IUS ET SCIENTIA
2024 • Vol. 10 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2024

La configuración de la cadena de custodia tecnológica en el ordenamiento jurídico español

LEGAL CONSTRUCTION OF THE DIGITAL CHAIN OF CUSTODY IN THE SPANISH SYSTEM

Andrea Jamardo Lorenzo*
Universidad de León
ajaml@unileon.es 0000-0001-5253-3157

Recibido: 14 de octubre de 2024 | Aceptado: 28 de noviembre de 2024

RESUMEN

El presente trabajo constituye una aportación necesaria en torno a la figura de la cadena de custodia tecnológica. A las dificultades propias de la cadena de custodia tradicional, dado lo exiguo de su regulación, se le suman diversas complejidades fruto de su dimensión tecnológica; en tal sentido, se expone cómo se construye y el modo en que se formulan sus vertientes material y formal. Con un enfoque dirigido a la reflexión, concluye con el análisis de la problemática específica que surge en el marco de su vertiente formal y, en particular, de cara a delimitar los diferentes modos de garantizar la corrección de la cadena de custodia tecnológica.

PALABRAS CLAVE

Cadena de custodia tecnológica
Mismidad de la prueba
Vertiente formal

ABSTRACT

In addition to the difficulties inherent to the traditional chain of custody, due to its lack of regulation, there are several other complexities related to its technological dimension. In this sense, this paper explains how the digital chain of custody is constructed, underlining its particularities and how its material and formal aspects are formulated. With an approach focused on reflection, it concludes with an analysis of the specific problems that appear under its formal aspect and, in particular, in order to define the different ways of ensuring the correctness of the digital chain of custody.

KEYWORDS

Digital chain of custody
Sameness of the evidence
Formal aspect

* Profesora Sustituta Doctora. Área de Derecho Procesal de la Universidad de León.

I. Introducción: origen y desarrollo de la figura de la cadena de custodia en el ordenamiento jurídico español

La configuración de la cadena de custodia en el ordenamiento jurídico español se encuentra, con toda probabilidad, en un contexto de tránsito. Aun cuando son diversos los indicios que sostienen la afirmación anterior, debemos poner el acento muy especialmente en la evolución que esta figura ha experimentado a lo largo de los años. Evolución que se inició en la década de los años noventa[1], continuando incansablemente hasta la actualidad y a lo largo de tres etapas diferenciadas, que canalizan la evolución jurisprudencial y la construcción jurídica de esta figura en nuestro ordenamiento jurídico: la primera, concerniente al origen de la cadena de custodia en nuestro ordenamiento jurídico; la segunda, en la que se profundiza en la materia mediante el avance en algunos puntos específicos; y, por último, la tercera y actual etapa, que se constituye con ocasión de la consolidación de los elementos que ahora conocemos como esenciales en materia de cadena de custodia (Jamardo Lorenzo, 2024a, 19 y ss.). Asimismo, debemos destacar que, en el marco de la etapa actual, se producen una serie de hechos que además nos ofrecen una perspectiva de futuro sumamente prometedora. Y es que, si bien en la actualidad todavía no existe en el ordenamiento jurídico español una regulación procesal expresa y unitaria de la cadena de custodia, surgen las primeras muestras de voluntad legislativa en la materia. Me estoy refiriendo, en concreto, a los dos intentos –ahora frustrados– de incorporar en la Ley de Enjuiciamiento Criminal[2] (en adelante LECrim) la tan esperada regulación procesal expresa. Sucedía esto con los Anteproyectos de LECrim (en adelante ALECrim) de 2011 y 2020. Aunque no han aportado todavía el éxito legislativo que merece esta figura, estos dos hitos reflejan una realidad innegable: la cadena de custodia está presente en los intereses legislativos contemporáneos. Volviendo sobre nuestra afirmación inicial, en este contexto de tránsito, nos encontramos, precisamente, a la espera del nacimiento de una nueva etapa, hecho que –naturalmente– se producirá con la aprobación de una regulación expresa y unitaria de la figura de la cadena de custodia (Jamardo Lorenzo, 2024a, 207 y ss.).

No debemos olvidar, volviendo sobre la situación normativa en materia de cadena de custodia, que la doctrina lleva años acusando la ausencia de una regulación procesal de carácter expreso y unitario. Y es que en esta época de cambio también ostenta un papel fundamental la ciencia procesalista[3], al menos a fin de subrayar las preocupaciones e inconvenientes que surgen ante un escenario como el actual y que convenientemente

1. Oportuno es señalar que este camino evolutivo comienza a nivel jurisprudencial y en respuesta a un contexto de ausencia normativa, circunstancia que impulsa directamente un papel excesivamente activo por parte de nuestros tribunales en la construcción jurídica de la cadena de custodia. Aunque ciertamente la tarea de remediar la problemática derivada de la ausencia de regulación corresponde, desde luego, al legislador).

2. Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. *Gaceta de Madrid*, 260, de 17 de septiembre de 1882. https://www.boe.es/buscar/pdf/1882/BOE-A-1882-6036-consolidado.pdf

3. Aunque la incorporación de la doctrina científica al debate se produce generalmente en el contexto de la tercera etapa, no podemos negar los esfuerzos realizados por diversos autores con anterioridad al despunte actual (Moreno Catena y Cortés Domínguez, 2004, 367-377; Guzmán Fluja, 2006, 309 y ss.). Sin embargo, el tratamiento ofrecido entonces comúnmente se localizaba en apartados de

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

ha de ser resulto con prontitud, de cara a suplir la orfandad legal que hoy en día la caracteriza. Con todo, no puede afirmarse una orfandad legal absoluta, por cuanto en nuestra LECrim es posible localizar ciertos preceptos que configuran una regulación indirecta de la cadena de custodia[4]. Es por ello que identificamos esta regulación por su carácter fragmentario –el cual deriva directamente de esta ausencia de regulación expresa y se manifiesta en atención a las diversas referencias indirectas y sectoriales que contiene nuestra LECrim– y heterogéneo –en este caso, emana de la pluralidad de textos normativos que regulan aspectos de la cadena de custodia, haciendo hincapié en que esto se produce no sólo desde el plano legal (donde las referencias son, en efecto, escasas) sino y fundamentalmente desde la perspectiva reglamentaria e institucional[5]–. Lo cierto es que son muchos los instrumentos que integran el marco normativo de la cadena de custodia bajo el prisma reglamentario y muy difícilmente pueden ser reseñados en su totalidad en unas pocas líneas. Se trata de una pluralidad de protocolos, manuales[6] o guías de actuación que constituyen la normativización de la cadena de custodia a través de normas de carácter procedimental[7] que componen –a fin de cuentas– un procedimiento

obras cuyo fin principal era otro. Aunque no por ello debemos obviar su importancia, si bien la complejidad de la temática demanda ahora un tratamiento sólido y profundo de la misma.

4. Sin embargo, su configuración actual en la LECrim no va más allá de una regulación muy indirecta, encontrando solo una referencia expresa, que, por cierto, no arroja claridad alguna sobre la figura analizada. Por otro lado, la diversidad de previsiones indirectas generalmente alude, por un lado, al deber de documentar el modo en que se producen los hallazgos de las fuentes de prueba y el modo en que se practican las diferentes diligencias de investigación; y, por otro lado, al deber de ofrecer a las fuentes de prueba un tratamiento que garantice su integridad o conservación. Estas disposiciones se plasman en la LECrim en modos muy diversos y empleando terminología variada, incorporándose principalmente en artículos relativos al cuerpo del delito, a las diligencias de investigación o a propósito de las actuaciones de la policía judicial, entre otros.

5. Al margen de la esfera legal, la perspectiva reglamentaria e institucional de la cadena de custodia reviste gran importancia. Desde este enfoque se examina normativa de muy diversa naturaleza que, en materia de cadena de custodia, ofrece algunas reglas de actuación a propósito del tratamiento ofrecido a las fuentes de prueba localizadas durante las investigaciones criminales. En particular, son diferentes normas de naturaleza reglamentaria, protocolos de actuación y demás normativa de carácter institucional donde la cadena de custodia, en algunos casos, ha alcanzado una notable presencia y mayor desarrollo que en la esfera legal.

6. Como, por ejemplo, el Manual de Criminalística para la Policía Judicial, editado por la Secretaría General Técnica del Ministerio del Interior en el año 2017, en el que se incorpora una sección dedicada a la cadena de custodia de las muestras o evidencias. En síntesis, recoge ciertas recomendaciones en el modo de actuar, previsiones relativas al correcto empaquetado de las evidencias o a la identificación de todas y cada una de las muestras que conforman unos mínimos que han de cumplirse como medio para garantizar el respeto a la cadena de custodia.

7. En este contexto es fundamental hacer referencia al papel de las directrices que, a propósito de las facultades y competencias investigadoras del Ministerio Fiscal y en conexión con la cadena de custodia, haya emitido la Fiscalía General del Estado en forma de circulares e instrucciones de obligado cumplimiento. Si bien en la actualidad la relevancia de éstas se limita a la unificación de criterios de actuación del propio órgano, no podemos perder de vista el alcance que adquirirían de materializarse el escenario proyectado en algunos textos prelegislativos en los que la dirección de la investigación se otorga al Ministerio Fiscal. Desde un enfoque tecnológico es especialmente destacable la Circular 5/2019, de 6 de marzo, sobre registro de dispositivos y equipos informáticos, donde además se examina la figura examinada en un apartado dedicado al efecto. De conformidad con esta Circular, son dos las condiciones que deben reunir los dispositivos informáticos desde la óptica de la cadena de custodia: las garantías de identidad e integridad –entendiendo identidad como la equivalencia entre el dispositivo incautado y el que posteriormente configura la prueba y, por otro lado,

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

de manipulación de las evidencias afectante a su condición práctica y técnica. Al hilo de lo anterior, sostiene la doctrina que justamente son las ciencias forenses las que mayor influencia tienen sobre «el desarrollo normativo sectorial de las técnicas de recogida, custodia y análisis» (Gutiérrez Sanz, 2016, 43), lo que –añado– implica el enfoque material de esta figura procesal.

En este escenario de insuficiencia normativa, además, surge una dificultad añadida a consecuencia del auge de las nuevas tecnologías. Y es que el contexto tecnológico nos pone en jaque ante situaciones menos comunes y más desconocidas. Justamente, el objetivo central de este trabajo es examinar la configuración de la cadena de custodia tecnológica, sin embargo, es imprescindible delimitar (como paso previo al abordaje de la cadena de custodia desde su vertiente tecnológica) la base dogmática de la cadena de custodia *per se*, esto es, en su vertiente más tradicional, para abordar el estudio de la problemática específica de la cadena de custodia tecnológica. De este modo, oportuno es exponer la noción de cadena de custodia sobre la que se desarrollará el presente trabajo. En tal sentido, entendemos la cadena de custodia como una garantía del derecho a la prueba que, desde su vertiente formal, constituye la garantía de la mismidad de la prueba, cuya acreditación se alcanza mediante la corrección de la cadena de custodia; y desde su vertiente material, constituye el conjunto de actos que se inician con la obtención de la fuente de prueba material y finalizan con su introducción en el juicio oral a través del medio de prueba oportuno (Jamardo Lorenzo, 2024b, 331-332).

II. La construcción de la cadena de custodia tecnológica en nuestro ordenamiento jurídico

2.1. La configuración de las vertientes formal y material de la cadena de custodia tecnológica

Se ha dicho anteriormente que la cadena de custodia está integrada por dos vertientes: por un lado, la vertiente formal –o procesal–; y, por otro, la material.

El reconocimiento de la cadena de custodia como garantía inherente a la prueba (y, en particular, como garantía de la mismidad) le confiere un estatus decisivo en pro de la verosimilitud de la prueba y, por tanto, determinante en su valoración. Es por ello que la vertiente formal de la cadena de custodia la integran los siguientes elementos: la mismidad de la prueba; los escenarios procesales emergentes (por un lado, la llamada corrección de la cadena de custodia; por otro, la presencia de eventuales contingencias en su desarrollo) y sus consecuencias jurídicas; la impugnación de la cadena de custodia; y la valoración de la prueba. En virtud de la configuración de la vertiente formal de la cadena de custodia, ocurre que los elementos que la conforman son invariables e inmutables, en tanto que son únicos para todas las fuentes de prueba. Esto se produce debido a que estos elementos se identifican con aquellos escenarios procesales que

integridad como la ausencia de alteraciones en los datos que conforman el contenido dispositivo–. A propósito de lo anterior, la circular ofrece algunas soluciones para acreditar las garantías de identidad e integridad de las fuentes de prueba.

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

se desprenden, en efecto, de la naturaleza procesal de la cadena de custodia como figura autónoma. En virtud de lo anterior, la vertiente formal se materializa como una vertiente estática.

En el marco de la vertiente formal, es preciso exponer qué entendemos por *mismidad de la* prueba, por un lado, y por *corrección de la cadena de* custodia, por otro. El primer de ello –la mismidad de la prueba– es un término asentado y consolidado por el Tribunal Supremo (en adelante TS) y que hace referencia a la garantía de la incolumidad de la prueba, esto es, la garantía de que la prueba no ha sufrido daños ni alteraciones, que se mantiene incólume desde su obtención, lo que se traduce en que la prueba es lo *mismo* desde su obtención y hasta su posterior análisis e introducción en juicio. La constante de ser lo mismo es, precisamente, lo que jurisprudencialmente se ha venido denominando como mismidad de la prueba[8]. Hoy en día, la mismidad de la prueba ha alcanzado una extraordinaria significación en materia de cadena de custodia, al ser el eje central de su planteamiento en el plano jurisprudencial. De ahí que el concepto aportado en este trabajo proyecte la cadena de custodia como la garantía de la mismidad de la prueba[9]. Ahora bien, la mismidad de la prueba no puede entenderse si no en torno a un significado jurídico y, en particular, vinculado con la finalidad de la cadena de custodia. Por ende, si partimos de la premisa de que la cadena de custodia busca acreditar la equivalencia procesal entre las fuentes de prueba material obtenidas en la investigación criminal y los medios de prueba aportados al juicio oral en su virtud, es preciso matizar que analizamos esta equivalencia exclusivamente a efectos procesales. Esto se traduce en que resulta indiferente si el concreto objeto que va a ser introducido al juicio oral a través del oportuno medio de prueba ha mutado a lo largo del proceso (ya sea su aspecto, su peso, el estado en el que se encontraba, etc.), siempre que se haya garantizado que –a pesar de las modificaciones o alteraciones sufridas por el devenir de las actuaciones procesales pertinentes– el medio de prueba se corresponde con la fuente obtenida durante la investigación criminal[10]. Dicho de otro modo, la fuente de prueba no debe forzosamente mantenerse invariable e idéntica en el tiempo, pues ésta no es la finalidad de la actividad probatoria, en términos generales, ni de la cadena de custodia, en particular. En suma, es irrelevante que la fuente de prueba haya sufrido alteraciones materiales por causa de las actuaciones procesales a las que haya sido sometida, cuando su mismidad ha quedado acreditada a través de la corrección de la

8. En virtud de la Sentencia del Tribunal Supremo (STS) núm. 1119/2009, Sala de lo Penal, de 3 de diciembre, ECLI:ES:TS:2009:7710; entre otras, el TS alude a la mismidad en los siguientes términos:

> En relación a la cadena de custodia el problema que plantea (…) es 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 sobre lo que recaerá la inmediación, publicidad y contradicción de las partes y el juicio de los juzgadores es lo mismo. Es a través de la cadena de custodia como se satisface la garantía de la 'mismidad' de la prueba.

9. Sorprende el hecho, no obstante, de que la doctrina científica haya obviado en numerosas ocasiones la especial trascendencia del término mismidad. Ahora bien, ello no implica que los procesalistas españoles hayan ignorado las cuestiones inherentes a esta mismidad, sino que han acudido a éstas a través de otros términos asociados (autenticidad, identidad, integridad, inalterabilidad, indemnidad, inmutabilidad o incolumidad acostumbran a ser los más comunes).

10. El ejemplo más evidente es la muestra de droga que varía su pesaje tras el correspondiente análisis pericial sobre la misma.

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

cadena de custodia[11]. Implica, en consecuencia, la contraposición entre la mismidad material y la mismidad formal de la prueba.

Por lo que se refiere, en segundo lugar, a la expresión corrección de la cadena de custodia, como su propia literalidad indica, hace referencia al correcto desarrollo de la cadena de custodia[12]. A nivel jurídico significa que no ha habido problemas procesales en su desarrollo y, por tanto, se ha garantizado la mismidad de la prueba. La apreciación de este escenario procesal implica, en suma, que la prueba ha alcanzado un grado de fiabilidad adecuado que tendrá su reflejo en sede de valoración. Éste es el escenario procesal idílico, al menos, desde el punto de vista de la Administración de Justicia, pues implica que la investigación ha transcurrido con normalidad. Hay que destacar que, basándonos en la presunción *iuris tantum* de veracidad que afecta a la cadena de custodia, oportuno es destacar que acreditar su corrección es, en principio, innecesario para las partes procesales (Álvarez de Neyra Kappler, 2015, 83). De modo que la dificultad se encuentra en acreditar, en su caso, la ruptura de la cadena de custodia como método para cuestionar la fiabilidad de la prueba y, en consecuencia, afectar a su valoración. Distinto escenario se produce ante la impugnación de la misma, sobre motivos fundados, pues ante esta situación sí resulta conveniente –para la parte interesada– concentrar sus esfuerzos en acreditar su corrección. En definitiva, el cumplimiento de la corrección de la cadena de custodia implica la acreditación de la mismidad de la prueba, esto es, la identidad procesal entre fuente y medio de prueba (que, en efecto, se traduce en la ausencia de alteraciones –o justificación de las mismas– en la prueba analizada, en línea con lo expuesto en las líneas precedentes).

11. A pesar de lo dicho en texto, en este punto se manifiesta un escenario doctrinal algo confuso en el que parte de la doctrina ha recibido el concepto jurisprudencial de mismidad adoptando una idea lo suficientemente literal como para generar fisuras en el término a nivel procesal. Al respecto de lo anterior, algunos autores (García Mateos, 2016, 131 y ss.) rechazan la tesis de que la cadena de custodia garantiza la mismidad de la prueba o, en palabras del autor, «el principio de mismidad», en base a la idea de que la mismidad de la prueba quiebra automáticamente cuando la evidencia se altera, con independencia del tipo de alteración sufrida, incluso tratándose de una modificación derivada del análisis pericial y perfectamente documentada.

12. Nuevamente se observa como punto negativo la ausencia de normativa expresa, en este caso, que regule las exigencias mínimas que ha de cumplir la corrección de la cadena de custodia. A pesar de no ser preceptiva la verificación de este escenario, es fundamental concretar estas condiciones de cara a ofrecer un escenario procesal que cumpla con unos estándares mínimos de seguridad jurídica. Tarea que ya ha sido afrontada tanto por la doctrina como por la jurisprudencia, habiendo construido todo un «*corpus* jurídico» que sintetiza todas aquellas cuestiones procedimentales y que, en palabras de Gutiérrez Sanz «es asumido como *cuasi* vinculante por la comunidad jurídica», de modo que los diversos operadores jurídicos que entran en contacto con la cadena de custodia tienden a respetarlo (Gutiérrez Sanz, 2016, 61 y ss.). Ahora bien, la normativa a la que alude la autora hace referencia esencialmente a la vertiente material de la cadena de custodia y aunque no podemos negar –y de hecho no lo negamos– el valor de la vertiente material (entendiendo que la adecuada sucesión de los actos integrantes de la perspectiva material ofrece una alta seguridad en la dimensión procesal y, en concreto, en el alcance de la corrección de la cadena de custodia), sin embargo, entiendo que la vertiente material no debe condicionar en extremo la prosperidad de la vertiente formal (esto es, de la corrección de la cadena de custodia), por lo que es preciso que este tipo de normativa formule unas condiciones mínimas que se orienten a la vertiente formal –quedando la regulación específica de la vertiente formal pendiente de ser desarrollada en la legislación procesal–.

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

Al contrario de lo que ocurre con la vertiente formal de la cadena de custodia, su vertiente material es dinámica. Este dinamismo emana de la amplitud de posibilidades en cuanto a fuentes de prueba se refiere y ello a consecuencia de su naturaleza extrajurídica. De ahí que los actos que integran la vertiente material puedan sufrir variaciones o, incluso, surgir actos diferenciados en función de la concreta fuente de prueba objeto de análisis. Es por ello que, en este punto, nos referiremos a los actos generales que integran esta vertiente material y no a los actos específicos de cada fuente de prueba concreta (que, no obstante, podrán ser encuadrados en alguno de los actos generales). En concreto, esto actos generales e integrantes de la vertiente material de la cadena de custodia son los siguientes: primero, el hallazgo y obtención de las evidencias; segundo, el aseguramiento y la conservación de la fuente de prueba; tercero, el análisis –en su caso– de las muestras; y cuarto, la incorporación de la prueba al juicio oral mediante el oportuno medio probatorio[13].

Siguiendo el esquema anterior, el primer acto material de la cadena de custodia –hallazgo y obtención de las evidencias– alude a la localización y obtención de las fuentes de prueba de carácter material y, en este caso, tecnológicas que, en un futuro, podrán ser incorporadas al proceso como medio de prueba. Obtenida la fuente de prueba material, se inicia la cadena de custodia y, en consecuencia, deben respetarse las actuaciones necesarias para garantizar el aseguramiento de las pruebas materiales. Es importante señalar que, una vez iniciada la cadena de custodia, también se inicia el deber de documentarla.

Obtenidas las evidencias, la segunda fase de la cadena de custodia hace referencia, ya específicamente, al aseguramiento y conservación de la fuente de prueba material tecnológica, esto es, se refiere a los actos de vigilancia y cuidado de las muestras, desde el momento de su recogida, transporte, pasando por un posible análisis científico de las evidencias, y hasta que se pongan a disposición judicial. Del mismo modo que ocurría en el anterior acto, el deber de documentar la cadena de custodia debe mantenerse también en este punto. La fuente de prueba habrá de ser asegurada y conservada en las condiciones que exija su propia naturaleza para evitar posibles alteraciones indeseadas; que, en el caso de la prueba tecnológica, las posibilidades se incrementan notablemente, pues no debemos olvidar que el objeto de la conservación hace alusión a los datos que pueda contener los dispositivos informáticos –pues éstos serán el objeto de la cadena de custodia en su vertiente tecnológica–.

En caso de que la fuente de prueba deba pasar un examen pericial (lo cual ocurre con frecuencia en el supuesto de cadena de custodia tecnológica, en relación, en concreto, con el informe pericial informático), se inicia el tercer acto: el análisis de las muestras obtenidas. En este punto se produce la recepción por parte de los expertos que van a

13. No obstante, ésta no es la única estructuración de la vertiente material, sino que son numerosos los autores que han ofrecido un enfoque propio (donde, a pesar de mantener una esencia similar, los concretos actos señalados no son coincidentes). Por un lado, algunos ejemplos ofrecen actos excesivamente específicos –aludiendo a cuestiones tales como el embalaje, el transporte, o el almacenaje final de las muestras– y que inciden en aspectos relacionados específicamente con el modo de actuación de los custodios (del Pozo Pérez, 2014; García de Yébenes y Gascó Alberchi, 2015, 130; Campos, 2002); por otro lado, otras posturas ilustran actos con un carácter menos procedimental y más procesal (Gutiérrez Sanz, 2016, 61 y ss.).

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

proceder al análisis de las mismas. Se exige que lo primero que se debe evaluar y documentar por parte de los expertos sea el estado en que se reciben las muestras (así como el aspecto del embalaje), debiendo reflejarlo detalladamente en el documento de recepción. Asimismo, tendrán que ser identificadas las personas que entrarán en contacto con las muestras. Una vez finalizados los análisis de las muestras, es necesario documentar su estado final, señalando los cambios que se hayan producido, en su caso, y justificándolos. En este punto, los procedimientos estarán excesivamente diferenciados en función de las concretas fuentes de prueba que acceden a los análisis, puesto que no será lo mismo efectuar un análisis sobre muestras de ADN[14] que un análisis sobre sustancias estupefacientes –e, incluso aquí, se pueden localizar distinciones en función del tipo de sustancia de que se trate–.

El último acto de la vertiente material es la incorporación de la prueba al juicio oral en virtud del oportuno medio probatorio (art. 299 de la Ley de Enjuiciamiento Civil[15]). Ello teniendo en cuenta que, para acceder a la fase de juicio oral deberá cumplir con los criterios de admisibilidad: licitud, pertinencia y utilidad y, aunque la cadena de custodia no se valora en admisión, las partes podrán alegar irregularidades en la misma en ese momento. En este punto, es importante recordar que el acceso de la prueba tecnológica al proceso encuentra mayores trabas –a casusa de los caracteres que le son propios–, debiendo superar ésta el denominado «test de admisibilidad» en relación con la acreditación de su autenticidad e integridad, así como de su licitud (Martín Ríos, 2020). En definitiva, la admisión de la prueba supone el final del trayecto de la fuente de prueba en su vertiente material y, por ende, la cadena de custodia concluye con este acto. A partir de este momento, es la autoridad judicial la encargada de custodiar la fuente de prueba hasta su valoración en sentencia.

2.2. Especificidades que conforman la problemática habida en la cadena de custodia tecnológica

2.2.1. En relación con la investigación tecnológica en el proceso penal

Plantear la temática de la investigación tecnológica en nuestro ordenamiento jurídico fuerza la necesidad de mencionar la Ley Orgánica (en adelante LO) 13/2015[16], de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica como

14. En este contexto las recomendaciones del GHEP-ISFG (grupo de habla española y portuguesa de la sociedad internacional de genética forense) sobre la localización, hallazgo y recogida de muestras de ADN son de carácter muy específico y vinculado a este tipo de muestras en exclusiva: por ejemplo, medidas de carácter higiénico sanitarias con dos objetivos: evitar la contaminación tanto del personal, como también de la propia muestra (López Valera, 2016, 799-801).

15. Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. *Boletín Oficial del Estado*, 7, de 8 de enero de 2000. https://www.boe.es/buscar/pdf/2000/BOE-A-2000-323-consolidado.pdf

16. Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. *Boletín Oficial del Estado*, 239, de 6 de octubre de 2015, pp. 90192-90219. https://www.boe.es/boe/dias/2015/10/06/pdfs/BOE-A-2015-10725.pdf

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

punto de referencia. La promulgación de la citada LO a finales del año 2015, situó España a la «vanguardia legislativa» (Bueno de Mata, 2019, 17). Hasta aquel entonces, nuestro ordenamiento jurídico destacaba por la insuficiencia normativa en materia de investigación tecnológica (Fuentes Soriano, 2016, 261-262), contando únicamente con un precepto al respecto en toda la LECrim. Sin embargo, como paso previo, la firma del Convenio de Budapest[17] por España supuso un primer hito en materia de investigación y obtención de prueba tecnológica en nuestro país. Uno de los grandes objetivos del Convenio era, en efecto, la implementación de una serie de medidas procesales de cara a avanzar en la lucha contra la ciberdelincuencia y, en particular, en relación con la investigación y la prueba tecnológica (Ortiz Padrillo, 2013, 76-80; Cuadrado Salinas, 2020, 519 y ss.). Siendo tal la conexión entre ambos instrumentos que, precisamente, el propio preámbulo de la LO 13/2015 apela al Convenio como referente en la implementación de la orden de conservación de datos como medida de aseguramiento, en aras a garantizar la preservación de los datos e informaciones que se contengan en un dispositivo electrónico, lo que nos evoca directamente al fin en sí mismo de la cadena de custodia tecnológica. En conexión con la temática que aquí nos ocupa, es importante señalar que la mejora del marco normativo en materia de investigación tecnológica también provocó cierta repercusión en materia de cadena de custodia tecnológica (Richard González, 2017).

Con todo, el impacto que la regulación concreta de la investigación tecnológica generó en materia de cadena de custodia se circunscribe también al respeto de los principios rectores de la investigación tecnológica. Estos principios se introducen en nuestro ordenamiento procesal con ocasión de la mencionada LO 13/2015, y, en concreto, son los siguientes: especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad (art. 588 bis a LECrim)[18]. En primer lugar, la LECrim establece el principio de especialidad (art. 588 bis a 2 LECrim) con arreglo a un aspecto positivo (en virtud del cual se exige que la medida se encuentre relacionada con la investigación de un delito concreto) y uno negativo (que implica, en cambio, la imposibilidad de autorizar medidas de investigación tecnológica tendentes a la prevención o el descubrimiento de delitos). Dicho de otro modo, prohíbe las investigaciones de carácter prospectivo. En segundo lugar, el principio de idoneidad, de acuerdo con el art. 588 bis a 3 LECrim, sirve para delimitar los ámbitos objetivo y subjetivo y la duración de la medida por razón de su utilidad[19]. En tercer lugar, en cuanto a los principios de excepcionalidad y necesidad el legislador los

17. Convenio del Consejo de Europa sobre el Cibercrimen firmado en Budapest el 23 de noviembre de 2001 y ratificado en por España en el año 2010.

18. Aunque la vigencia de estos principios en nuestra LECrim se remonta al año 2015, es justo señalar que, en la práctica, ya se venían aplicando por la jurisprudencia desde algunos años atrás, en aquellos supuestos en los que las medidas a adoptar limitaban los DDFF de las personas (Garcimartín Montero, 2018, 29; Roca Martínez, 2020, 710 y ss.).

19. Distintos autores han reconocido la utilidad de la medida como elemento identificador del principio de idoneidad (Sánchez Melgar, 2016, 20 y ss.; Garcimartín Montero, 2018, 34-35; Delgado Martín, 2018, 371). Este último afirma que la razón de ser del principio de idoneidad estriba en la existencia de una «relación de adecuación entre la concreta medida de investigación y el fin perseguido», de modo que, expresa el autor, esto se traduce en que la medida ha de servir a fin de «conseguir datos útiles para investigar las circunstancias del delito». Y añade que, en virtud del art. 588 bis c 3, la resolución judicial que autoriza la medida debe concretar la finalidad perseguida con la misma. También (Vegas Torres, 2017, 22 y ss.).

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

reúne en el mismo precepto, el art. 588 bis a 4, en virtud del cual la media únicamente podrá adoptarse cuando no exista la posibilidad de adoptar medidas menos gravosas (apartado a, art. 588 bis a 4 LECrim) o cuando el fin perseguido por la medida no pueda alcanzarse mediante la adopción de otra medida distinta (apartado b, art. 588 bis a 4 LECrim)[20]. Finalmente, el principio de proporcionalidad se regula en el art. 588 bis a 5 LECrim y se cumple cuando la injerencia en derechos fundamentales (en adelante DDFF) es menor que el beneficio que aporta la medida al proceso penal. De cara a valorar si se cumple o no el principio de proporcionalidad se habrán de examinar los siguientes aspectos: primero, la gravedad del hecho; segundo, la trascendencia social; tercero, el ámbito tecnológico de producción; cuarto, la intensidad de los indicios existentes; y, finalmente, la relevancia del resultado perseguido con la restricción del derecho (Bueno de Mata, 2019, 37-38)[21]. En definitiva, se trata de ponderar una vez más el respeto a los DDFF del investigado frente al correcto desarrollo de la investigación, todo ello desde la perspectiva de menor lesividad a los derechos del encausado.

Todo lo anterior hace referencia a especificidades que condicionan el desarrollo de la vertiente material de la cadena de custodia tecnológica, en tanto que implica que las investigaciones en estos casos han de desarrollarse con especial atención a los principios señalados anteriormente.

2.2.2. En relación con la protección de derechos fundamentales

Quizá uno de los principales retos de la digitalización de la justicia es mantener la salvaguarda de los DDFF y principios del proceso, máxime teniendo en cuenta el uso generalizado de los medios informáticos y tecnológicos en el ámbito de la vida privada, por lo que suele ocurrir que el contenido de estos dispositivos se vincule directamente con los DDFF de las personas. Ésa es la razón por la que la protección de ciertos DDFF cobra una relevancia significativa en materia de cadena de custodia tecnológica. Ahora bien, es importante distinguir entre aquellos DDFF que guardan relación con la configuración de la cadena de custodia en sí misma (y, por tanto, mantienen una vinculación más directa); respecto de aquellos que adquieren una posición sensiblemente más vulnerable en el contexto de la cadena de custodia tecnológica. Estos últimos son el derecho a la protección de datos personales del art. 18.4 de la Constitución Española[22] (en adelante

20. Al respecto de lo anterior existen dos modos de comprender los principios de excepcionalidad y necesidad. Algunos autores sostienen que el principio de excepcionalidad se recoge en el apartado a) del art. 588 bis a 4 LECrim y el de necesidad en el apartado b) del mismo precepto (Espín López, 2021a, 44 y ss.); en cambio, la otra vertiente doctrinal defiende la unificación de ambos principios en uno (Garcimartín Montero, 2018, 36; Delgado Martín, 2018, 371), entendiendo el principio de excepcionalidad como un principio de subsidiariedad (Espín López, 2021a, 45). En el caso de los autores que unifican ambos principios, sin embargo, la equivalencia se produce también respecto del principio de necesidad. De ahí que autores como Delgado Martín aludan a este principio en virtud del principio de subsidiariedad (Delgado Martín, 2018, 371). De modo similar, Bueno de Mata sostiene que ambos principios han de ser interpretados de manera complementaria (Bueno de Mata, 2019, 36).

21. Además, como expone el autor, estos principios se encuentran desarrollados por parte de la Fiscalía General del Estado en su Circular 1/2019.

22. Constitución Española. *Boletín Oficial del Estado,* 311, de 29 de diciembre de 1978. https://www.boe.es/buscar/pdf/1978/BOE-A-1978-31229-consolidado.pdf

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

CE); el derecho a la intimidad personal del art. 18.1 CE; y el derecho al secreto de las comunicaciones del art. 18.2 CE (Mestre Delgado, 2015, 50). Sin embargo, la especial trascendencia de estos DDFF en materia de cadena de custodia tecnológica se vincula con su vertiente material y, en particular, en relación con la posibilidad de vulnerarlos durante la práctica de las distintas diligencias de investigación, lo que implicaría la exclusión de la prueba por vulneración de DDFF (por lo que el examen de la corrección de la cadena de custodia pasaría a ser irrelevante al producirse una prueba prohibida).

En relación con el derecho fundamental a la protección de datos personales[23], en primer lugar, lo fundamental reside en el reconocimiento al interesado de un régimen de control y disposición sobre sus datos personales (Velasco Núñez, 2020), en virtud de los derechos de acceso, rectificación, supresión y limitación del tratamiento, así como la previsión de los principios rectores en la materia y fijando el consentimiento del interesado como fundamento esencial para el tratamiento de sus datos (Colomer Hernández, 2023, 40 y ss.; Pérez Gil, 2019, 431). Por tanto, teniendo en cuenta que parte de la problemática habida en la cadena de custodia tecnológica reside en la conservación de los datos digitales, el respeto a este derecho es fundamental. Conviene destacar, asimismo, que su consideración como derecho autónomo deriva de la configuración jurisprudencial efectuada por el Tribunal Constitucional (en adelante TC) con ocasión de la Sentencia del TC (en adelante STC) núm. 292/2000, de 30 de noviembre; debiendo señalar, además, que el derecho a la protección de datos personales adquiere una cobertura más amplia que el derecho a la intimidad, ya que su protección se extiende a cualquier dato personal de carácter personal y no necesariamente íntimo.

En segundo lugar, tampoco cabe duda de que la proliferación de las nuevas tecnologías pone en riesgo la protección de los DDFF a la intimidad y al secreto a las comunicaciones. Por un lado, la facultad otorgada por el derecho a la intimidad[24], consiste en esencia en impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad perseguida por quien la capta o difunde. Por su parte, el contenido del derecho fundamental al secreto de las comunicaciones[25] ha sido desarrollado por el TC ha desarrollado, estableciendo que su protección se extiende a la interceptación de las comunicación ajenas, bien en sentido estricto (aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o captación del proceso de comunicación), bien por el conocimiento

23. En los últimos años, se han ido produciendo diversos avances legislativos en materia de protección de datos, tanto en el seno de la Unión Europea como a nivel interno, con la clara finalidad de atajar los riesgos derivados del aumento de la circulación transfronteriza de los datos personales de los ciudadanos. Con carácter general, el derecho a la protección de datos personales se recoge a nivel nacional en el art. 18.4 CE, asimismo, la LO 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales, personifica la normativa clave en la materia y establece los principios básicos para el tratamiento de los datos personales: siendo estos los de lealtad y la limitación de su acceso, fijando el consentimiento del interesado como fundamento esencial para el tratamiento de los datos.

24. El derecho a la intimidad está reconocido en el art. 18.1 CE y, asimismo, en el art. 8 del Convenio Europeo de Derechos Humanos (CEDH). Además, el contenido del mismo ha sido desarrollado por el TC en las STC 81/2001, de 26 de marzo. BOE 104, de 1 de mayo 2001, en relación con la STC 231/1988, de 2 de diciembre. BOE núm. 307, de 23 de diciembre de 1988.

25. Art. 18.3 CE y 8 CEDH, entre otros textos de protección internacional.

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario o de un mensaje emitido por correo electrónico o a través de telefonía móvil, por ejemplo). Hay que destacar que el concepto de secreto de la comunicación cubre no sólo el contenido de la comunicación, sino también otros aspectos de la misma, como la identidad subjetiva de los interlocutores[26]. En definitiva, se trata de la protección de las comunicaciones en su más amplio sentido. Tampoco cabe duda de que, en virtud del contenido de ambos derechos, la afectación de los mismos resulta más plausible en las investigaciones penales tras el auge de la prueba tecnológica. En materia de cadena de custodia, suponen –además– un riesgo a mayores, dado que los actos que integran la vertiente material de la cadena de custodia pueden incidir en el contenido de estos derechos cuando la prueba en cuestión sea tecnológica y no se sigan de forma adecuada los protocolos de actuación a fin de evitar posibles injerencias en DDFF.

III. El alcance de la vertiente formal de la cadena de custodia tecnológica

Tomando como base la división en las dos vertientes –formal y material– aludidas en puntos anteriores, resulta esencial examinar en mayor profundidad la vertiente formal de la cadena de custodia tecnológica en torno a la reflexión que suscita su tecnologización. En particular, son tres los aspectos esenciales a valorar en materia de cadena de custodia tecnológica: en primer lugar, la corrección de la cadena de custodia tecnológica como método de acreditación de la mismidad de la prueba; en segundo lugar, la impugnación de la cadena de custodia tecnológica; y, en tercer lugar, la fiabilidad de la prueba tecnológica en virtud de su cadena de custodia.

3.1. La corrección de la cadena de custodia tecnológica

3.1.1. ¿Cómo acreditar la mismidad de la prueba tecnológica?

En los últimos años y con relativa frecuencia, la doctrina procesalista ha ido exponiendo la idea de que la cadena de custodia alcanza una importancia sin precedentes en el contexto tecnológico. Partiendo de la veracidad de tal afirmación, me parece conveniente realizar una leve matización. Esta relevancia que adquiere la cadena de custodia tecnológica atiende, muy particularmente, a la desconfianza que genera la prueba tecnológica en los distintos operadores jurídicos. De cara a afianzar la más reciente aseveración, es imperativo iniciar la reflexión sobre la base del fin inherente a la cadena de custodia. Finalidad que ha sido expresada desde los inicios de este trabajo y que no es otra que la de garantizar la mismidad de la prueba material. Tomando como base lo anterior, la desconfianza a la que hacíamos referencia previamente afecta directamente a la fiabilidad de la prueba tecnológica y deriva de los caracteres propios de ésta –ante

26. STC 142/2012, de 2 de julio. BOE núm. 181, de 30 de julio de 2012, en relación con la STC 230/2007, de 5 de noviembre. BOE núm. 295, de 10 de diciembre de 2007.

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

todo, en virtud de su carácter volátil y su presunta fácil manipulación[27]–. La reiteración de estos caracteres hizo que saltasen todas las alarmas e impulsó una preocupación generalizada en la doctrina acerca de cómo se habrá de acreditar la autenticidad de una fuente de prueba tecnológica[28]. Pero, además, esta confianza continúa en detrimento con la aparición de las tecnologías disruptivas. Este nuevo contexto tecnológico exhibe problemáticas que van más allá de la mera facilidad de manipulación y que reflejan ahora la posibilidad de creación *ad hoc* de pruebas que, aunque falsas, lucen auténticas[29]. Volviendo sobre la idea reflejada líneas arriba, la desconfianza en la prueba tecnológica se traduce en una baja graduación de su fiabilidad. Pero lo cierto es que esta desventaja emana de un aspecto lógico: la fuente de prueba tecnológica contiene ciertos datos (datos que pretenden ser valorados como prueba) que, comúnmente, se han incorporado al dispositivo tecnológico de forma previa a su localización durante la investigación criminal[30]. Por ello las posibilidades de alteración o creación *ad hoc* de las pruebas se perciben mayores. Es oportuno señalar que también en el contexto tecnológico nos encontramos ante un escenario de vacío legal en materia de cadena de custodia. Hecho éste ciertamente coherente con el estado actual de su regulación procesal, pues no existiendo tal regulación de la cadena de custodia *per se*, una regulación de su vertiente tecnológica luciría incongruente[31]. Y ésta es, sin duda, la visión que se defiende en este trabajo: es fundamental regular la cadena de custodia tradicional,

27. Al efecto, muy acertadamente expone Ariza Colmenarejo que, en el ámbito informático, «la modificabilidad hace de los documentos digitales una fuente de prueba susceptible de ser impugnada» (González Granda y Ariza Colmenarejo, 2021, 484 y ss.). Y es que justamente, ante esa falta de confianza, en la práctica la impugnación de los documentos digitales es un arma muy utilizada. Por otro lado, diversos autores han destacado las cautelas que habrán de ser tomadas antes de confiar en la exactitud de una prueba de carácter tecnológico (Sánchez Rubio, 2019, 289), entre otros.

28. Precisamente ésta es la verdadera consecuencia de la ausencia de confianza, si bien es importante tener en cuenta en este punto, tal y como afirma Arrabal Patero, que, a pesar de que reiteradamente se ha resaltado la posibilidad de alteración de las pruebas de carácter tecnológico, lo cierto es que esta circunstancia también ocurre en las pruebas más tradicionales (Arrabal Platero, 2020, 45).

29. Esta circunstancia se concreta muy en particular respecto de la posibilidad de valerse de una inteligencia artificial (IA) que genera imágenes, vídeos, sonidos… que emulan al original y que son de muy difícil o imposible diferenciación. Son hechos que ya hemos visto en la realidad: IAs que imitan las voces de los famosos, que modifican imágenes reales transformándolas por completo o crean imágenes desde cero a partir de una descripción, etc. Las posibilidades son infinitas y la utilización de este tipo de herramientas se vuelve cada vez más accesible y cómoda para el usuario, lo cual acrecienta exponencialmente la peligrosidad de estas herramientas de cara a una incorrecta aplicación. Ahora bien, la creación de imágenes falsas no es una novedad que haya introducido la IA, no obstante, la sencillez que ofrece la IA a la hora de manipular imágenes o vídeos es abrumadora.

30. Diferencia fundamental con respecto a, por ejemplo, los análisis periciales efectuados por organismos oficiales.

31. Sin perjuicio de lo expresado en texto, no se puede obviar la sorpresa causada por la ausencia de previsiones al respecto tras la reforma operada por la LO 13/2015, mucho más teniendo en cuenta que el propio legislador manifestó entonces la facilidad de alteración que podría sufrir la prueba tecnológica. A pesar de ello, el legislador optó por incorporar únicamente vagas referencias a la necesidad de adoptar las garantías para asegurar la integridad de las fuentes de prueba obtenidas tras la práctica de algunas y concretas medidas de investigación (Espín López, 2021b). En el ámbito de la UE, por otro lado, tiene especial consideración el Reglamento 2023/1543, relativo a las órdenes europeas de producción y conservación de prueba electrónica en los procesos penales, si bien tampoco aporta novedades relevantes en materia de cadena de custodia.

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

como garantía procesal, para después abordar la problemática específica de la cadena de custodia tecnológica.

En relación con la acreditación de la mismidad de la prueba tecnológica y una vez planteadas las diferentes problemáticas, se ha iniciado una búsqueda constante de nuevas formas de garantizar la mismidad de la prueba en el terreno tecnológico[32]. Aunque acreditar la corrección de la cadena de custodia de una prueba de carácter tecnológico puede efectuarse –al igual que ocurre cuando se trata de una prueba más tradicional[33]– por diferentes vías. Por ejemplo, ciertas propuestas doctrinales consideran que una forma de garantizar la mismidad de la fuente de prueba tecnológica consiste en que la obtención o el acceso a la fuente de prueba se efectúe en presencia de un fedatario público –ya se sea un notario o ante el Letrado de la Administración de Justicia–, de modo que el fedatario sea quien garantice el contenido de dicha fuente de prueba electrónica, dando fe del contenido de la misma[34]. Si bien la posición más compartida sostiene que la pericial informática[35] es el mejor modo de acreditar la mismidad de una prueba tecnológica. Para ello, un perito informático deberá analizar el dispositivo tecnológico a fin de comprobar que su contenido no haya sido adulterado.

3.3.2. Mención especial al uso de tecnología blockchain como método para garantizar la corrección de la cadena de custodia

En el terreno de las tecnologías disruptivas[36], no obstante, existen otras opciones que están alcanzando mucha fuerza como métodos para garantizar la cadena de custodia

32. Autores como Arellano y Castañeda (Arellano y Castañeda, 2012, 67-81) exponen un modo de proceder bastante detallado para la preservación de la cadena de custodia digital, siguiendo las fases de detección, identificación y registro, recolección de los elementos y recolección de la evidencia digital.

33. En síntesis, la diferencia fundamental es que la confianza que depositamos en una y en otra, y tratándose la cadena de custodia de una garantía que impacta directamente en la fiabilidad que el juzgador otorga a la prueba en fase de valoración, ciertamente la cadena de custodia adquiere una relevancia sin precedentes en el plano digital, ello porque partimos de un grado de desconfianza mayor en la fuente de prueba aportada.

34. Es conveniente recordar que existe unanimidad doctrinal al respecto de que lo verdaderamente determinante es el contenido/información y no el dispositivo en sí mismo. En este caso concreto, se habla de la presencia de fedatarios públicos en el «primer momento del acceso al contenido de la prueba», en tanto que «podrían presenciar el momento del acceso, bloqueo y clonado» (Calaza López y Muinelo Cobo, 2020, 473 y ss.).

35. Arrabal Platero expone los beneficios de acudir a este tipo de medios, afirmando la utilidad de la pericia para el caso de que se requiera un análisis sobre los metadatos de la prueba tecnológica que se ha accedido al proceso, ello lo expone en referencia a los modos de introducir la información contenida en un dispositivo tecnológico, sin embargo, tales afirmaciones son trasladables al ámbito de la cadena de custodia (Arrabal Platero, 2021, 536); Calaza López sostiene que la pericial informática puede servir para acreditar la autenticidad e integridad de la prueba electrónica (Calaza López, 2022, 39 y ss.). En el mismo sentido: (Sanjurjo Ríos, 2020, 206; Martínez Galindo, 2022, 15 y ss.); también Fuentes Soriano, en relación con la forma de acreditar la autenticidad de un correo electrónico (Fuentes Soriano, 2017, 202 y ss.) o Rubio Alamillo, quien alude a la importancia de que el perito firmante sea informático (Rubio Alamillo, 2018). Aunque no en relación con la acreditación de la mismidad en concreto, de Urbano Castrillo expone la conveniencia de la pericia informática (de Urbano Castrillo, 2009, 69).

36. Tecnologías que se enmarcan en el contexto de la llamada cuarta revolución industrial o industria 4.0. Término introducido por el economista Schwab (Schwab, 2016).

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

tecnológica. Se trata de la conocida tecnología *blockchain* –o cadena de bloques–[37]. En particular, la notoriedad de la tecnología *blockchain* viene dada a consecuencia de la popularidad que adquirió el modo en que esta tecnología gestiona la información, justamente en aras a garantizar la confianza y credibilidad sobre la misma[38]. Precisamente los debates doctrinales giran en torno a su eventual aprovechamiento en el proceso con especial consideración en el ámbito probatorio, dado que ofrece la posibilidad de aplicar una serie de mecanismos que permiten afianzar la confianza en la información tecnológica que pretende acceder al proceso como prueba[39]. En concreto, se trata de un mecanismo de encriptación de datos mediante el empleo de códigos *hash*. El código *hash* se obtiene a través de la aplicación de un algoritmo que traduce una cantidad de datos informáticos, con independencia de su tamaño, en un valor alfanumérico compuesto por un número determinado de bits[40]. Ocurre aquí que, una vez obtenido el código *hash,* si se modifica un único bit del conjunto de datos, el valor del *hash* será diferente[41]. Del mismo

37. La *blockchain* se formula como una categoría propia de la *Distributed Ledger Technology* (DLT) o tecnología de registro distribuido y, en concreto, se perfila como un modo de aplicar este tipo de tecnología. Muy sucintamente, la tecnología *blockchain* opera como un libro mayor de carácter digital, distribuido e inmutable, garantizado a través de sistemas de criptografía avanzada mediante una red *peer-to-peer* en la que los nodos (usuarios) validan la transacción en virtud de un mecanismo de consenso, puesto que el control de la operación está descentralizado (Ibáñez Jiménez, 2018, 15 y ss.; Gimeno Beviá, 2022, 608).

38. Esta confianza sobre el origen y el contenido de los datos es decisiva para el éxito de los sistemas de información y comunicación, no obstante, la tecnología *blockchain* –basada en sistemas de criptografía– ofrece soluciones aptas para asegurar esta confianza. Los sistemas de criptografía se basan en unos mecanismos de carácter matemático que hacen viable la identificación, por un lado, del origen de las informaciones y, por otro, el control sobre las posibles modificaciones y alteraciones (Arroyo Guardeño, Díaz Vico, y Hernández Encinas, 2019, 6 y ss.).

39. Ello se debe a su propia configuración, según la cual ésta se materializa como una cadena de bloques, en la que los «bloques» constituyen el conjunto de datos que incorporan las transacciones ejecutadas en la red *peer-to-peer* por parte de los nodos que la integran; y la «cadena» representa el enlace criptográfico que mantiene unidos unos bloques con otros. En concreto, este enlace se ejecuta por vía de código *hash*. Esto es, funciones resumen. Se trata de una función con la capacidad de transformar una información o mensaje a una longitud o tamaño en bits determinado, con independencia de su longitud o tamaño original. Al resultado de la operación se le denomina *hash*. Es importante señalar que las funciones *hash* «no cifran ni descifran mensajes, pero son las herramientas indispensables para comprobar la integridad de determinada información» (Arroyo Guardeño, Díaz Vico, y Hernández Encinas, 2019, 21 y ss.; Ibáñez Jiménez, 2018, 20 y ss.).

A grandes rasgos, Pérez Campillo expone los caracteres principales de la tecnología *blockchain,* que identifica como el «ADN» de esta tecnología: primero, la integridad de los datos y de la información, en tanto que los datos –una vez incorporados a la cadena– no son susceptibles de modificaciones en ningún caso; segundo, la confidencialidad; tercero, la autenticación de usuario, como complementario a la confidencialidad; cuarto, la autenticación del remitente y del destinatario, de modo que garantiza la seguridad entre las transacciones, evitando posibles suplantaciones; y quinta, la descentralización de internet e identidad digital, siendo ésta una de las características básicas de la *blockchain* (Pérez Campillo, 2019, 263-264).

40. Los códigos *hash,* en concreto, se obtienen «mediante la aplicación de un algoritmo que convierte una gran cantidad de datos, de un tamaño variable, en un valor pequeño y de tamaño uniforme, por eso los valores hash también son conocidos como números resúmenes». Esto es, la función *hash* convierte una serie de datos (correo electrónico, disco duro, documento ofimático, etc.) en una función matemática a fin de obtener un valor alfanumérico: el *hash* (Sánchez Rubio, 2019, 297).

41. (Sánchez Rubio, 2019). Por su parte, Barria Nievas expone que el enlace de un bloque con otro mediante código *hash* implica que cada bloque se encuentra «criptográficamente vinculado

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

modo, una modificación de los datos en una *blockchain* supondría la alteración de todos los *hashes* que integran la cadena y, en consecuencia, cualquier alteración sería perfectamente verificable[42]. En particular, será un perito informático el encargado de verificar la corrección de la cadena de custodia mediante el examen y comprobación de los códigos *hashes* de la *blockchain* (Santisteban Castro, 2023). De ahí que el grado de credibilidad que ofrece la tecnología *blockchain* se perciba elevado[43].

En definitiva, éste es el fundamento de la hipótesis según la cual el empleo de tecnología *blockchain* es útil en aras a garantizar la corrección de la cadena de custodia de los datos digitales aportados al proceso como prueba[44]. Pero no solo encuentra su encaje en los análisis doctrinales, sino que también en la LECrim podemos localizar el fundamento para la integración de la tecnología *blockchain* como método para garantizar la cadena de custodia. Éste deriva de la reforma operada por la LO 13/2015[45] y, en concreto, de la introducción del art. 588 octies LECrim, el cual establece que el Ministerio Fiscal o la policía judicial:

> Podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión.

En virtud del citado precepto se reconoce la posibilidad de establecer un mecanismo de protección y conservación de pruebas electrónicas cuya aplicación podría tener encaje con arreglo a tecnología *blockchain* (Bueno de Mata, 2023, 82 y ss.).

al anterior y encriptado», de modo que cada bloque contiene una referencia al bloque anterior, de modo que la totalidad de la información contenida queda garantizada con la inclusión de un nuevo bloque a la cadena (Barria Nuevas, 2022, 5 y ss.).

42. A este respecto, conviene señalar que, si bien la modificación de los datos de contenidos en la cadena de bloques es técnicamente posible, no se advierte como probable. Esto deriva de la propia configuración de este tipo de tecnología DLT, puesto que los nodos tienen la capacidad de controlar e impedir los intentos de modificación de los datos, ya que la introducción de modificaciones en la red P2P únicamente es posible contando con el acuerdo de la mayoría de los nodos que la integran, todo ello en virtud del llamado protocolo de consenso (Ibáñez Jiménez, 2018, 22 y ss.).

43. Al hilo de lo anterior, expone Ibáñez Jiménez en relación con la blockchain: «Es, de este modo, una cadena de hashes o identificadores, porque los hashes tienen, junto a la función identificadora de los datos, la de conectar o ligar bloques, haciendo virtualmente irrompible la cadena, y, por ende, dotándola de seguridad material o tecnológica. De esta suerte, la cadena de identificadores de bloques (…) facilita el rastreo, seguimiento, persecución, investigación y (…) trazabilidad de todos los datos; a la par que, merced al mecanismo de la encriptación, veda la posibilidad de alterar la información engarzada» (Ibáñez Jiménez, 2018, 22).

44. En los últimos años son diversos los autores que han formalizado la propuesta de emplear sistemas *blockchain* y funciones *hash* como método para garantizar la inalterabilidad de la fuente de prueba de carácter digital (Sánchez Rubio, 2019, 289 y ss.; González Granda y Ariza Colmenarejo, 2021, 484-487; Soana, 2021, 605 y ss.; Preira Puigvert, 2014); Al hilo de lo anterior, sostiene García Mateos que la única forma de garantizar, a nivel informático, que la evidencia digital no ha sufrido alteración alguna a lo largo de su existencia es a través de su huella digital, esto es, su *hash* (García Mateos, 2016, 136).

45. Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. *Boletín Oficial del Estado*, 239, de 6 de octubre de 2015, pp. 90192-90219. https://www.boe.es/boe/dias/2015/10/06/pdfs/BOE-A-2015-10725.pdf

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

No podemos dejar de mencionar el sistema jurídico de EEUU, donde ya se ha previsto esta posibilidad. Tras una enmienda a las *Federal Rules of Evidence* en el año 2017 (Rothstein, 2021, 1045-1046; Graham, 2021, 695-696)[46], integran en la regla 902 la regulación sobre la prueba que se autoautentica (Marín González y García Sánchez, 2014). Alude a una suerte de presunción *iuris tantum* respecto a la autoautenticación de aquellas pruebas electrónicas que posean un código *hash*, tales como los archivos electrónicos encontrados en un almacenamiento informático. A este respecto, la enmienda mencionada establece la presunción de autenticación de aquellos datos con un código *hash* idéntico, aunque en ocasiones continúe siendo necesaria la intervención de profesionales con formación técnica en la materia que puedan confirmar dicha autenticidad, de ahí, la posibilidad de que la parte contraria pueda emplear las pruebas que considere oportunas para contradecir dicha presunción de autenticidad.

En particular, el citado párrafo 902 (14) FRE establece lo siguiente:

> Certified Data Copied from an Electronic Device, Storage Medium, or File. Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule (902(11) or (12). The proponent also must meet the notice requirements of Rule 902 (11).

La relevancia de esta enmienda, en concreto, radica en que configura el fundamento para la introducción de sistemas *blockchain* como elemento de autoautenticación de las pruebas, esto es, como método para garantizar la cadena de custodia de la prueba digital de forma automática, todo ello en virtud de la seguridad que ofrece el empleo de *hashes*.

3.2. La impugnación de la cadena de custodia tecnológica y la carga de su prueba

Al igual que ocurre con su vertiente tradicional, uno de los puntos más conflictivos de la dimensión tecnológica de la cadena de custodia se encuentra en su impugnación. A pesar de la presencia de peculiaridades propias, la premisa de partida se fija en idénticos parámetros que los que influyen en la cadena de custodia *per se*, principalmente teniendo en cuenta que la impugnación ha de efectuarse en el primer momento en que se tenga conocimiento de la circunstancia que perjudica el desarrollo de la cadena de custodia. También las diversas posibilidades que podrían poner en jaque la mismidad de la prueba pueden sintetizarse en las mismas posibilidades –a saber, la contaminación accidental de la evidencia, la manipulación consciente de la evidencia y la ausencia o errores burocráticos en la documentación de la cadena de custodia (Jamardo Lorenzo, 2024b)–. Con todo, en el caso de la prueba tecnológica las preocupaciones se centran

46. Además, también cuentan con algunos manuales prácticos que orientan las actuaciones tendentes a garantizar la cadena de custodia digital: el más destacado es el *Electronic crime scene investigation: a guide for first responders,* redactado por el Departamento de Justicia. Documento que puede ser consultado en la siguiente página web: https://www.ojp.gov/pdffiles1/nij/219941.pdf (fecha de consulta: 20/09/2024).

IUS ET SCIENTIA • 2024
Vol. 10 • N° 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

especialmente en la posibilidad de manipulación consciente de la evidencia, si bien también se le otorga cierta relevancia a la contaminación accidental de la misma.

Una vez más, la cuestión orbita alrededor de la desconfianza que desprende la prueba tecnológica. Los operadores jurídicos acostumbran a desconfiar de la autenticidad de este tipo de pruebas, aduciendo su fácil manipulación o alteración, motivo por el cual es común impugnar la autenticidad de las mismas (Pérez Daudí, 2020, 1560 y ss.). Al hilo de esto y una vez impugnada la prueba de carácter tecnológico[47], la consecuencia estriba en que se ha de acreditar su mismidad para alcanzar la confianza del juzgador[48]. Es lo que se ha denominado como la prueba sobre la prueba, en tanto que el objeto de ésta es acreditar la autenticidad del contenido del medio probatorio, pero no el objeto del proceso[49]. Teniendo en cuenta que la autenticidad es uno de los elementos que integran el concepto de mismidad de la prueba, esta necesidad de acreditar su autenticidad una vez la misma ha sido impugnada, supone una matización a la presunción de veracidad sobre la corrección de la cadena de custodia en el terreno tecnológico. La excepción viene dada sobre la base de que, en el contexto de la cadena de custodia tradicional, el seguimiento de la fuente de prueba lo efectúan organismos oficiales.

Por otro lado, de impugnarse un documento cuya autenticidad fue acreditada mediante tecnología *blockchain*, para acreditar la mismidad del documento impugnado se podrá acudir, también, a una prueba pericial de carácter instrumental que arroje luz acerca de la autenticidad de los datos. Al tratarse de un documento encriptado, ocurre en este caso que el informe pericial que se efectúe sobre la mismidad del documento plasmará el valor *hash* de la información contenida en él (Rubio Alamillo, 2016). Por tanto, si la prueba hubiese sido alterada, esta manipulación se reflejaría en una alteración del valor *hash*.

Finalmente, tiene interés el Dictamen 1/2016 de la unidad de Criminalidad Informática de la Fiscalía General del Estado (en adelante FGE), donde se expone que las distintas herramientas TIC ofrecen diversas posibilidades de cara a la manipulación de la prueba tecnológica, en tanto que posibilitan la simulación total o parcial del contenido de las fuentes de prueba. Asimismo, el Dictamen 1/2016 ya puso sobre la mesa la cuestión del desplazamiento de la carga de la prueba ante la impugnación de la prueba tecnológica y, en concreto, en relación a la valoración de las evidencias, ya sean en soporte papel o en soporte electrónico, que acceden al proceso como medio

47. Señala Espín López que no hay previsión normativa al respecto, sin embargo, ésta podrá ser impugnada al igual que cualquier otra prueba (Espín López, 2021b, 270).

48. En este sentido, y a propósito de la impugnación de la prueba tecnológica, Arrabal Platero expone que, una vez superado el trámite de admisión de la prueba, ésta podrá ser impugnada por la otra parte «por considerar que no concurre en ellas los requisitos de autenticidad e integridad». Y añade la autora que las partes impugnarán las pruebas de contrario ante su eventual falsedad, sobre la base de la inautenticidad –«la prueba ha sido creada *ex novo* para el proceso»– o de la manipulación –la alteración de la prueba por medio de la supresión o modificación de datos– de las mismas (Arrabal Platero, 2020, 335 y ss.).

49. Al respecto de la impugnación de la prueba tecnológica, afirma la Sánchez Rubio que la carga sobre 'la prueba sobre la prueba' se sitúa en la parte que pretende beneficiarse de los efectos probatorios de la prueba. En opinión de la autora, al contrario de lo que ocurre con la prueba tradicional, será la parte contraria quien deba probar la ausencia de fiabilidad de la prueba (Sánchez Rubio, 2019, 292 y ss.).

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

de prueba de comunicaciones electrónicas[50]. Al respecto, la postura de la FGE rechaza el desplazamiento automático, entendiendo que se determinará en virtud de la seriedad y razonabilidad del planteamiento impugnatorio que habrá de ser analizado en cada caso.

3.3. La valoración de la actividad probatoria. La fiabilidad de la prueba tecnológica en virtud de la cadena de custodia

La valoración de la prueba se produce una vez superados los requisitos de admisibilidad –licitud, pertinencia y utilidad– y que, además, su práctica se haya efectuado en el juicio oral –con las excepciones de la prueba anticipada y preconstituida– y con el debido respeto a las garantías de oralidad, inmediación y contradicción. Es importante destacar que, en la valoración de un medio de prueba cuya cadena de custodia pueda proyectar alguna duda menor sobre el juzgador, los restantes elementos del acervo probatorio serán determinantes a la hora de apreciarla o no.

Respecto de los elementos materiales de prueba (y, en particular, cuando su carácter es tecnológico) no podemos negar la importancia de que se cumplan ciertas condiciones para que puedan ser valorados. Por un lado, es preciso que la obtención la prueba se efectúe con respeto a los DDFF (de lo contrario, estaremos ante un supuesto de prueba prohibida); pero, además, de cara a afianzar la fiabilidad de la prueba material es preciso ofrecer garantías suficientes sobre la autenticidad e integridad del elemento (Merkel, 2022, 97), lo que conecta muy de cerca con la acreditación de la cadena de custodia. Y, en concreto, cuando hablamos de prueba tecnológica, esto será imprescindible cuando su autenticidad haya sido impugnada. De ese modo, la fiabilidad de una prueba material sobre la cual se ha acreditado fehacientemente la corrección de la cadena de custodia, adquiere mayor dimensión que una prueba respecto de la cual no se haya acreditado ni desacreditado tales extremos. En tal sentido, la prueba ofrecerá una mayor sensación de confianza al juez que, no obstante, valorará libremente la prueba.

Lo anterior tiene gran importancia, en tanto que, una vez más, la desconfianza que genera la prueba tecnológica vuelve a ser protagonista. Lo crucial en este punto es reparar el bajo grado de fiabilidad del que partimos, por lo que se habrá de acudir a las herramientas procesales que nos permitan incrementar esta fiabilidad de cara a su valoración. En definitiva, si una parte introduce una prueba de carácter tecnológico y –además– introduce al proceso los medios suficientes para acreditar la corrección de la cadena de custodia, esto repercutirá muy positivamente en la valoración de la prueba tecnológica. En este sentido, la relación entre valoración de la prueba y corrección de la cadena de custodia parte de premisas similares, pero se intensifica cuando se trata de pruebas de carácter tecnológico.

50. Muy sintéticamente, queremos resaltar dos cuestiones: la primera, señala el Dictamen que, una vez impugnado el medio de prueba que pretende introducir al proceso el contenido de las comunicaciones electrónicas, podrá ser necesaria la práctica de nuevas diligencias de prueba que acrediten la existencia de la comunicación, su origen, destino o contenido; la segunda, que no en todos los casos será necesario un informe pericial informático, sosteniendo que éste únicamente podrá ser imprescindible cuando no sea posible acreditar la autenticidad de las comunicaciones por otros medios.

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

Bibliografía

Álvarez de Neyra Kappler, S. (2015). La cadena de custodia en materia de tráfico de drogas. En C. Figueroa Navarro (dir.), *La cadena de custodia en el proceso penal* (pp. 81-106). Edisofer.

Arellano, L. E. y Castañeda, C. M. (2012). La cadena de custodia informático-forense. *Cuadernos informático-forense,* 3 (1), 67-81.

Arrabal Platero, P. (2020). *La prueba tecnológica: aportación, práctica y valoración*. Tirant lo Blanch.

Arrabal Platero, P. (2021). El valor probatorio de la información contenida en un dispositivo tecnológico. En L. Bujosa Vadell (dir.), *Derecho procesal: retos y transformaciones* (pp. 521-539). Atelier.

Arroyo Guardeño, D., Díaz Vico, J. y Hernández Encinas, L. (2019). *Blockchain*. Editorial CSIC.

Barria Nuevas, S. (2022). Introducción al Blockchain: análisis del *play to earn*. *Revista Blockchain e Inteligencia Artificial,* 3 (4), 1-28.

Bueno de Mata, F. (2019). *Las diligencias de investigación penal en la cuarta revolución industrial: principios teóricos y problemas prácticos.* Aranzadi.

Bueno de Mata, F. (2023). Blockchain, identidad autosoberana y prueba electrónica transfronteriza. En A. Hernández López y M. E. Laro González (dirs.), *Proceso penal europeo: últimas tendencias, análisis y perspectivas* (pp. 71-86). Aranzadi.

Calaza López, S. (2022). Cadena de custodia y prueba tecnológica. En C. Villegas Delgado y P. Martín Ríos (dirs.), *El drerecho en la encrucijada tecnológica: estudios sobre derechos fundamentales, nuevas tecnologías e inteligencia artificial* (pp. 39-61). Tirant lo Blanch.

Calaza López, S. y Muinelo Cobo, J. C. (2020). La digitalización y custodia de la prueba pericial electrónica sobre evidencias virtuales. En J. Picó i Junoy (dir.), *La prueba pericial a examen: propuestas de lege ferenda* (pp. 471-481). J. M. Bosch.

Campos, F. (2002). La relevancia de la cadena de custodia en la investigación judicial. *Medicina legal de Costa Rica,* 19 (1).

Colomer Hernández, I. (2023). Limitaciones en el uso de la información y los datos personales en un proceso penal digital. En C. Angüena Fanego, M. de Hoyos Sancho y E. Pillado González (dirs.), *El proceso penal ante una nueva realidad tecnológica europea* (pp. 39-74). Aranzadi.

Cuadrado Salinas, C. (2020). La obtención de pruebas electrónicas transfronterizas: nuevos retos y nuevas consideraciones desde la perspectiva de la Unión Europea. En J. M. Asencio Mellado (dir.), *Derecho probatorio y otros estudios procesaler. Liber Amicorum: Vicente Gimeno Sendra* (pp. 517-534). Ediciones Jurídicas Castillo de Luna.

de Urbano Castrillo, E. (2009). *La valoración de la prueba electrónica*. Tirant lo Blanch.

del Pozo Pérez, M. (2014). *Diligencias de investigación y cadena de custodia.* Sepín.

Delgado Martín, J. (2018). *Investigación tecnológica y prueba digital en todas las jurisdicciones* (2ª ed.). La Ley.

Espín López, I. (2021a). *Investigación sobre equipos informáticos y su prueba en el proceso penal.* Aranzadi.

Espín López, I. (2021b). La cadena de custodia en el proceso penal. Propuestas en relación con el análisis y custodia de la prueba digital. *La Ley penal* (151).

Fuentes Soriano, O. (2016). La intervención de las comunicaciones tecnológicas tras la reforma de 2015. En J. Alonso-Cuevillas Sayrol (dir.), *El nuevo proceso penal tras las reformas de 2015* (pp. 261-285). Atelier.

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

Fuentes Soriano, O. (2017). El valor probatorio de los correos electrónicos. En J. M. Asencio Mellado (dir.), *Justicia penal y nuevas formas de delincuencia* (pp. 183-210). Tirant lo Blanch.

García de Yébenes, P. y Gascó Alberchi, P. (2015). La cadena de custodia de muestras relacionadas con presuntos ilícitos contra el medio ambiente. En C. Figueroa Navarro (dir.), *La cadena de custodia en el proceso penal* (pp. 129-137). Edisofer.

García Mateos, J. A. (2016). Cadena de custodia vs. mismidad. En R. Oliva León, S. Valero Barceló y Á. Dolado Pérez (dirs.), *La prueba electrónica: validez y eficacia procesal* (pp. 130-136). Juristas con futuro.

Garcimartín Montero, R. (2018). *Los medios de investigación tecnológicos en el Proceso Penal.* Aranzadi.

Gimeno Beviá, J. (2022). Blockchain y resolución de conflictos: algunas reflexiones. En J. Martín Pastor y R. Juan Sánchez (dirs.), *El Derecho Procesal: entre la Academia y el Foro* (pp. 607-613). Atelier.

González Granda, P. y Ariza Colmenarejo, M. J. (2021). *Justicia y proceso: una revisión procesal contemporánea bajo el prisma constitucional.* Dykinson.

Graham, M. H. (2021). *Federal Rules of Evidence in a nutshell* (11ª ed.). West Academic Publiching.

Gutiérrez Sanz, M. R. (2016). *La cadena de custodia en el proceso penal español.* Civitas.

Guzmán Fluja, V. C. (2006). *Anticipación y preconstitución de la prueba en el proceso penal.* Tirant lo Blanch.

Ibáñez Jiménez, J. W. (2018). *Blockchain: primeras cuestiones en el ordenamiento español.* Dykinson.

Jamardo Lorenzo, A. (2024a). *Construcción jurisprudencial y evolución de la cadena de custodia: análisis sistemático.* Colex.

Jamardo Lorenzo, A. (2024b). La cadena de custodia: configuración jurídica y estado actual de la cuestión. *Justicia: revista de derecho procesal* (1), 299-387.

López Valera, M. (2016). Localización, hallazgo y recogida de muestras de ADN en la cadena de custodia. *Revista de Derecho UNED* (19), 777-808.

Marín González, J. C. y García Sánchez, G. J. (2014). Problemas que enfrenta la prueba digital en los Estados Unidos de América. *Revista de Estudios de Justicia* (21), 75-91.

Martín Ríos, P. (2020). Problemas de admisibilidad de la prueba obtenida de dispositivos de almacenamiento digital. *Revista General de Derecho Procesal* (51).

Martínez Galindo, G. (2022). Problematica jurídica de la prueba digital y sus implicaciones en los principios penales. *Revista Electrónica de Ciencia Penal y Criminología* (24).

Merkel, L. (2022). *Derechos humanos e investigaciones policiales. Una tensión constante*. Marcial Pons.

Mestre Delgado, E. (2015). La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos. En C. Figueroa Navarro (dir.), *La cadena de custodia en el proceso penal* (pp. 39-79). Edisofer.

Moreno Catena, V. y Cortés Domínguez, V. (2004). *Derecho Procesal Penal.* Tirant lo Blanch.

Ortiz Padrillo, J. C. (2013). *Problemas procesales de la ciberdelincuencia.* Colex.

Pérez Campillo, L. (2019). Blockchain: ¿amenaza o solución en la protección de datos y privacidad? En F. Bueno de Mata (dir.), *Fodertics 7.0: estudios sobre derecho digital* (págs. 261-268). Comares.

Pérez Daudí, V. (2020). La prueba electrónica: naturaleza jurídica e impugnación. En J. M. Asencio Mellado (dir.), *Derecho probatorio y otros estudios procesales. Liber Amicorum: Vicente Gimeno Sendra* (pp. 1557-1576). Ediciones Jurídicas Castillo de Luna.

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05

Pérez Gil, J. (2019). Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal. En F. Jiménez Conde y R. Bellido Penadés (dirs.), *Justicia: ¿garantías versus eficiencia?* (pp. 399-441). Tirant lo Blanch.

Preira Puigvert, S. (2014). Sistema de hash y aseguramiento de la prueba informática. Especial referencia a las medidas de aseguramiento adoptadas inaudita parte. En F. Bueno de Mata (dir.), *Fodertics II: hacia una justicia 2.0* (pp. 75-83). Comares.

Richard González, M. (2017). La investigación y prueba de hechos y dispositivos electrónicos. *Revista General de Derecho Procesal* (43).

Roca Martínez, J. M. (2020). Nuevas tecnologías e investigación penal: garantías ante injerencias y motivación de su autorización. En L. A. Fernández Villalón (dir), *Derecho y nuevas tecnologías* (pp. 71-92). Civitas.

Rothstein, P. F. (2021). *Federal Rules of Evidence* (3ª ed.). Thomson Reuters.

Rubio Alamillo, J. (2016). Conservación de la cadena de custodia de una evidencia informática. *Diario la Ley* (8859).

Rubio Alamillo, J. (2018). Cadena de custodia y análisis forense de smartphones y otros dispositivos móviles en procesos judiciales. *Diario la Ley* (9300).

Sánchez Melgar, J. (2016). La nueva regulación de las medidas de investigación tecnológica. Estudio de su parte general. *Práctica penal: cuaderno jurídico* (82).

Sánchez Rubio, A. (2019). Cadena de custodia y prueba electrónica: la mismisdad del hash como requisito para la fiabilidad probatoria. En F. Bueno de Mata (dir.), *FODERTICS 7.0: estudios sobre derecho digital* (pp. 289-299). Comares.

Sanjurjo Ríos, E. I. (2020). Proceso penal y volatilidad/mutabilidad de las fuentes de prueba electrónicas: sobre la conveniencia y el modo de asegurarlas eficazmente. En P. González Granda (dir.), *Exclusiones probatorias en el entorno de la investigación y prueba electrónica* (pp. 195-224). Reus.

Santisteban Castro, M. (2023). Algunas consideraciones en torno al valor probatorio de la tecnología blockchain en el ámbito europeo: presente y futuro. *La Ley probática* (12).

Schwab, K. (2016). *La cuarta revolución industrial.* Debate.

Soana, G. (2021). Block-chain y prueba digital. Una oportunidad para la cadena de custodia. En S. Pereira Puigvert y X. Ordóñez Ponz (dirs.), *Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos* (pp. 605-628). Aranzadi.

Vegas Torres, J. (2017). Las medidas de investigación tecnológica. En M. Cedeño Hernán (dir.), *Nuevas tecnologías en el proceso* (pp. 21-47). Aranzadi.

Velasco Núñez, E. (2020). Investigación penal y protección de datos. *El cronista social y democrático de Derecho* (88-89), 136-151.

IUS ET SCIENTIA • 2024
Vol. 10 • Nº 2 • pp. 101-122
ISSN 2444-8478 • https://dx.doi.org/10.12795/IESTSCIENTIA.2024.i02.05