. Aunque el carácter técnico-informático de la prueba electrónica no justifica la aplicación automática de un sistema de valoración de prueba tasada, resulta, sin embargo, de extraordinaria relevancia la intervención de un perito informático para elaborar el correspondiente dictamen pericial determinante, sin duda, de la ulterior convicción del tribunal, dada la complejidad de la materia.

XVI. El sistema de prueba legal se aplicará –solo y exclusivamente– en los casos que la Ley así lo disponga de modo expreso, como sucede cuando la prueba electrónica se basa en un documento público con firma electrónica avanzada 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.

XVII. Finalmente, si la prueba informática es traída al proceso sin las debidas garantías de custodia policial y control judicial sobre su identidad e integridad, pudiera lesionar el derecho a un proceso con todas las garantías. No estamos ante una garantía meramente legal, sino ante una que afecta a la validez constitucional de la prueba. Por tanto, la ausencia de control judicial de las evidencias electrónica lesiona y vicia la pertinencia de la prueba

Recibido: marzo de 2021; aceptado: junio de 2021