InDret
2.2025

La dimensión tecnológica de la cadena de custodia: algunas claves

Andrea Jamardo Lorenzo
Universidad de León

Sumario

El presente trabajo constituye una reflexión conducente al enunciado de algunas claves en torno a la dimensión tecnológica de la cadena de custodia en el ordenamiento jurídico español. 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, analizando específicamente la problemática que surge de cara a la acreditación de la mismidad de la prueba tecnológica y las diferentes soluciones contempladas. Finalmente, concluye con una serie de reflexiones y propuestas de lege ferenda.

Abstract

This paper is a study of the technological nature of the chain of custody in the Spanish legal system. In addition to the difficulties inherent to the traditional chain of custody, given its limited regulation, there are several complexities resulting from its technological dimension; in this sense, the paper explains how it is constructed and the way in which its material and formal aspects are formulated. It specifically analyzes the problem that arises in the face of the accreditation of the sameness of technological evidence and examines the different solutions that have arisen. It concludes with a few reflections and proposals de lege ferenda.

Title: *Some issues on the digital nature of the chain of custody*

Palabras clave: análisis prospectivo-legal; cadena de custodia tecnológica; mismidad de la prueba tecnológica; tecnologías disruptivas.
Keywords**:** *prospective legal analysis; digital chain of custody; sameness of the digital evidence; disruptive technologies.*

DOI: 10.31009/InDret.2025.i2.07

InDret

2.2025

Recepción
10/12/2024
-
Aceptación
05/02/2025
-

Índice

-

-

1. Introducción: origen y construcción de la cadena de custodia en el ordenamiento jurídico español*

Constituye la cadena de custodia una realidad compleja cuyo interés no ha hecho sino crecer con el tiempo. Reflejo de ello es la evolución que esta figura ha experimentado con el paso del tiempo: evolución que se inició en la década de los años noventa, 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: 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[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.

Atendiendo muy especialmente a la evolución sintetizada en las líneas anteriores y con el propósito de precisar el camino que parece seguir la configuración jurídica de la cadena de custodia en el ordenamiento jurídico español, podemos sostener que nos hallamos, con toda probabilidad, en un contexto de tránsito en el que, precisamente, estamos a la espera del nacimiento de una nueva etapa (hecho que naturalmente se producirá con la aprobación de una

* Andrea Jamardo Lorenzo (ajaml@unileon.es). Doctora en Derecho y profesora sustituta de Derecho Procesal. Universidad de León.

[1] En relación con la diferenciación de estas tres etapas evolutivas, muy sintéticamente podemos exponer algunos de los hitos jurisprudenciales que las componen. Así, la primera etapa se encuadra temporalmente entre los años noventa y hasta aproximadamente el año 2002. Si bien lo característico de esta etapa es el escaso desarrollo jurídico de la cadena de custodia, no podemos dejar de mencionar ciertas resoluciones jurisprudenciales que ponen en valor la figura analizada (al menos, dejan entrever el comienzo de este camino evolutivo). Éste es el caso de la SAP SE 440/1998, de 11 de julio, ECLI:ES:APM:1998:4277, donde se alude a la "continuidad de la cadena de custodia"; también, muy en relación con el deber de documentación como medio de acreditar la regularidad de la cadena de custodia o con la posibilidad de subsanar errores en base a las testificales de los intervinientes en la misma, podemos mencionar la STS 936/1998, de 13 de julio, ECLI:ES:TS:1998:4686, y la SAP SE 687/1998, de 16 de noviembre, ECLI:ES:APSE:1998:3825. Cobran especial relevancia, además, la STSJ CAT 1/2000, de 21 de febrero, ECLI:ES:TSJCAT:2000:2298 (rompe con la vinculación en exclusiva de la cadena de custodia con las muestras de droga y se vincula al análisis de una prueba de ADN) y la STS 1587/2001, de 11 de septiembre, ECLI:ES:TS:2001:6733 (introduce el término 'corrección de la cadena de custodia'). Con la llegada de la segunda etapa (años 2003 a 2009, aproximadamente) surgen las primeras conceptualizaciones y una superficial concreción de las consecuencias de la ruptura de la cadena de custodia en relación con su incidencia en la fiabilidad de la prueba pericial (ilustra esta cuestión, entre otras, la STS 925/2008, Sala de lo Penal, de 26 de diciembre, ECLI:ES:TS:2008:7258). Finalmente, la tercera y actual etapa se inicia con la introducción del término mismidad de la prueba (SAP B 123/2009, de 25 de febrero, ECLI:ES:APB:2009:1719; STS 1190/2009, de 3 de diciembre, ECLI:ES:TS:2009:7710; STS 6/2010, de 27 de enero, ECLI:ES:TS:2009:542) y se caracteriza por la consolidación jurisprudencial de los elemento esenciales de la cadena de custodia, concretando más concienzudamente las consecuencias jurídicas de una eventual ruptura de la misma (por ejemplo, STS 587/2014, de 18 de julio, ECLI:ES:TS:2014:3086; STS 90/2021, de 3 de febrero, ECLI:ES:TS:2021:319; STS 241/2024, de 13 de marzo, ECLI:ES:TS:2024:1342; STS 317/2024, de 22 de julio, ECLI:ES:TS:2024:11267). *Vid.* JAMARDO LORENZO, *Construcción jurisprudencial y evolución de la cadena de custodia: análisis sistemático*, Colex, A Coruña, 2024, pp. 19 ss.

regulación expresa y unitaria de la cadena de custodia[2]). A fin de respaldar esta afirmación, resulta muy conveniente destacar algunos hechos que se han producido en el marco de la tercera y actual etapa y que nos ofrecen una perspectiva de futuro sumamente prometedora. Y es que, a pesar de la ausencia de regulación expresa, lo cierto es que en los últimos años se han manifestado las primeras muestras de voluntad legislativa en la materia, lo que demuestra una realidad innegable: la cadena de custodia está presente en los intereses legislativos contemporáneos. En concreto, me estoy refiriendo a los dos intentos, ahora frustrados, de incorporar en la Ley de Enjuiciamiento Criminal (en adelante LECrim) la tan anhelada regulación procesal expresa de la figura analizada. Sucedía esto con los Anteproyectos de LECrim (en adelante ALECrim) de los años 2011 y 2020. Tampoco debemos olvidar que la doctrina lleva años acusando la ausencia de esta regulación procesal expresa. 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 ha de ser resulto con prontitud, de cara a suplir la orfandad legal que hoy en día caracteriza a la figura analizada. Asimismo, resulta oportuno señalar que, pese a la situación normativa en España –y, en general, en Europa[4]–, la regulación de la figura de la cadena de custodia es una realidad en una variedad de ordenamientos jurídicos. Precisamente el análisis de otros sistemas de Derecho comparado es particularmente oportuno en materia de

[2] *Ibidem*, pp. 207 y 208.

[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/CORTÉS DOMÍNGUEZ, *Derecho Procesal Penal,* Tirant lo Blanch, Valencia, 2004, pp. 367-377; GUZMÁN FLUJA, *Anticipación y preconstitución de la prueba en el proceso penal,* Tirant lo Blanch, Valencia, 2006, pp. 309 ss.). Sin embargo, el tratamiento ofrecido entonces comúnmente se localizaba en apartados de 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] En este contexto, es reseñable también el Reglamento (UE) 2023/1543, relativo a las órdenes europeas de producción y conservación de prueba electrónica en los procesos penales (que, no obstante, no ha hecho alusión alguna a la cadena de custodia pese al ámbito en el que opera), circunstancia acorde con la realidad europea. Ausencia que ya ha sido advertida por GONZÁLEZ GRANDA cuando el citado Reglamento europeo era todavía una propuesta. *Vid.* GONZÁLEZ GRANDA, «Órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento criminal: próximo avance en materia de prueba penal transfronteriza», en MORENO CATENA/ROMERO PRADAS (dirs.), *Nuevos postulados de la cooperación judicial en la Unión Europea. Libro homenaje a la Profª. Isabel González Cano*, Tirant lo Blanch, Valencia, 2021, p. 1099. Pues no debemos olvidar que tampoco la Orden Europea de Investigación (OEI) incorporó previsiones al respecto y ello a pesar de que, tratándose de un instrumento que opera en el entorno de la investigación penal y la obtención de fuentes de prueba, naturalmente se manifiesta presente la problemática derivada de la cadena de custodia. Al no haberse previsto normas específicas para el mantenimiento de la cadena de custodia, es necesario que los Estados implicados se pongan de acuerdo a fin de ejecutar la OEI del mejor modo posible para asegurar la cadena de custodia y evitar de ese modo las fatales consecuencias que su ruptura pudiese ocasionar. Uno de los supuestos más comunes es la diligencia de entrega vigilada. Lo fundamental se produce cuando España actúa como Estado de emisión. Ocurre aquí que el Estado de ejecución no está obligado a seguir la normativa española, si bien ambos Estados podrán ponerse de acuerdo a fin de cumplir pequeñas formalidades y exigencias procedimentales mínimas, a fin de evitar la pérdida de validez de la diligencia en el Estado de emisión. En tal sentido, el Estado de ejecución podrá aceptar estas cuestiones cuando las peticiones formuladas no sean contrarias a su ordenamiento jurídico. En materia de cadena de custodia, señala LARO GONZÁLEZ que es crucial el acta que levanten los agentes, donde se debe indicar la descripción del continente y también del contenido, «así como las características concretas del material de la remesa, por ejemplo, el peso, el envoltorio, el color, etc., las personas intervinientes en cada momento y lugar, el tiempo que hayan permanecido en posesión de las mismas, y aquellas circunstancias que sean relevantes para su preservación». Asimismo, la autora recalca la importancia de cumplir con las exigencias de cadena de custodia a fin de evitar la vulneración del derecho a un proceso con todas las garantías. En definitiva, la coordinación entre autoridades policiales y judiciales es esencial en la ejecución de entregas vigiladas en aras a garantizar la plena eficacia de la medida. *Vid.* LARO GONZÁLEZ, *La Orden Europea de Investigación en el Espacio Europeo de Justicia*, Tirant lo Blanch, Valencia, 2021, pp. 261 ss.

cadena de custodia (a causa de la situación normativa interna) y contribuye a una comprensión más exhaustiva e integral de la figura examinada. Sobra decir que ofrecer un estudio comparado no es el propósito de este trabajo, sin embargo, sí queremos dejar de manifiesto que la construcción jurídica de la cadena de custodia en nuestro país se produce con años de retraso con respecto a otros ordenamientos jurídicos ajenos, principalmente en atención al sistema jurídico de Estados Unidos[5] –productor de la figura de la cadena de custodia– y a diversos ordenamientos iberoamericanos[6].

Ahora bien, tomando como base esta característica de orfandad legal de nuestro ordenamiento interno, es preciso, no obstante, hacer una matización. Y es que no es posible hablar de una orfandad legal absoluta, por cuanto en nuestra LECrim existen ciertos preceptos que, en conjunto, ofrecen una regulación indirecta de la cadena de custodia[7]. Con todo, esta regulación se identifica 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 (de conformidad con la pluralidad de textos normativos que regulan aspectos de la cadena de custodia). Si bien debemos hacer hincapié en que esta heterogeneidad se produce no sólo desde el plano legal –donde las referencias son, en efecto, escasas– sino y fundamentalmente desde la perspectiva reglamentaria e institucional[8]. En efecto, multitud de instrumentos 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

[5] Con carácter general, la cadena de custodia en EEUU está regulada en la regla 901 de las *Federal Rules of Evidence*. En su texto original, la regla 901(a) establece lo siguiente: «*In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is*». *Vid.* ROTHSTEIN, *Federal Rules of Evidence,* 3ª ed., Thomson Reuters, Eagan, 2021, pp. 1014 ss., ofrece una visión detallada de los ejemplos contenidos en la Regla 901(b), completando cada uno de ellos con diversas referencias a la jurisprudencia de los tribunales estadounidenses. Especialmente revelador resulta que el autor hace referencia a la cadena de custodia en los siguientes términos: «*Insuring that the real item of physical evidence is the same as that offered at Trial or for testing*», lo que naturalmente evoca a una de las características fundamentales de la cadena de custodia en España: la mismidad de la prueba.

[6] Ilustra esta afirmación muy especialmente el ordenamiento jurídico colombiano, con regulación expresa de la cadena de custodia desde el año 2000, con la aprobación del Código de Procedimiento Penal del año 2000 –expedido mediante la Ley 600 de 2000–, convirtiéndose en uno de los grandes referentes en la materia, regulación expresa que mantiene su actual Código de Procedimiento Penal del año 2004 (arts. 254 a 266), en el que se contiene un capítulo dedicado enteramente a la cadena de custodia (incorporado en el Título I –la indagación y la investigación–; a su vez, en el Libro II –técnicas de investigación de la prueba y sistema probatorio–). *Vid*. LEMUS SOLER, «Cadena de custodia en el ordenamiento jurídico colombiano a la luz de la Ley 906, ¿ficción o realidad?», *Revista Iter ad Veritatem*, núm. 12, 2014, p. 125.

[7] 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.

[8] 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.

líneas. Se trata de una pluralidad de protocolos, manuales[9] o guías de actuación que constituyen la normativización de la cadena de custodia a través de normas de carácter procedimental[10] y que, a fin de cuentas, constituyen un procedimiento de manipulación de las evidencias, por tanto, afectante a la condición práctica y técnica de la figura analizada. Al hilo de esto, sostiene la doctrina que justamente son las ciencias forenses las que mayor influencia tienen sobre «el desarrollo sectorial de las técnicas de recogida, custodia y análisis»[11], 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, en principio, más desconocidas y menos tradicionales. Justamente, el objetivo central de este trabajo es examinar la configuración de la cadena de custodia tecnológica. Con todo, es imprescindible delimitar (como paso previo al abordaje de la cadena de custodia desde su dimensión 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[12] material y finalizan con su introducción en el juicio oral a través del medio de prueba oportuno[13].

[9] Un ejemplo de ello es 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.

[10] 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, 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.

[11] GUTIÉRREZ SANZ, *La cadena de custodia en el proceso penal español*, Civitas, Navarra, 2016, p. 43.

[12] Es oportuno señalar que la diferenciación conceptual entre fuente y medio de prueba no ha estado exenta de críticas. Sobre el particular, surge un sector doctrinal actual que ha criticado la excesiva relevancia teórica de la distinción entre ambos conceptos, sosteniendo que ésta no tiene una auténtica significación práctica o, al menos, no de tal magnitud. Al respecto, *vid.* NIEVA FENOLL, «La prueba preconstituida: un concepto erróneo e imposible», *Diario la Ley,* núm. 10532, 2024. A pesar de la posición doctrinal expuesta, considero que –en el concreto ámbito de la cadena de custodia– diferenciar entre ambos conceptos es preciso para exponer adecuadamente tanto el concepto como la finalidad de la cadena de custodia, como así ha quedado patente en la definición que, sobre la figura analizada, se ha ofrecido en texto.

[13] JAMARDO LORENZO, «La cadena de custodia: configuración jurídica y estado actual de la cuestión», *Justicia: revista de derecho procesal,* núm. 1, 2024, pp. 331-332.

2. Exposición de la problemática específica que afecta a la cadena de custodia tecnológica

Decíamos en la introducción de este trabajo que surge una dificultad añadida a la complejidad propia de la figura de la cadena de custodia en atención a su formulación en el contexto tecnológico. En tal sentido, no podemos obviar que los avances tecnológicos que se han ido produciendo, desde la última década del siglo XX, han tenido gran repercusión en la construcción de la sociedad contemporánea, de modo que la proyección de las nuevas tecnologías se observa no sólo en la disciplina jurídica, sino en todos los ámbitos de la sociedad actual[14]. Y es que el fenómeno de la digitalización se extiende –en efecto– a todos los ámbitos de nuestras vidas, ya sea a través de la creación de nuevos espacios digitalizados desde su origen o mediante la transformación de entornos más tradicionales de cara a su también digitalización[15].

La Administración de Justicia, sin duda, pertenece al grupo de aquellos entornos tradicionalmente analógicos que se van digitalizando progresivamente con la llegada de las nuevas tecnologías a nuestras vidas. Naturalmente, la tecnologización del ámbito jurídico exige la implementación de nuevas perspectivas en el análisis y estudio del Derecho a fin de abordar la problemática específica y en aras a alcanzar soluciones adecuadas en relación con la respuesta jurídica que deba ofrecerse a los problemas derivados de la omnipresencia de las tecnologías en el proceso. Así las cosas, la consolidación de la sociedad digitalizada propicia el surgimiento de escenarios novedosos, por ejemplo, en el ámbito probatorio –en particular, en relación con un incremento de las fuentes de prueba de carácter tecnológico y, en consecuencia, su introducción al proceso a través de los medios de prueba adecuados para ello[16]–, así como en el contexto de la investigación criminal o la aparición de la llamada

[14] El hecho de que, en la actualidad, las tecnologías se posicionen en el núcleo de la sociedad contribuye al empleo de términos tales como era digital, sociedad digital, cuarta revolución industrial o, incluso, en el ámbito jurídico el surgimiento del que ha sido llamado Derecho Digital (aunque este último, en realidad, no ha sido propulsado como una rama independiente del Derecho, cierto es que la omnipresencia de las tecnologías ostenta gran repercusión en el contexto jurídico y hay autores, como BARRIO ANDRÉS, *Manual de Derecho Digital,* 2ª ed., Tirant lo Blanch, Valencia, 2022, pp. 36 ss., que sostienen que el derecho digital «aspira a ser una nueva disciplina jurídica», defendiendo –así– el nacimiento de una rama jurídica autónoma, que «disponga de su propia regulación, lenguaje y elementos axiológicos». En cuanto a la expresión 'cuarta revolución industrial', SCHWAB, *La cuarta revolución industrial*, Debate, Barcelona, 2016, pp. 19 ss., introdujo este término para referirse a la constante transformación del mundo en que vivimos debido a la cada vez mayor presencia de las diferentes tecnologías.

[15] ARRABAL PLATERO expone acertadamente varios ejemplos de entornos tradicionales que han ido modificándose con la llegada de Internet, tales como la prensa –con el crecimiento de la prensa digital–; las plataformas de entretenimiento; los modelos de negocio *peer to peer* propias de la llamada «economía colaborativa» o las entidades bancarias –las sucursales tradicionales están dando paso a las aplicaciones que nos ofrecen la posibilidad de gestionar nuestros productos bancarios a través de nuestro teléfono móvil–, entre otros. *Vid.* ARRABAL PLATERO, *La prueba tecnológica: aportación, práctica y valoración*, Tirant lo Blanch, Valencia, 2019*,* pp. 23 ss. A estos podemos añadir prácticamente cualquier ejemplo: desde la facilidad actual para realizar la compra en un supermercado a través de su página web –o de cualquier otro producto, ya que actualmente la mayor parte de los negocios ofrecen sus servicios a través de Internet– hasta la transformación de los modelos de trabajo –con el cambio del modelo presencial en una oficina física hacia el teletrabajo, muy potenciado especialmente con ocasión de la pandemia originada por el COVID-19–.

[16] BUENO DE MATA, «El derecho probatorio en la cuarta revolución industrial», en ASENCIO MELLADO (dir.), *Derecho probatorio y otros estudios procesales. Liber Amicorum: Vicente Gimeno Sendra*, Ediciones Jurídicas Castillo de Luna, Madrid, 2020, pp. 310 ss.; MAGRO SERVET, «¿Cómo aportar la prueba digital en el proceso penal?», *Diario la Ley,* núm. 9824, 2021.

ciberdelincuencia[17]. Y precisamente en este contexto se plantea la formulación de la cadena de custodia desde su dimensión tecnológica.

Atendiendo a lo expuesto en las líneas anteriores, es importante destacar que abordar la problemática específica de la cadena de custodia tecnológica requiere un enfoque desde cuatro perspectivas: primero, en relación con la fuente de prueba tecnológica; segundo, en relación con la investigación tecnológica; tercero, en relación con el incremento de la ciberdelincuencia y, por último, en relación con la protección de ciertos derechos fundamentales (en adelante DDFF). Lo veremos a continuación.

2.1. En relación con los caracteres específicos de la fuente de prueba tecnológica

Hoy en día, la omnipresencia de las nuevas tecnologías en la vida de las personas tiene un reflejo directo en la proliferación de la prueba de carácter tecnológico en el ámbito jurídico. Y es que cada vez con mayor frecuencia los dispositivos tecnológicos se configuran como fuentes de prueba en el proceso penal, ya sea por tratarse de los medios utilizados para la comisión de los hechos delictivos como por la posibilidad de que contengan evidencias de la comisión de los delitos[18].

En el plano de la prueba tecnológica y a fin de concretar su delimitación conceptual, es preciso partir de los postulados clásicos a propósito de la diferenciación entre fuente y medio de prueba. Y ello porque ha de quedar muy claro que la fuente de prueba hace referencia a la información o datos contenidos o transmitidos por dispositivos tecnológicos; mientras que el medio de prueba es el modo en que dicha información accede al proceso[19]. Así, la prueba tecnológica puede identificarse, por un lado, con los datos informáticos con trascendencia en un proceso y, por otro, con las evidencias que se hayan obtenido a través de medios tecnológicos[20]. En cuanto a las características propias de la prueba tecnológica, siguiendo a

[17] La delincuencia se ha digitalizado y, en tal sentido, la irrupción de las tecnologías en la sociedad supuso la aparición de nuevas formas de delincuencia: la llamada ciberdelincuencia. En palabras de DELGADO MARTÍN, la ciberdelincuencia alude a la comisión de ilícitos penales en el «ciberespacio», entendiendo éste como el «ámbito artificial creado por medios informáticos». *Vid.* DELGADO MARTÍN, *Investigación tecnológica y prueba digital en todas las jurisdicciones,* 2ª ed., La Ley, Madrid, 2018, p. 300.

[18] MESTRE DELGADO, «La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos», en FIGUEROA NAVARRO (dir.), *La cadena de custodia en el proceso penal,* Edisofer, Madrid, 2015, pp. 46 ss.; Además, en el ámbito de la lucha contra la delincuencia informática se desprende el problema de la dificultad añadida en la obtención de las fuentes de prueba tecnológica. En primer lugar, porque el propio modo de comisión de los hechos delictivos favorece la ocultación de la identidad de su autor. Pero también por las dificultades que supone la ausencia de regulación legal que facilite la lucha contra la ciberdelincuencia. *Vid.* ESPÍN LÓPEZ, «La cadena de custodia en el proceso penal. Propuestas en relación con el análisis y custodia de la prueba digital», *La Ley Penal*, núm. 151, 2021.

[19] GONZÁLEZ GRANDA/ARIZA COLMENAREJO, Justicia y proceso: una revisión procesal contemporánea bajo el prisma constitucional, Dykinson, Madrid, 2021, p. 466.

[20] ARRABAL PLATERO, *La prueba tecnológica: aportación, práctica y valoración*, Tirant lo Blanch, Valencia, 2019, pp. 35 ss. En definitiva, la noción de prueba tecnológica es más amplia. Por su parte, COLOMER HERNÁNDEZ afirma que el aspecto diferencial de la prueba tecnológica es la intervención de las nuevas tecnologías, ya sea en su formación o en su producción. Quiere decir el autor con esto que la afectación de la tecnología puede darse tanto en la constitución de la fuente de prueba como en el instrumento o medio a través del cual la fuente de prueba es conocida por el tribunal. *Vid.* COLOMER HERNÁNDEZ, «Prueba tecnológica», en GONZÁLEZ CANO (dir.), *La prueba en el proceso civil,* Tirant lo Blanch, Valencia, 2017, pp. 581 ss. También BELHADJ BEN GÓMEZ, «La prueba digital. Aspectos procesales», *Revista Derecho y Proceso*, núm. 3, 2023, pp. 29-45, hace un recorrido por los distintos caracteres que identifican la prueba digital, así como las cuestiones problemáticas a nivel procesal.

ARRABAL PLATERO, estas pueden identificarse con las siguientes: heterogeneidad, referida a la disparidad de posibilidades; fácil manipulación; huella digital, en relación con el rastro que toda actividad tecnológica produce, mediante los llamados metadatos; ubicuidad, referida a la transnacionalidad, en tanto que gran parte de las pruebas tecnológicas se generan, se desarrollan u obtienen en la red; media electrónica, en relación con el riesgo de que se generen identidades ficticias; y publicidad, característica que deriva directamente de aquellas pruebas que operan en internet y, en concreto, en redes abiertas[21]. Precisamente a consecuencia de su propia naturaleza, uno de los retos probatorios que han sido observados en materia de prueba tecnológica se identifica, sin duda, con el hecho de que la información que pretende acceder al proceso únicamente puede ser leída en un dispositivo tecnológico –dispositivo con capacidad de traducir la información desde el lenguaje informático a nuestro lenguaje natural, de modo que sea comprensible por su receptor[22]–, teniendo en cuenta asimismo que toda fuente de prueba ha de acceder al proceso a través de un concreto medio de prueba legalmente previsto en las leyes procesales. En definitiva, se trata de una fuente de prueba que, por su propia naturaleza, debe ser leída a través de un dispositivo electrónico y que, además, ha de respetar los mecanismos tradicionales de acceso al proceso[23].

Pero lo verdaderamente relevante en atención al concreto objeto de este trabajo, es el modo en que los caracteres propios de la prueba tecnológica afectan a la dimensión asimismo tecnológica de la figura de la cadena de custodia. Esta afectación deriva directamente de su característica de fácil manipulación y, en concreto, de la desconfianza que genera la prueba tecnológica en los diversos operadores jurídicos al observar su carácter mutable y alterable[24] y que conecta especialmente con la cadena de custodia[25]. Todo ello habrá de ser medido desde la perspectiva del aseguramiento de la prueba en relación con la garantía de su fiabilidad. En este sentido, tanto la jurisprudencia como la doctrina han dado el primer paso en la búsqueda de soluciones a los problemas planteados, sin que se haya alcanzado unanimidad al respecto o soluciones enteramente adecuadas, circunstancia compleja teniendo en cuenta que la casuística puede ser muy diferente en función del tipo de prueba tecnológica de que se trate y,

[21] ARRABAL PLATERO, *La prueba tecnológica: aportación, práctica y valoración,* Tirant lo Blanch, Valencia, 2019, pp. 41-54.

[22] GONZÁLEZ GRANDA/ARIZA COLMENAREJO, Justicia y proceso: una revisión procesal contemporánea bajo el prisma constitucional, Dykinson, Madrid, 2021, p. 467.

[23] Todo ello en un contexto en el que el papel cede ante el soporte tecnológico. Circunstancia que motiva especialmente la necesidad de determinar qué se entiende por documento electrónico. Al respecto, el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza de las transacciones electrónicas en el mercado interior (conocido como Reglamento eIDAS) recoge la definición de documento electrónico en su art. 3.35, entendiendo como tal «todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual». Pero, además, también se ha de concretar si es éste –el documento electrónico– es el modo de incorporar la prueba tecnológica al proceso. *Vid.* ABEL LLUCH, *La prueba electrónica*, J. M. Bosch, Barcelona, 2011; CASTILLEJO MANZANARES, «La prueba en el proceso penal: el documento electrónico», *Revista de Derecho Penal*, núm. 29, 2010, pp. 17 ss.

[24] VELASCO NÚÑEZ, *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*, Sepín, Madrid, 2015, p. 89.

[25] En atención a la necesidad de asegurarla a fin de evitar cualquier manipulación o alteración de su estado original. *Vid.* MESTRE DELGADO, «La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos», en FIGUEROA NAVARRO (dir.), *La cadena de custodia en el proceso penal,* Edisofer, Madrid, 2015, pp. 49 ss.; FALCIANI, «La prueba digital en el proceso civil: la cadena de la prueba», en FUENTES SORIANO (dir.), *Era digital, sociedad y Derecho*, Tirant lo Blanch, Valencia, 2020, pp. 371 ss., precisamente esta ausencia de fiabilidad en la prueba digital hace que el autor hable de la posibilidad de establecer una cadena de custodia similar a la penal en los demás órdenes jurisdiccionales.

fundamentalmente, teniendo en cuenta que el progreso tecnológico es constante. Éste es, en definitiva, el rasgo de la prueba tecnológica que mayor impacto tiene en la formulación de la cadena de custodia tecnológica.

2.2. En relación con el incremento de la ciberdelincuencia y la investigación tecnológica en el proceso penal

Una de las principales consecuencias de la sociedad digital se manifiesta en el surgimiento e incremento de la llamada ciberdelincuencia[26]. Aunque directamente atinente a la faceta propia del derecho penal sustantivo, el incremento de la ciberdelincuencia, como es lógico, incide asimismo en el plano procesal en conexión muy directa con la investigación tecnológica –y, en lo que aquí respecta, también tiene cierta repercusión en la dimensión tecnológica de la cadena de custodia–. Pero, antes de entrar en el análisis específico de la problemática que plantea en relación con la figura examinada, es conveniente delimitar el concepto de cibercrimen. Al respecto, la doctrina sostiene que integra el concepto de cibercrimen cualquier delito en el que las tecnologías de la información y las comunicaciones (en adelante TIC) desempeñan un papel determinante en su comisión (o, dicho de otro modo, cualquier delito cometido en el llamado ciberespacio)[27].

Examinar el fenómeno de la ciberdelincuencia exige hacer alusión al Convenio sobre el Cibercrimen (conocido como Convenio de Budapest)[28], teniendo en cuenta que, tal y como se expone en el propio preámbulo del referido Convenio, los Estados firmantes del mismo expresaban su convencimiento sobre la necesidad de aplicar «una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional». En tal sentido, la redacción del Convenio de Budapest viene motivada por el surgimiento de preocupaciones diversas en materia de ciberdelincuencia[29] que orientan los objetivos perseguidos, entre otros, hacia «dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, así como facilitar la obtención de pruebas electrónicas de los delitos», todo ello con respeto al debido equilibrio entre el ejercicio de la acción penal y los DDFF de los afectados.

De conformidad con lo expuesto en las líneas precedentes, el incremento de la ciberdelincuencia tiene una repercusión directa en el auge de la investigación y prueba tecnológica y conecta directamente con la formulación de la cadena de custodia desde su vertiente tecnológica. Plantear la temática de la investigación tecnológica en nuestro ordenamiento jurídico fuerza la necesidad de mencionar la Ley Orgánica (en adelante LO)

[26] El incremento de la ciberdelincuencia en nuestro país ha sido reflejado en el Informe sobre la cibercriminalidad en España del año 2023. Puede consultarse en el siguiente enlace: https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Informe-Cibercriminalidad_2023.pdf.

[27] MIRÓ LLINARES, *El cibercrimen: fenomenología y criminología de la ciberdelincuencia en el ciberespacio*, Marcial Pons, Madrid, 2012, p. 44.

[28] 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.

[29] Entre otras, preocupaba a los Estados firmantes del Convenio de Budapest el «riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes».

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 como punto de referencia. La promulgación de la citada LO a finales del año 2015, situó España a la «vanguardia legislativa»[30], pues hasta entonces nuestro ordenamiento jurídico destacaba por la insuficiencia normativa en materia de investigación tecnológica[31], contando únicamente con un precepto al respecto en toda la LECrim. Ahora bien, como paso previo, la firma del Convenio de Budapest 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[32]. 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 (de cara a evitar los riesgos derivados del carácter intangible y volátil de los datos que circulan por el ciberespacio), 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[33], impacto que se concreta en el debido 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 son, en concreto, los siguientes: especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad (art. 588 bis a LECrim)[34]. 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[35]. En tercer lugar, en

[30] BUENO DE MATA, *Las diligencias de investigación penal en la cuarta revolución industrial: principios teóricos y problemas prácticos*, Aranzadi, Navarra, 2019, p. 17.

[31] FUENTES SORIANO, «La intervención de las comunicaciones tecnológicas tras la reforma de 2015» En ALONSO-CUEVILLAS SAYROL (dir.), *El nuevo proceso penal tras las reformas de 2015*, Atelier, Barcelona, 2016, pp. 261-262.

[32] ORTIZ PRADILLO, *Problemas procesales de la ciberdelincuencia*, Colex, A Coruña, 2013, pp. 76-80; CUADRADO SALINAS, «La obtención de pruebas electrónicas transfronterizas: nuevos retos y nuevas consideraciones desde la perspectiva de la Unión Europea», en ASENCIO MELLADO (dir.), *Derecho probatorio y otros estudios procesaler. Liber Amicorum: Vicente Gimeno Sendra*, Ediciones Jurídicas Castillo de Luna, Madrid, 2020, pp. 519 ss.

[33] RICHARD GONZÁLEZ, «La investigación y prueba de hechos y dispositivos electrónicos», *Revista General de Derecho Procesal*, núm. 43, 2017.

[34] 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. *Vid.* GARCIMARTÍN MONTERO, *Los medios de investigación tecnológicos en el proceso penal,* Aranzadi, Navarra, 2018, p. 29; ROCA MARTÍNEZ, «Nuevas tecnologías e investigación penal: garantías ante injerencias y motivación de su autorización», en FERNÁNDEZ VILLALÓN, *Derecho y nuevas tecnologías,* Civitas, Navarra, 2020, pp. 710 ss.

[35] Distintos autores han reconocido la utilidad de la medida como elemento identificador del principio de idoneidad. Al respecto, SÁNCHEZ MELGAR, «La nueva regulación de las medidas de investigación tecnológica. Estudio de su parte general», *Práctica penal: cuaderno jurídico*, núm. 82, 2016, pp. 20 ss.; GARCIMARTÍN MONTERO,

cuanto a los principios de excepcionalidad y necesidad el legislador los 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)[36]. Finalmente, el principio de proporcionalidad se regula en el art. 588 bis a 5 LECrim y se cumple cuando la injerencia en 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[37]. 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. Específicamente, lo anterior genera un impacto en la vertiente material de la cadena de custodia tecnológica, pues alude a especificidades que condicionan el correcto desarrollo de esta vertiente, en tanto que las investigaciones tecnológicas han de desarrollarse con especial atención a los principios expuestos.

2.3. 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. Y es que suele ocurrir que el contenido de los dispositivos tecnológicos se vincula directamente con los DDFF de las personas, siendo ésta la razón por la que la protección de ciertos DDFF cobra una relevancia

Los medios de investigación tecnológicos en el Proceso Penal, Aranzadi, Navarra, 2018, pp. 34 ss.; DELGADO MARTÍN, *Investigación tecnológica y prueba digital en todas las jurisdicciones*, 2ª ed., La Ley, Madrid, 2018, p. 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, «Las medidas de investigación tecnológica», en CEDEÑO HERNÁN (coord.), *Nuevas tecnologías y Derechos Fundamentales en el proceso*, Aranzadi, Navarra, 2017, pp. 22 ss.

[36] 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, *Investigación sobre equipos informáticos y su prueba en el proceso penal*, Aranzadi, Navarra, 2021, pp. 44 y ss.). En cambio, la otra vertiente doctrinal defiende la unificación de ambos principios en uno (GARCIMARTÍN MONTERO, *Los medios de investigación tecnológicos en el Proceso Penal*, Aranzadi, Navarra, 2018, p. 36; DELGADO MARTÍN, *Investigación tecnológica y prueba digital en todas las jurisdicciones*, 2ª ed., La Ley, Madrid, 2018, p. 371), entendiendo el principio de excepcionalidad como un principio de subsidiariedad ESPÍN LÓPEZ, *Investigación sobre equipos informáticos y su prueba en el proceso penal*, Aranzadi, Navarra, 2021, p. 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, *Investigación tecnológica y prueba digital en todas las jurisdicciones*, 2ª ed., La Ley, Madrid, 2018, p. 371). De modo similar, BUENO DE MATA sostiene que ambos principios han de ser interpretados de manera complementaria. *Vid.* BUENO DE MATA, *Las diligencias de investigación penal en la cuarta revolución industrial: principios teóricos y problemas prácticos,* Aranzadi, Navarra, 2019, p. 36.

[37] BUENO DE MATA, *Las diligencias de investigación penal en la cuarta revolución industrial: principios teóricos y problemas prácticos,* Aranzadi, Navarra, 2019, pp. 37-38. Además, como expone el autor, estos principios se encuentran desarrollados por parte de la Fiscalía General del Estado en su Circular 1/2019.

significativa en materia de cadena de custodia tecnológica. Ahora bien, es importante distinguir entre aquellos DDFF –de contenido procesal, en este caso– que guardan relación con la configuración de la cadena de custodia en sí misma[38] (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 ya no afectan al contenido procesal de la cadena de custodia y son el derecho a la protección de datos personales del art. 18.4 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[39].

En relación con el derecho fundamental a la protección de datos personales[40], en primer lugar, lo fundamental reside en el reconocimiento al interesado de un régimen de control y disposición sobre sus datos personales[41], 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[42]. 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 Tribunal Constitucional (en adelante STC) 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,

[38] Como, por ejemplo, el vínculo que mantiene con el derecho a un proceso con todas las garantías, en virtud del cual es posible apreciar vulneración de este derecho a consecuencia de la actuación del tribunal sentenciador. Para que se produzca la injerencia, es preciso que el tribunal sentenciador valore como prueba de cargo una cuya cadena de custodia adolezca de las garantías necesarias, debiendo haberse probado la ruptura de la cadena de custodia por infracción grave de la misma. Así se desprende de la STC 170/2003, de 29 de septiembre; y STC 281/2006, de 9 de octubre.

[39] MESTRE DELGADO, «La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos», en FIGUEROA NAVARRO, *La cadena de custodia en el proceso penal,* Edisofer, Madrid, 2015, p. 50.

[40] En los últimos años, se han ido produciendo diversos avances legislativos en materia de protección de datos, tanto en el seno de la UE 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.

[41] VELASCO NÚÑEZ, «Investigación penal y protección de datos», *El cronista social y democrático de Derecho,* núm. 88-89, 2020.

[42] COLOMER HERNÁNDEZ, «Limitaciones en el uso de la información y los datos personales en un proceso penal digital», en ARANGÜENA FANEGO/DE HOYOS SANCHO/PILLADO GONZÁLEZ (dirs.), *El proceso penal ante una nueva realidad tecnológica europea,* Aranzadi, Navarra, 2023, pp. 40 ss.; PÉREZ GIL, «Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal», en JIMÉNEZ CONDE/BELLIDO PENADÉS (dirs.), *Justicia: ¿garantías versus eficiencia?*, Tirant lo Blanch, Valencia, 2019, p. 431.

la facultad otorgada por el derecho a la intimidad[43] 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[44] –que ha sido desarrollado por el TC– y, en concreto, la cobertura que ofrece se extiende a la interceptación de las comunicaciones 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 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[45]. Esto es, 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.

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 tratarse de un supuesto de prueba prohibida), por lo que no será necesario examinar la cadena de custodia. Dicho de otro modo, el especial cuidado que hay que poner durante el desarrollo de la cadena de custodia tecnológica a fin de evitar la vulneración de ciertos DDFF afecta al desarrollo de la vertiente material de la cadena de custodia (en el sentido de que el desarrollo de las diferentes guías o protocolos de actuación habrá de tener especial cuidado de formular actos respetuosos con estos DDFF), en tanto que si se produce la efectiva vulneración de derecho fundamental nos encontramos ya en el terreno de las exclusiones probatorias y no podremos entrar a valorar la cadena de custodia, pues la prueba habrá de ser excluida del proceso.

3. La configuración de la cadena de custodia tecnológica

3.1. La formulación de las vertientes formal y material

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 vertiente 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

[43] El derecho a la intimidad está reconocido en el art. 18.1 CE y, asimismo, en el art. 8 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.

[44] Art. 18.3 CE y 8 CEDH, entre otros textos de protección internacional.

[45] 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.

verosimilitud de la prueba y, por tanto, determinante en su valoración[46]. Es por ello por lo 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 se desprenden, en efecto, de la naturaleza procesal de la cadena de custodia. 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 primero de ellos –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[47]. 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[48]. Ahora bien, la mismidad de la prueba no puede entenderse sino en

[46] Muy en sintonía con la formulación jurisprudencial de la cadena de custodia como sistema formal de garantía de la mismidad de la prueba: STS 587/2014, de 18 de julio, ECLI:ES:TS:2014:3086; STS 1012/2024, de 13 de noviembre, ECLI:ES:TS:2024:5536; SAP LE 541/2017, de 12 de diciembre, ECLI:ES:APLE:2017:1387; SAP B 793/2024, de 23 de octubre, ECLI:ES:APB:2024:14935.

Y es que no debemos olvidar que se concreta como una figura de carácter instrumental (STS 1190/2009, de 3 de diciembre, ECLI:ES:TS:2009:7710; STS 129/2011, de 10 de marzo, ECLI:ES:TS:2011:1308; STS 1/2014, de 21 de enero, ECLI:ES:TS:2014:53; SAP V 310/2015, de 30 de marzo, ECLI:ES:APV:2015:1944; SAP GR 23/2018, de 26 de enero, ECLI:ES:APGR:2018:256; SAP AV 69/2022, de 2 de junio, ECLI:ES:APAV:2022:159) que no goza de valor probatorio, siendo su objetivo el de garantizar la mismidad de la fuente de prueba desde que es recogida hasta que es analizada; en segundo lugar, no siendo prueba en sí misma, se configura como un presupuesto de fiabilidad y no de validez y, por consiguiente, afecta a la llamada verosimilitud de la prueba (SAP B 132/2009, de 25 de febrero, ECLI:ES:APB:2009:1719; SAP M 70/2011, de 14 de julio, ECLI:ES:APM:2011:9546; SAP BI 17/2013, de 20 de marzo, ECLI:ES:APBI:2013:2054; STS 777/2013, de 7 de octubre, ECLI:ES:TS:2013:5677; SAP TF 325/2014, de 7 de julio, ECLI:ES:APTF:2014:1112; STS 726/2017, de 8 de noviembre, ECLI:ES:TS:2017:3957; STS 1026/2021, de 17 de marzo, ECLI:ES:TS:2021:978; entre otras), en tercer lugar, y partiendo de la premisa de que la cadena de custodia se manifiesta como una sucesión de actos desde la obtención de la fuente de prueba y hasta su incorporación como prueba al juicio oral, nace el deber (subsanable) de documentación del recorrido seguido por la fuente de prueba (SAP B 132/2009, de 25 de febrero, ECLI:ES:APB:2009:1719) y, en último término, la irregularidad de la cadena de custodia no implica, por sí misma, ni vulneración de DDFF ni ilicitud de la prueba (STS 587/2014, de 18 de julio, ECLI:ES:TS:2014:3086, entre otras).

[47] En virtud de la STS 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».

[48] 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

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[49]. 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 cadena de custodia[50]. 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*[51], como su propia literalidad indica, hace referencia al correcto desarrollo de la cadena de custodia[52]. A nivel jurídico significa que no ha habido problemas procesales en su desarrollo y,

---

ignorado las cuestiones inherentes a esta mismidad, sino que han acudido a éstas a través de otros términos (autenticidad, identidad, integridad, inalterabilidad, indemnidad, inmutabilidad o incolumidad acostumbran a ser los más comunes). Entre otros, podemos citar a GUTIÉRREZ SANZ quien alude a términos como 'identidad' o 'indemnidad' (GUTIÉRREZ SANZ, *La cadena de custodia en el proceso penal español*, Civitas, Navarra, 2016, p. 30); FIGUROA NAVARRO hace referencia a la 'identidad', la 'integridad' y la 'autenticidad' (FIGUEROA NAVARRO, «El aseguramiento de las pruebas y cadena de custodia», *La Ley Penal,* núm. 84, 2011); RICHARD GONZÁLEZ se decanta por los términos 'autenticidad', 'inalterabilidad' e 'indemnidad' (RICHARD GONZÁLEZ, «La cadena de custodia en el proceso penal», *Diario la Ley,* núm. 8187, 2013); o DEL POZO PÉREZ quien, por su parte, emplea los conceptos 'identidad', 'integridad' y 'autenticidad' (DEL POZO PÉREZ, Marta, *Diligencias de investigación y cadena de custodia*, Sepín, Madrid, 2014).

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

[50] 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, 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. Éste es el caso de GARCÍA MATEOS, «Cadena de custodia vs. mismidad», en OLIVA LEÓN/VALERO BARCELÓ (coords.), *La prueba electrónica: validez y eficacia procesal,* Editorial Juristas con futuro, Madrid, 2016, pp. 131 ss.

[51] Expresión introducida jurisprudencialmente por la STS 1587/2001, de 11 de septiembre, ECLI:ES:TS:2001:6733.

[52] 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. *Vid.* GUTIÉRREZ SANZ, *La cadena de custodia en el proceso penal español,* Civitas, Navarra, 2016, pp. 61 ss. Ahora bien, la normativa a la que alude la autora hace referencia esencialmente a la

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[53], oportuno es destacar que acreditar su corrección es, en principio, innecesario para las partes procesales[54]. 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).

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 por lo 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[55].

---

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–.

[53] Se trata de una característica que la jurisprudencia ha ido anunciado y exponiendo a lo largo de los años: SAP M 217/2003, de 7 de marzo, ECLI:ES:APM:2003:2979; SAP M 785/2009, de 6 de julio, ECLI:ES:APM:2009:8425; SAP M 1492/2009, de 30 de noviembre, ECLI:ES:APM:2009:15479. De forma similar, la SAP V 19/2001, de 3 de mayo, ECLI:ES:APV:2001:2731, recoge esta presunción de veracidad.

[54] ÁLVAREZ DE NEYRA KAPPLER, «La cadena de custodia en materia de tráfico de drogas», en FIGUEROA NAVARRO (dir.), *La cadena de custodia en el proceso penal*, Edisofer, Madrid, 2015, p. 83.

[55] 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, *Diligencias de investigación y cadena de custodia*, Sepín, Madrid, 2014; GARCÍA DE YÉBENES/GASCÓ ALBERCHI, «La cadena de custodia de muestras relacionadas con presuntos ilícitos contra el medio ambiente», en FIGUEROA NAVARRO (dir.), *La cadena de custodia en el proceso penal*, Edisofer, Madrid, 2015, p. 130; CAMPOS, «La relevancia de la cadena de custodia en la investigación judicial», *Medicina legal de Costa Rica*, vol. 19, núm. 1, 2022, pp. 75

Es fundamental la diferenciación entre ambas vertientes (formal y material) para comprender la cadena de custodia en toda su amplitud. Con esta clasificación se pretende poner el acento en la delimitación de los elementos que integran el contenido procesal de la cadena de custodia como figura jurídica autónoma. Así, integran la vertiente formal aquellos elementos que condiciona su significado (el de la cadena de custodia) en el proceso, mientras que la vertiente material implica la individualización de los actos que, aun con significación procesal, no integran el contenido procesal de la cadena de custodia, sino que componen la parte más procedimental de la misma y que se producen desde la obtención de la prueba y hasta su incorporación.

3.2. 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 el punto anterior, son tres los aspectos esenciales a valorar en el desarrollo de la vertiente formal 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.

a. La corrección de la cadena de custodia tecnológica y la mismidad de la prueba

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 de carácter tecnológico 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 todo, en virtud de su carácter volátil y su presunta fácil manipulación[56]–. 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[57]. Pero, además, esta confianza continúa en

ss.); por otro lado, otras posturas ilustran actos con un carácter menos procedimental y más procesal (GUTIÉRREZ SANZ, *La cadena de custodia en el proceso penal español,* Civitas, Navarra, 2016, pp. 61 ss.).

[56] 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/ARIZA COLMENAREJO, *Justicia y proceso: una revisión procesal contemporánea bajo el prisma constitucional,* Dykinson, Madrid, 2021, pp. 484 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 (entre ellos, SÁNCHEZ RUBIO, «Cadena de custodia y prueba electrónica: la mismidad del hash como requisito para la fiabilidad probatoria», en BUENO DE MATA (dir.), *FODERTICS 7.0: estudios sobre derecho digital*, Comares, Granada, 2019, p. 289).

[57] 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

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[58]. 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[59]. 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[60]. Y ésta es, sin duda, la visión que se defiende en este trabajo: es fundamental regular la cadena de custodia tradicional, 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[61]. 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[62]– 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

posibilidad de alteración de las pruebas de carácter tecnológico, lo cierto es que esta circunstancia también ocurre en las pruebas más tradicionales. *Vid.* ARRABAL PLATERO, *La prueba tecnológica: aportación, práctica y valoración*, Tirant lo Blanch, Valencia, 2019, p. 45.

[58] Esta circunstancia se concreta muy en particular respecto de la posibilidad de valerse de una 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.

[59] Diferencia fundamental con respecto a, por ejemplo, los análisis periciales efectuados por organismos oficiales.

[60] 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, «La cadena de custodia en el proceso penal. Propuestas en relación con el análisis y custodia de la prueba digital», La Ley penal, núm. 151, 2021).

[61] ARELLANO/CASTAÑEDA, «La cadena de custodia informático-forense», *Cuadernos informático-forense*, núm. 3, 2012, pp. 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.

[62] 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.

en presencia de un fedatario público –ya se sea un notario o ante el Letrado de la Administración de Justicia–[63], de modo que el fedatario sea quien garantice el contenido de dicha fuente de prueba electrónica, dando fe del contenido de la misma[64]. Si bien la posición más compartida –y coincido– sostiene que la pericial informática[65] 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[66].

b. La impugnación de la cadena de custodia tecnológica y carga de la 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

[63] Ejemplo de ello es el AAP M 712/2023, de 26 de abril, ECLI:ES:APM:2023:3237A, en el que se recoge un protocolo para conceder valor probatorio a los mensajes de mensajería instantánea (redacto por el Auto de la AP GU 328/2018, de 30 de noviembre): en primer lugar, indica la AP que se habrá de aportar el dispositivo electrónico que contenga la aplicación de mensajería instantánea a fin de garantizar la cadena de custodia, en segundo lugar, transcripción del contenido de los mensajes; en tercer lugar, cotejo por el Letrado de la Administración de Justicia (si bien también alude a la posibilidad de efectuar el volcado por parte de un perito informático, introduciéndose en tal caso al proceso como prueba pericial); y, finalmente, lectura del contenido de los mensajes en el juicio oral. Llama la atención la solución expuesta en la STSJ AND 2807/2024, de 10 de octubre, ECLI:ES:TSJAND:2024:14637 (que se dicta a causa de un procedimiento seguido en el orden jurisdiccional social), en aras a acreditar la cadena de custodia se procede al vaciado de los datos contenidos en un sistema informático por parte de un perito informático y en presencia de un notario, de modo que conjugan los dos sistemas expuestos.

[64] 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». *Vid.* CALAZA LÓPEZ/MUINELO COBO, «La digitalización y custodia de la prueba pericial electrónica sobre evidencias virtuales», en PICÓ I JUNOY (dir.), *La prueba pericial a examen: propuestas de lege ferenda,* J. M. Bosch, Barcelona, 2020, pp. 473 ss.

[65] 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, «El valor probatorio de la información contenida en un dispositivo tecnológico», en BUJOSA VADELL (dir.), *Derecho procesal: retos y transformaciones*, Atelier, Barcelona, 2021, p. 536); CALAZA LÓPEZ sostiene que la pericial informática puede servir para acreditar la autenticidad e integridad de la prueba electrónica CALAZA LÓPEZ, «Cadena de custodia y prueba tecnológica», en VILLEGAS DELGADO/MARTÍN RÍOS (dirs.), *El derecho en la encrucijada tecnológica: estudios sobre derechos fundamentales, nuevas tecnologías e inteligencia artificial*, Tirant lo Blanch, Valencia, 2022, pp. 39 ss. En el mismo sentido, SANJURJO RÍOS, «Proceso penal y volatilidad/mutabilidad de las fuentes de prueba electrónicas: sobre la conveniencia y el modo de asegurarlas eficazmente», en GONZÁLEZ GRANDA (dir.), *Exclusiones probatorias en el entorno de la investigación y prueba electrónicas*, Reus, Madrid, 2020, p. 206; MARTÍNEZ GALINDO, «Problemática jurídica de la prueba digital y sus implicaciones en los principios penales», *Revista Electrónica de Ciencia Penal y Criminología*, núm. 24, 2022. También FUENTES SORIANO, «El valor probatorio de los correos electrónicos», en ASENCIO MELLADO (dir.), *Justicia penal y nuevas formas de delincuencia*, Tirant lo Blanch, Valencia, 2017, pp. 202 ss., en relación con la forma de acreditar la autenticidad de un correo electrónico; o RUBIO ALAMILLO, quien alude a la importancia de que el perito firmante sea informático RUBIO ALAMILLO, «Cadena de custodia y análisis forense de smartphones y otros dispositivos móviles en procesos judiciales», *Diario la Ley*, núm. 9300, 2018. Aunque no en relación con la acreditación de la mismidad en concreto, también DE URBANO CASTRILLO expone la conveniencia de la pericia informática DE URBANO CASTRILLO, Eduardo, *La valoración de la prueba electrónica*, Tirant lo Blanch, Valencia, 2009, p. 69.

[66] Es importante resaltar que ésa y no otra ha de ser la finalidad del perito informático, de modo que el informe pericial no debe contener valoraciones jurídicas sobre la apreciación de la prueba. Así lo expone la SAP CE 51/2022, de 27 de junio, ECLI:ES:APCE:2021:67.

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[67]–. Con todo, en el caso de la prueba tecnológica las preocupaciones se centran 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, orbita la cuestión 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 estas[68]. Al hilo de esto y una vez impugnada la prueba de carácter tecnológico[69], la consecuencia estriba en que se ha de acreditar su autenticidad[70] para alcanzar la confianza del juzgador[71]. 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 ha sido impugnada, supone una matización a la presunción de veracidad de la cadena de custodia en el terreno tecnológico. La excepción a esta 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[72].

---

[67] JAMARDO LORENZO, «La cadena de custodia: configuración jurídica y estado actual de la cuestión», *Justicia: revista de derecho procesal,* núm. 1, 2024.

[68] PÉREZ DAUDÍ, «La prueba electrónica: naturaleza jurídica e impugnación», en ASENCIO MELLADO (dir.), *Derecho probatorio y otros estudios procesales. Liber Amicorum: Vicente Gimeno Sendra*, Ediciones Jurídicas Castillo de Luna, Madrid, 2020, pp. 1560 ss.

[69] Señala ESPÍN LÓPEZ que no hay previsión normativa al respecto, sin embargo, ésta podrá ser impugnada al igual que cualquier otra prueba. *Vid*. ESPÍN LÓPEZ, *Investigación sobre equipos informáticos y su prueba en el proceso penal*, Aranzadi, Navarra, 2021, p. 270.

[70] 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. Al respecto de la impugnación de la prueba tecnológica, afirma la autora 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 SÁNCHEZ RUBIO, al contrario de lo que ocurre con la prueba tradicional, será la parte contraria quien deba probar la ausencia de fiabilidad de la prueba. Una vez más, esta cuestión deriva directamente de la falta de confianza en este tipo de pruebas. *Vid.* SÁNCHEZ RUBIO, «Cadena de custodia y prueba electrónica: la mismidad del hash como requisito de fiabilidad probatoria», en BUENO DE MATA (dir.), *FODERTICS 7.0: estudios sobre derecho digital,* Comares, Granada, 2019, pp. 292 ss.

[71] 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, *La prueba tecnológica: aportación, práctica y valoración*, Tirant lo Blanch, Valencia, 2019, pp. 335 ss.).

[72] La SAN 22/2024, de 13 de noviembre, ECLI:ES:AN:2024:5955, pone de relieve justamente esta matización. Si bien se sigue hablando de que no es suficiente únicamente con alegar las irregularidades, sino que se deba aportar algún dato objetivo del que poder deducir la falta de autenticidad de los elementos informáticos (como así recuerda la STS 14 de octubre de 2020, ECLI:ES:TS:2020:3191), también enfatiza la necesidad de activar ciertas salvaguardas en aras a una adecuada valoración de su fiabilidad.

Finalmente, tiene interés el Dictamen 1/2016 de la unidad de Criminalidad Informática de la Fiscalía General del Estado, 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 de prueba de comunicaciones electrónicas[73]. Al respecto, la postura de la Fiscalía General del Estado 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[74].

c. La fiabilidad y valoración 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 ha 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 apreciar o no la prueba. Dicho de otro modo, la valoración de la prueba no se asienta en la formulación de una ciencia exacta y, por ende, la verosimilitud de una prueba no puede o debe descansar única y exclusivamente en la fiabilidad del concreto medio de prueba, sino –necesariamente– en la fiabilidad que se desprende de la valoración de la actividad probatoria en su conjunto.

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[75], 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

[73] 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.

[74] Muy en sintonía con lo expuesto en texto, la STS 403/2024, de 16 de mayo, ECLI:ES:TS:2024:2570, rechaza la impugnación de la cadena de custodia de una prueba tecnológica al entender que no hay base suficiente en los motivos alegados por la defensa para generar desconfianza sobre la integridad de la prueba. Similar enfoque ofrece la STS 332/2019, de 27 de junio, ECLI:ES:TS:019:2205, donde además se expone la relevancia de las aclaraciones efectuadas por los peritos informáticos en relación con las presuntas deficiencias que, en opinión de la defensa, presentaban las pruebas tecnológicas. Precisamente las explicaciones de los peritos informáticos han servido para reforzar la desestimación del motivo de casación en el que se planteaba la ruptura de la cadena de custodia. También la SAP M 737/2024, de 27 de noviembre, ECLI:ES:APM:2024:13164.

[75] MERKEL, Derechos humanos e investigaciones policiales. Una tensión constante, Marcial Pons, Madrid, 2022, p. 97.

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.

3.3. El alcance de la vertiente material de la cadena de custodia tecnológica

Siguiendo el esquema de la vertiente material expuesto anteriormente, el primer acto material de la cadena de custodia –hallazgo y obtención de las evidencias– alude a la localización 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 y a su obtención. Obtenida la fuente de prueba material, se inicia la cadena de custodia y, en consecuencia, deben respetarse las actuaciones necesarias para garantizar la protección 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 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.

Igualmente pasa con su conservación, 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 –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 y en relación 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 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[76] 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 LEC). 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 la valoración de la prueba tecnológica en el 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[77]. 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.

A propósito de la reglamentación de la vertiente material de la cadena de custodia, quizá una de las normas reglamentarias más completas, a pesar de su ámbito de aplicación ciertamente limitado, sea la Orden JUS/1291/2010, de 13 mayo, por la que se aprueban las normas para la preparación y remisión de muestras objeto de análisis por el Instituto Nacional de Toxicología y Ciencias Forenses[78]. Lo completo de esta orden deriva de la exhaustividad y detalle con que se recogen las exigencias procedimentales para todas aquellas personas que intervienen en la cadena de custodia en su concreto ámbito de actuación. Además, en palabras de CABEZUDO BAJO, esta norma recoge gran parte de los aspectos de carácter científico-tecnológico que inciden en la obtención de las muestras de ADN[79]. Otra norma dictada a propósito de las muestras de ADN es la norma ISO/IEC 17025:2017, que recoge ciertas previsiones para el contexto de los laboratorios de análisis de ADN. Otro de los ejemplos que contamos en nuestro ordenamiento jurídico, en relación con la normativización de la vertiente material de la cadena de custodia, es 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. Este manual está específicamente dirigido a la

[76] 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. *Vid.* LÓPEZ VALERA, «Localización, hallazgo y recogida de muestras de ADN en la cadena de custodia», *Revista de Derecho UNED,* núm. 19, 2016, pp. 799-808.

[77] MARTÍN RÍOS, «Problemas de admisibilidad de la prueba obtenida de dispositivos de almacenamiento digital», *Revista General de Derecho Procesal,* núm. 51, 2020.

[78] Esta orden del Ministerio de Justicia nace con la vocación de actualizar a su predecesora del año 1996 (la Orden del Ministerio de Justicia de 8 de noviembre de 1996 por la que se aprueban las normas para la preparación y remisión de muestras objeto de análisis por el Instituto de Toxicología), ahora derogada. En esta orden ministerial ya se aludía a la cadena de custodia, incluso a pesar del contexto temporal, en los siguientes términos: «Debe existir un documento anejo al envío de muestras, que acredite la observación en todo momento de la 'cadena de custodia', desde la toma de muestras hasta su recepción en el INT. Se propone como modelo el que figura incluido como anexo (…) pudiendo ser válido cualquier otro documento, siempre que quede constancia firmada de todas las personas bajo cuya responsabilidad hayan estado las muestras», todo ello en relación con la documentación preceptiva para la remisión de las muestras objeto de análisis por parte del Instituto Nacional de Toxicología.

[79] CABEZUDO BAJO, *Propuestas para una regulación armonizada de la obtención de la prueba de ADN como prueba científica-tecnológica de probabilidad en el proceso penal*, Aranzadi, Navarra, 2017, pp. 95 ss.

policía judicial y los peritos especializados en criminalística. En síntesis, establecen unos puntos mínimos que han de cubrir para garantizar el respeto a la cadena de custodia y unas 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. Sin embargo, en ninguno de los casos señalados se incorporan previsiones específicas en relación con la cadena de custodia tecnológica, aunque de manera justificada en las dos primeras dado el concreto ámbito material en el que se encuadran.

En el contexto comparado sí encontramos, en cambio, diversos ejemplos de reglamentación de la vertiente material de la cadena de custodia tecnológica en ordenamientos jurídicos ajenos. Ejemplo de ello es el ordenamiento jurídico de Estados Unidos (en adelante EEUU). Si bien es cierto que no existe norma específica que regule su admisibilidad, sí existe, no obstante, diversos manuales prácticos al efecto[80]. En concreto, el más destacado es el *Electronic crime scene investigation: a guide for first responders*[81], redactado por el Departamento de Justicia. En este manual, se recoge el marco general en relación con la obtención, aseguramiento y transporte de pruebas digitales y que va dirigido a todos los intervinientes en la investigación y que mantienen contacto con las pruebas digitales. Tal y como expone el propio manual, el tratamiento de la prueba digital debe regirse por los siguientes principios: primero, que los procesos de recolección, aseguramiento y transporte de prueba digital no pueden alterar la propia prueba; segundo, que la prueba digital debe ser examinada únicamente por aquellos capacitados específicamente para ello; y tercero, que todo lo realizado durante la incautación, transporte y almacenamiento de la prueba digital debe ser enteramente documentado, preservado y encontrarse disponible para su análisis. En concreto, hace referencia específica al mantenimiento de la cadena de custodia durante el procedimiento de traslado de las pruebas digitales que hayan sido obtenidas, debiendo igualmente documentar todas las actuaciones que se lleven a cabo durante dicho transporte. Además, muestra su preocupación al respecto de la intromisión en los datos personales de los ciudadanos que pueda producirse a consecuencia de la incautación u obtención de las pruebas digitales objeto de tratamiento en este manual. En concreto, alude a la posibilidad de vulnerar normas tales como el *Electronic Communications Privacy Act* (1986) y el *Privacy Protection Act* (1980).

Otro ejemplo lo encontramos en el ordenamiento jurídico mexicano, donde cobra especial interés el Acuerdo General del Pleno del Consejo de la Judicatura Federal[82], por el que se aprueba el Protocolo de actuación para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales. En este acuerdo y a lo largo de los diversos considerandos del texto, se exponen las inquietudes que genera el respeto a la cadena de custodia en el plano tecnológico. Al respecto, en el considerando sexto se afirma que «con el auge de las tecnologías de la información, es necesario proporcionar métodos y procedimientos que aseguren la detección, recolección, manejo, autentificación, análisis, procesamiento y resguardo de los recursos informáticos y/o evidencias digitales» que hayan sido obtenidos, en general, de cualquier dispositivo de comunicación, almacenamiento y transmisión de datos –incluyendo una

[80] SIMARRO PEDREIRA, «La cadena de custodia en la prueba digital: España vs. EEUU», en GONZÁLEZ GRANDA (dir.), *Exclusiones probatorias en el entorno de la investigación y prueba electrónica*, Reus, 2020, pp. 235 y ss.

[81] Documento que puede ser consultado en la siguiente página web: https://www.ojp.gov/pdffiles1/nij/219941.pdf.

[82] Publicado en el Diario Oficial de la Federación el día 17 de junio del 2016.

enumeración, a modo ilustrativo, de algunos de estos dispositivos–. A continuación, el considerando séptimo expone:

> «La obtención de información (elementos de prueba) constituye una de las facetas útiles dentro del éxito de una investigación, aspecto que demanda de los encargados de la recolección, preservación, análisis y presentación de las evidencias, una eficaz labor que garantice la autenticidad e integridad de estas, a fin de ser utilizadas posteriormente como parte de los diversos procedimientos que se tramitan en el Consejo de la Judicatura Federal y/o en su caso ante las autoridades ministeriales o judiciales correspondientes».

Mientras que, por su parte, el considerando octavo añade:

> «Uno de los principales problemas en el análisis de la evidencia digital entendida como información probatoria almacenada o transmitida digitalmente, es la cadena de custodia, es decir, el procedimiento controlado que se aplica a los indicios materiales relacionados con la investigación desde su localización hasta su valoración y que tiene como fin no viciar el manejo que de ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones».

El protocolo se divide en once fases y finaliza con la introducción de un glosario, seguido de los transitorios. Las fases de la evidencia que reconoce el protocolo son las siguientes: procedencia (I); inspección, detección, aseguramiento y documentación (II); recolección (III); registro (IV); embalaje (V); traslado y entrega para análisis (VI); desembalaje (VII); análisis e informes (VIII); almacenamiento en el lugar de resguardo (IX); traslado para la presentación de los recursos informáticos y/o evidencia digital como material probatorio (X); y destino final (XI). En cada una de estas fases el protocolo alude al responsable de la misma y a las actividades propias que se desarrollarán en concreto. En opinión de MANSILLA MOYA el procedimiento de la cadena de custodia de la evidencia digital es esencialmente equivalente al seguido para los demás indicios materiales, con la singularidad de que el personal responsable de las etapas cuyo objeto es el *hardware* será el personal autorizado por la Dirección General de las Tecnologías de la Información, independientemente de su adscripción, «con la finalidad de que sean personas expertas quienes manejen los indicios probatorios para evitar la pérdida o contaminación de los mismos»[83]. Y en tal sentido, señala que se ha de diferenciar entre el *hardware* y el *software*, exponiendo el autor que el *hardware* es «el elemento material de un sistema informático», identificándolo con los recursos informáticos; mientras que el *software* es «la información contenida» en el dispositivo y lo identifica con la evidencia digital[84].

No podemos dejar de mencionar la Tesis Aislada I.2o.P.49 P (10a.) del Segundo Tribunal Colegiado del Primer Circuito en materia penal, derivada del Amparo directo 97/2016, de 11 de agosto de 2016, y que, además, fue dictada poco tiempo después de la aprobación del citado Acuerdo. En relación con la prueba tecnológica, el tribunal establece como criterios de validez de la prueba derivada comunicaciones electrónicas, por un lado, haber sido obtenida lícitamente y, por otro, que la cadena de custodia se haya respetado. Al efecto, el tribunal

[83] MANSILLA MOYA/MANSILLA MOYA, «Cadena de custodia 2.0», *Revista Mexicana de Ciencias Penales,* Vol. 5, núm. 18, 2022, p. 57.

[84] Ibidem.

expone para constatar la veracidad tanto del origen como del contenido de la evidencia digital, es necesario que se cumplan los registros de cadena de custodia en aras a satisfacer el principio de mismidad perseguido por ésta, lo que se traduce en que el contenido de la fuente digital sea el mismo que el aportado al proceso. Afirma el tribunal que esta exigencia deriva del carácter fácilmente manipulable o alterable de este tipo de evidencias, sosteniendo que de no acreditarse tales extremos la prueba electrónica podría carecer de eficacia probatoria por falta de fiabilidad.

4. Las tecnologías disruptivas al servicio de la cadena de custodia

La denominada cuarta revolución industrial o industria 4.0 alude a la nueva revolución tecnológica que envuelve a la sociedad actual[85]. Las tecnologías disruptivas pertenecen, en efecto, a lo que se ha dado en llamar la cuarta revolución industrial. Estas tecnologías adquieren una notoria relevancia a nivel general y, en concreto, en el mundo jurídico[86]. Hemos de señalar, no obstante, que la irrupción de la tecnología en la esfera jurídica no es una situación novedosa en sí misma, al igual que tampoco lo es en la sociedad. Al contrario, esta intromisión lleva produciéndose desde décadas atrás, aunque ciertamente existen diferencias sustanciales entre la tecnología que inundó nuestros procesos judiciales en un inicio –aquellas que se han venido llamando nuevas tecnologías– y la tecnología que actualmente está copando las preocupaciones de la doctrina científica: las tecnologías disruptivas.

4.1. La corrección de la cadena de custodia a través del uso de sistemas *blockchain*

Al margen de la pericial informática como medio para acreditar la integridad de una prueba tecnológica, en el terreno de las tecnologías disruptivas existen otras opciones que, además, están alcanzando mucha fuerza como métodos para garantizar la cadena de custodia tecnológica, tales como la conocida tecnología *blockchain* –o cadena de bloques–[87]. Se trata de

[85] Ya hemos aludido anteriormente a este término, introducido por el economista SCHWAB, quien –además– ha afirmado que los datos son el petróleo del siglo XXI. Al respecto, *vid*. SCHWAB, *La cuarta revolución industrial,* Debate, Barcelona, 2016, pp. 19 ss.

[86] En este escenario, no podemos obviar que uno de los elementos fundamentales de la llamada Industria 4.0 es el fenómeno del Internet of Things (IoT). En tal sentido, afirma BARONA VILAR que internet «se convirtió en una especie de 'bien global' de la sociedad, un instrumento que se presentaba como esencial para garantizar una sociedad acomodada, eficiente y ágil». *Vid.* BARRIO ANDRÉS, *Manual de Derecho Digital,* 2ª ed., Tirant lo Blanch, Valencia, 2022, p. 90., identifica el IoT como uno de los agentes de la cuarta revolución industrial. En tal sentido, afirma BARONA VILAR que internet «se convirtió en una especie de 'bien global' de la sociedad, un instrumento que se presentaba como esencial para garantizar una sociedad acomodada, eficiente y ágil». Al efecto, BARONA VILAR, «Algoritmización de la prueba y la decisión judicial en el proceso penal: ¿utopía o distopia?», en ARANGÜENA FANEGO/DE HOYOS SANCHO/PILLADO GONZÁLEZ (dirs.), *El proceso penal ante una nueva realidad europea,* Aranzadi, Navarra, 2023, p. 135.

[87] Esta tecnología ha sido identificada como una de las grandes protagonistas y motor de la transformación digital de la segunda década del siglo XXI (ARROYO GUARDEÑO/DÍAZ VICO/HERNÁNDEZ ENCINAS, *Blockchain,* Editorial CSIC, Madrid, 2019, p. 5) y su origen se remonta al año 2008, materializándose con la creación de la red Bitcoin, la cual ha sido reconocida como la primera tecnología blockchain operativa. Para mayor información al respecto de la tecnología *Blockchain*, pueden consultarse las publicaciones del *Blockchain Intelligence Law Institute* y, en particular, el artículo doctrinal publicado por DE LA MATA MUÑOZ, «Fundamentos de Blockchain». Consultado en la siguiente página web: https://blockchainintelligence.es/wp-content/uploads/2020/10/Articulo-doctrinal_Fundamentos-Blockchain_Almudena-de-la-Mata.pdf.

La red *Bitcoin* se circunscribe al sector de las monedas electrónicas, sin embargo, lo fundamental de esta nueva propuesta recayó en la inexistencia de autoridad central alguna, de modo que posibilitó por primera vez el intercambio de valores entre las partes en virtud de una red *peer-to-peer*, sin la intermediación de terceros, y en

una categoría propia de la *Distributed Ledger Technology* (DLT) o tecnología de registro distribuido y, en concreto, la *blockchain* 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[88].

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[89]. 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[90]. En concreto, es 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[91]. Ocurre aquí que, una

---

modo estrictamente digital. *Vid.* ARROYO GUARDEÑO/DÍAZ VICO/HERNÁNDEZ ENCINAS, *Blockchain,* Editorial CSIC, Madrid, 2019*,* pp. 12 ss.

[88] *Vid.* IBÁÑEZ JIMÉNEZ, *Blockchain: primeras cuestiones en el ordenamiento español,* Dykinson, Madrid, 2018, pp. 15 ss.; GIMENO BEVIÁ, «Blockchain y resolución de conflictos: algunas reflexiones», en MARTÍN PASTOR/JUAN SÁNCHEZ (Dirs.), *El Derecho Procesal: entre la Academia y el Foro,* Atelier, Barcelona, 2022, p. 608.

[89] 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/HERNÁNDEZ ENCINAS, *Blockchain*, Editorial CSIC, Madrid, 2019, pp. 6 ss.).

[90] 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/HERNÁNDEZ ENCINAS, *Blockchain*, Editorial CSIC, Madrid, 2019, pp. 21 ss.; IBÁÑEZ JIMÉNEZ, *Blockchain*: *primeras cuestiones en el ordenamiento español,* Dykinson, Madrid, 2018, pp. 20 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*. *Vid*. PÉREZ CAMPILLO, «Blockchain: ¿amenaza o solución en la protección de datos y privacidad?», en BUENO DE MATA (dir.), *Fodertics 7.0: estudios sobre derecho digital*, Comares, Granada, 2019, pp. 263-264.

[91] 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, «Cadena de custodia y prueba electrónica: la mismidad del hash como requisito para la fiabilidad probatoria», en BUENO DE MATA (dir.), *FODERTICS 7.0: estudios sobre derecho digital*, Comares, Granada, 2019, p. 297).

vez obtenido el código *hash,* si se modifica un único bit del conjunto de datos, el valor del *hash* será diferente[92]. Del mismo 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[93]. 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*[94]. De ahí que el grado de credibilidad que ofrece la tecnología *blockchain* se perciba elevado[95].

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[96]. 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 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

[92] *Ibidem*. 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 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, «Introducción al Blockchain: análisis del play to earn», *Revista Blockchain e Inteligencia Artificial*, vol. 3, núm. 4, 2022, p. 5 ss.).

[93] 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, *Blockchain: primeras cuestiones en el ordenamiento español*, Dykinson, Madrid, 2018, pp. 22 ss.).

[94] SANTISTEBAN CASTRO, «Algunas consideraciones en torno al valor probatorio de la tecnología blockchain en el ámbito europeo: presente y futuro», *La Ley probática*, núm. 12, 2023.

[95] 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». *Vid.* IBÁÑEZ JIMÉNEZ, *Blockchain: primeras cuestiones en el ordenamiento español*, Dykinson, Madrid, 2018, pp. 22 ss.

[96] 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, «Cadena de custodia y prueba electrónica: la mismidad del hash como requisito para la fiabilidad probatoria», en BUENO DE MATA (dir.), *FODERTICS 7.0: estudios sobre derecho digital*, Comares, Granada, 2019, pp. 289 ss.; GONZÁLEZ GRANDA/ARIZA COLMENAREJO, *Justicia y proceso: una revisión procesal contemporánea bajo el prisma constitucional*, Dykinson, Madrid, 2021, pp. 484-487; SOANA, «Block-chain y prueba digital. Una oportunidad para la cadena de custodia», en PEREIRA PUIGVERT/ORDÓÑEZ PONZ (dirs.), *Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos*, Aranzadi, Navarra, 2021, pp. 605 ss.; PEREIRA PUIGVERT, «Sistema de hash y aseguramiento de la prueba informática. Especial referencia a las medidas de aseguramiento adoptadas inaudita parte», en BUENO DE MATA (dir.), *Fodertics II: hacia una justicia 2.0*, 2014, Comares, Granada, pp. 75 ss. 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*. *Vid*. GARCÍA MATEOS, «Cadena de custodia vs. mismidad», en OLIVA LEÓN/VALERO BARCELÓ (coords.), *La prueba electrónica: validez y eficacia procesal*, Editorial Juristas con futuro, Madrid, 2016, p. 36.

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*[97].

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[98]. Por tanto, si la prueba hubiese sido alterada, esta manipulación se reflejaría en una alteración del valor *hash.*

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[99], integran en la regla 902 la regulación sobre la prueba que se autoautentica[100]. 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*.

---

[97] BUENO DE MATA, «Blockchain, identidad autosoberana y prueba electrónica transfronteriza», en HERNÁNDEZ LÓPEZ/LARO GONZÁLEZ (coords.), *Proceso penal europeo: últimas tendencias, análisis y perspectivas*, Aranzadi, Navarra, 2023, pp. 82 ss.

[98] RUBIO ALAMILLO, «Conservación de la cadena de custodia de una evidencia informática», *Diario la Ley*, núm. 8859, 2016.

[99] ROTHSTEIN, *Federal Rules of Evidence*, 3ª ed., Thomson Reuters, Eagan, 2021, pp. 659-696; GRAHAM, *Federal Rules of Evidence in a nutshell*, 11ª ed., West Academic Publiching, Saint Paul, 2021, pp. 695-696. 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.

[100] MARÍN GONZÁLEZ/GARCÍA SÁNCHEZ, «Problemas que enfrenta la prueba digital en los Estados Unidos de América», *Revista de Estudios de Justicia*, núm. 21, 2014, pp. 75-91.

4.2. La eventual aplicación de inteligencia artificial en el ámbito de la investigación y actividad probatoria con incidencia en la cadena de custodia

a. Nociones previas

Delimitar el concepto de inteligencia artificial (en adelante IA) es una tarea especialmente compleja y desafiante, no por la complejidad inherente al propio término, sino por el riesgo de caer en la obsolescencia al tratarse de un concepto que evoluciona a gran velocidad[101]. Sin perjuicio de la complejidad inherente a su delimitación conceptual, hoy en día se puede afirmar que el término IA, sucintamente, se emplea para referirse a los «sistemas que manifiestan un comportamiento 'inteligente', esto es, sistemas que tienen la capacidad de analizar su entorno y, con cierto grado de autonomía, tomar decisiones para alcanzar objetivos específicos»[102]. Si nos remontamos a los orígenes de la IA tal y como la conocemos en la actualidad, debemos retroceder, en primer lugar, hasta el año 1950, cuando el matemático británico Alan TURING publica un artículo en el que se pregunta si las máquinas pueden pensar[103] y donde establece los cimientos de la IA contemporánea[104]. Un segundo hito lo proporciona el informático estadounidense John MCCARTHY, considerado padre fundador de la IA[105] por ser quien acuña el

[101] CUATRECASAS MONFORTE, La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional, La Ley, Madrid, 2022, p. 23.

[102] BORGES BLÁZQUEZ, *Inteligencia Artificial y proceso penal*, Aranzadi, Navarra, 2021, p. 39. En otras palabras, NILSSON afirma que la «artificial intelligence is that activity devoted to making machines intelligent», y añade que «intelligence is that quality that enables an entity to function appropriately and with foresight in its environment». *Vid*. NILSSON, *The Quest for Artificial Intelligence: A History of Ideas and Achievements*, Cambridge University Press, Nueva York, 2010, p. 13. En similares términos, también alude NIEVA FENOLL a esa capacidad 'intelectual' que adquieren las máquinas en virtud de la IA y sostiene que, en cierto modo, puede afirmarse que las máquinas piensan o, en palabras del autor, «más bien imiten el pensamiento humano a base de aprender y utilizar las generalizaciones que las personas usamos para tomar nuestras decisiones habituales». *Vid*. NIEVA FENOLL, *Inteligencia artificial y proceso judicial*, Marcial Pons, Madrid, 2018, p. 20. Justamente en virtud de la definición que afirma la adquisición de inteligencia por parte de las máquinas, algunos autores defienden la necesidad de entender qué es la inteligencia humana como paso previo para comprender qué es la IA. Lo expone CUATRECASAS MONFORTE, autora que –no obstante– rechaza esta postura, afirmando que tanto máquinas como personas presentamos ciertas limitaciones en comparación con las capacidades del contrario. Al efecto, ilustra la autora que, por un lado, las personas no tenemos la capacidad de realizar diferentes tareas que las máquinas sí ejecutan; mientras que, por otro, las máquinas carecen de sensibilidad, sentido común o capacidad de improvisación. CUATRECASAS MONFORTE, *La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*, La Ley, Madrid, 2022, pp. 23-24. Precisamente a este respecto, KAPLAN sostiene que hay pocas razones, al menos por ahora, para creer que la IA tenga mucha relación con la inteligencia humana. *Vid*. KAPLAN, *Artificial Intelligence. What everyone needs to know,* Oxford University Press, Nueva York, 2016, p. 1. En este punto es de interés la afirmación sostenida por NIEVA FENOLL: «La Inteligencia Artificial es humana, porque la han hecho humanos, incluso aunque sea capaz de 'aprender' de los datos que va recopilando». Pero, además, no podemos perder de vista las siguientes palabras del autor: «Es crucial entender y asumir las limitaciones de unos y otros [máquinas y personas] para no suponer a la inteligencia artificial capacidades que no puede tener; pero tampoco para exagerar las potencialidades del ser humano». *Vid*. NIEVA FENOLL, *Inteligencia artificial y proceso judicial*, Marcial Pons, Madrid, 2018, pp. 16 y 23.

[103] TURING, «Computing machine and intelligence», *Mind,* vol. 59, 1950, p. 433.

[104] CUATRECASAS MONFORTE, La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional, La Ley, Madrid, 2022, p. 26 expone que TURING fue pionero al diseñar un programa informático capaz de jugar al ajedrez.

[105] Así lo identifica KAPLAN, Artificial Intelligence. What everyone needs to know, Oxford University Press, Nueva York, 2016, p. 1; también CUATRECASAS MONFORTE, La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional, La Ley, Madrid, 2022, p. 27.

término en el año 1955[106]. Empero, a pesar de lo anterior, lo cierto es que la IA no empieza a tomar fuerza hasta finales del siglo XX[107].

Muy brevemente, podemos exponer que el funcionamiento de la IA se basa en la capacidad de procesar y 'entender' el lenguaje. Así, el eje de su actividad son los datos (en concreto, el *Big Data*) y los algoritmos, entendiendo como algoritmo «el esquema ejecutivo de la máquina almacenando todas las opciones de decisión en función de los datos que se vayan conociendo»[108]. De ese modo, el algoritmo necesita para funcionar una gran cantidad de datos que figuren ordenados en modo comprensible (denominada *Smart Data*), de los que se nutrirá un modelo matemático a fin de establecer patrones[109]. Especialmente relevantes son los algoritmos de aprendizaje automático, o *machine learning*[110]. Lo identificativo en este punto es que están configurados para seguir 'aprendiendo' al tiempo que se utilizan, de modo que –en palabras de DE HOYOS SANCHO– se van nutriendo progresivamente de nuevos datos[111]. Cuantos más datos tenga en su haber, mayor será el conocimiento adquirido por la máquina.

Atendiendo a lo anterior, la doctrina científica se plantea nuevos cuestionamientos en torno a la introducción de la IA en el proceso. Muy sintéticamente podemos resumirlas en los

---

[106] XAVIER JANUÁRIO, «Vulnerabilidad e hiposuficiencia 4.0: la protección jurídico-penal de los consumidores en la era de la inteligencia artificial», en FONTESTAD PORTALÉS (dir.), *La Justicia en la sociedad 4.0: nuevos retos en el siglo XXI*, Colex, A Coruña, 2023, p. 189; MCCARTHY/MINKSKY/ROCHESTER/SHANNON, «A proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955», *AI Magazine*, Vol. 27, núm. 4, 2006, pp. 12 ss.

[107] GÓMEZ COLOMER, «Problemas legales del juez robot desde una perspectiva procesal y orgánica», en ARANGÜENA FANEGO/DE HOYOS SANCHO/PILLADO GONZÁLEZ (dirs.), *El proceso penal ante una nueva realidad tecnológica europea*, Aranzadi, Navarra, 2023, p. 164.

Precisamente al hilo del proceso evolutivo de la IA, diversos autores precisan que tras la exaltación inicial y a consecuencia de varios intentos fallidos, el desarrollo tecnológico de la IA sufrió algunas fases de estancamiento (a los que se les ha denominado «inviernos de IA»), siendo en el momento actual cuando esta tecnología está siendo objeto de un desarrollo sin precedentes. *Vid.* NIEVA FENOLL, *Inteligencia artificial y proceso judicial*, Marcial Pons, 2018; CUATRECASAS MONFORTE, *La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*, La Ley, Madrid, 2022, p. 28. Así las cosas, desde su origen hasta la actualidad la IA ha pasado por tres generaciones. Lo expone CASTILLEJO MANZANARES, quien aclara que cada una de estas generaciones están inspiradas en un interrogante propio al que la IA ha de ofrecer respuesta. Así, la primera generación responde a la pregunta «¿qué pasó?» y, por tanto, la autora la identifica como la generación de la «analítica descriptica»; la segunda, responde a «¿por qué sucedió?», y está identificada como la generación del «análisis de diagnóstico»; finalmente, en la tercera y actual generación el interrogante que la caracteriza –y al que da respuesta en base a lo que ya ha sucedido– es «¿qué podría suceder en el futuro?», y se conoce como la generación del «análisis predictivo». *Vid.* CASTILLEJO MANZANARES, «Cuáles son las razones que obstaculizan la introducción de la IA en el proceso judicial. Especial referencia al proceso penal», en MARTÍN RÍOS/VILLEGAS DELGADO (dirs.), *La tecnología y la Inteligencia Artificial al servicio del proceso,* Colex, A Coruña, 2023, pp. 84 ss. Para mayor profundización en la historia de la IA, además, puede consultarse KAPLAN, *Artificial Intelligence. What everyone needs to know,* Oxford University Press, Nueva York, 201, pp. 13 ss.

[108] NIEVA FENOLL, *Inteligencia artificial y proceso judicial*, Marcial Pons, Madrid, 2018, p. 21. En otras palabras, los algoritmos son «series de operaciones matemáticas que se van entrelazando para proporcionarnos un resultado» (BORGES BLÁZQUEZ, *Inteligencia Artificial y proceso penal*, Aranzadi, Navarra, 2021, p. 46).

[109] BORGES BLÁZQUEZ, *Inteligencia Artificial y proceso penal*, Aranzadi, Navarra, 2021, p. 46.

[110] La mayoría de los sistemas de IA en la actualidad se basan en *machine learning. Vid.* DOMÍNGUEZ PADILLA, «Aspectos relevantes de la implementación de la Inteligencia Artificial en el proceso judicial», en FONTESTAD PORTALÉS (dir.), *La justicia en la sociedad 4.0: nuevos retos para el siglo XXI,* Colex, A Coruña, 2023, p. 486.

[111] DE HOYOS SANCHO, «El Libro Blanco sobre inteligencia artificial de la Comisión Europea: reflexiones desde las garantías esenciales del proceso penal como 'sector de riesgo'», *REDE: Revista Española de Derecho Europeo,* núm. 76, 2020, pp. 12 ss. También BORGES BLÁZQUEZ, *Inteligencia Artificial y proceso penal,* Aranzadi, Navarra, 2021, p. 47.

siguientes: en primer lugar, se plantea la posibilidad de colisión entre el empleo de IA en el proceso penal y las garantías de los justiciables[112] y el respeto a sus DDFF[113]; en segundo lugar, también se ha puesto de relieve la dicotomía transparencia del Servicio Público de Justicia frente a los derechos de propiedad intelectual de los desarrolladores de este tipo de tecnologías; y en tercer lugar, preocupa el grado de fiabilidad de estos sistemas, en tanto que en algunos de ellos ya se han detectado ciertos sesgos que impiden una actuación igualitaria. Lo cierto es que todas estas cuestiones ya han sido advertidas por los legisladores y los distintos ordenamientos jurídicos han estado trabajando en los últimos años en la adaptación de sus sistemas al nuevo mundo digital[114].

En el contexto de la Unión Europea (UE), uno de los primeros pasos dados de cara a la normativización de la IA lo proporciona la *Carta ética europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno*[115], aprobada en diciembre de 2018 por la Comisión Europea para la eficacia de la justicia. Esta Carta ética precede –y su contenido influye directamente[116]– a la redacción del Libro Blanco sobre inteligencia artificial[117], publicado el 19 de febrero de 2020 por la Comisión Europea y que se manifiesta como paso previo al Reglamento (UE) 2024/1689 de inteligencia artificial (en adelante RIA)[118]. En base al

[112] CASTILLEJO MANZANARES, «Nuevas tecnologías y prueba en el proceso penal. Especial incidencia en Inteligencia Artificial», *Derecho Digital e Innovación*, núm. 11, 2022.

[113] MARTÍN DIZ, «Inteligencia Artificial y derecho procesal: luces, sombras y cábalas en clave de derechos fundamentales», en MORENO CATENA/ROMERO PRADAS (dirs.), *Nuevos postulados de la cooperación judicial en la Unión Europea. Libro homenaje a la Profª. Isabel González Cano*, Tirant lo Blanch, Valencia, 2021, pp. 970 ss. Todo ello sobre la base que este tipo de tecnologías se nutre de datos, con el riesgo que ello comporta para la efectividad del derecho a la protección de datos personales. Precisamente a consecuencia del auge de este tipo de tecnologías, son varios los autores que ya han calificado nuestros datos personales como el petróleo del siglo XXI. *Vid.* BARONA VILAR, «La sociedad post coronavirus con *big data*, algoritmos y vigilancia digital, ¿excusa por motivos sanitarios? ¿y los derechos dónde quedan?», *Revista Bolivariana de Derecho*, núm. 30, 2020, p. 26.

[114] BARONA VILAR expone, al efecto, que en Europa se está haciendo un esfuerzo regulatorio, y no solo económico o de coordinación como ocurre en otros países –la autora lo ilustra enumerando a China, Japón, Corea, Singapur, Rusia, EEUU o India– y afirma que en Asia y EEUU son mucho más permisivos, en aras del progreso «y desde luego con preeminencia de este sobre cualquier otra connotación humana o ética». *Vid.* BARONA VILAR, *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice*, Tirant lo Blanch, Valencia, 2021, pp. 149 ss. Con todo, este esfuerzo regulatorio europeo no ha estado exento de críticas provenientes de aquellos que consideran que estas políticas están frenando el desarrollo económico e innovativo en Europa. En este punto, compartimos la opinión manifestada por la autora, y entendemos que el camino seguido por la UE es la opción correcta.

[115] Esta Carta ética se concibe como un instrumento de *soft law* –que, por tanto, carece de obligatoriedad–, empero, ofrece un contenido de gran interés, principalmente orientado a exponer la importancia de respetar las garantías procesales cuando se emplee IA en el ámbito judicial. *Vid.* DE HOYOS SANCHO, «El Libro Blanco sobre inteligencia artificial de la Comisión Europea: reflexiones desde las garantías esenciales del proceso penal como 'sector de riesgo'», *REDE: Revista Española de Derecho Europeo,* núm. 76, 2020, pp. 11 ss. Es importante destacar que estas implicaciones éticas del uso de la IA en la labor jurisdiccional es una de las cuestiones que mayor inquietud despierta en el conjunto de jueces y magistrados (resaltando, principalmente, la exigencia de respetar la independencia judicial), hecho que se expone perfectamente en algunos de los Dictámenes de las Comisiones de Ética Judicial. *Vid.* al respecto GONZÁLEZ GRANDA/JAMARDO LORENZO, «Medios tecnológicos y uso de la Inteligencia Artificial en el ámbito judicial: una mirada desde el análisis de la ética judicial», *Derecho Digital e Innovación*, núm. 18, 2023.

[116] DE HOYOS SANCHO, «El Libro Blanco sobre inteligencia artificial de la Comisión Europea: reflexiones desde las garantías esenciales del proceso penal como 'sector de riesgo'», *REDE: Revista Española de Derecho Europeo,* núm. 76, 2020, p. 11.

[117] Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza, COM (2020) 65 final.

[118] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos

RIA, el futuro de la IA en la UE se prevé restrictivo. Con una regulación que antepone los valores de la UE frente al desarrollo y uso incontrolable[119]. Y no debe ser de otro modo, precisamente éste es uno de los aspectos más positivos del marco normativo que la UE pretende configurar. No se debe pasar por alto que el empleo de *Big Data* puede causar un impacto brutal en la esfera de privacidad de los ciudadanos de la Unión[120]. Ante este panorama, es imperativo mantenerse estrictos y fomentar la conformación de un escenario garantista. Con todo, la Comisión Europea conoce los riesgos, de ahí que haya organizado los tipos de IA en función de los riesgos a ella asociados. De este modo, el Reglamento reconoce cuatro niveles de riesgo: riesgo inadmisible, alto riesgo, riesgo limitado y riesgo mínimo[121]. Asimismo, el pasado septiembre la UE ha firmado el Convenio Marco sobre Inteligencia Artificial del Consejo de Europa[122] (convenio que se redacta con la destacable vocación de convertirse en el primer tratado internacional jurídicamente vinculante en la materia), siendo éste un texto perfectamente compatible con el RIA.

b. Análisis de las posibilidades

Siguiendo a GÓMEZ COLOMER, los ámbitos en los que el empleo de la IA puede resultar eficaz en el plano procesal penal son los siguientes: en primer lugar, en el terreno de la investigación criminal; segundo, en la elaboración de perfiles de los sospechosos, investigados o acusados; tercero, en el campo de la justicia negociada; cuarto, en la decisión sobre la imposición de medidas cautelares; quinto, en relación con los medios de prueba; sexto, en el ámbito de la valoración de la prueba; y, en último lugar, en fase de ejecución de la condena[123]. Ahora bien, en lo que aquí respecta, nos interesa los usos de la IA que pueden ser trasladables al ámbito de la cadena de custodia y que se circunscriben, fundamentalmente, a dos de los escenarios mencionados: la investigación criminal y la actividad probatoria. No obstante, debemos

(CE) 300/2008, (UE) 167/2013, (UE) 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

[119] BUENO DE MATA, «La necesidad de regular la Inteligencia Artificial y su impacto como tecnología disruptiva en el proceso: de desafío utópico a cuestión de urgente necesidad», en BUENO DE MATA (dir.), *El impacto de las tecnologías disruptivas en el derecho procesal,* Aranzadi, Navarra, 2022, p. 23. Ocurre en el modelo europeo, que se instaura un modelo de gobernanza ético. Se trata de un enfoque prudente, en el que la balanza se inclina a favor de la privacidad, la fiabilidad y el buen uso de la IA. En el marco normativo que la UE está desarrollando priman los DDFF frente al desarrollo económico, lo que se traduce en un contexto en el que el desarrollo tecnológico de la IA ha de seguir avanzando en línea con el debido respeto hacia los principios y valores de la Unión, principalmente en aras a garantizar la privacidad de los ciudadanos. *Vid.* BAENA PEDROSA, *Aplicación de la Inteligencia Artificial por los Tribunales Europeos*, Tirant lo Blanch, Valencia, 2022, pp. 87 y 88.

[120] BUENO DE MATA, «La necesidad de regular la Inteligencia Artificial y su impacto como tecnología disruptiva en el proceso: de desafío utópico a cuestión de urgente necesidad», en BUENO DE MATA (dir.), *El impacto de las tecnologías disruptivas en el derecho procesal,* Aranzadi, Navarra, 2022, p. 24; BARRIO ANDRÉS, «Objeto, ámbito de aplicación y sentido del Reglamento Europeo de Inteligencia Artificial», en BARRIO ANDRÉS (dir.), El Reglamento Europeo de Inteligencia Artificial, Tirant lo Blanch, Valencia, 2024, pp. 40 ss.

[121] BUENO DE MATA, «La necesidad de regular la Inteligencia Artificial y su impacto como tecnología disruptiva en el proceso: de desafío utópico a cuestión de urgente necesidad», en BUENO DE MATA (dir.), *El impacto de las tecnologías disruptivas en el derecho procesal,* Aranzadi, Navarra, 2022, p. 24.

[122] Siendo conscientes de que la entrada de la IA en el ámbito judicial puede generar múltiples beneficios (en íntima conexión con la eficiencia procesal y digital), pero también numerosas preocupaciones en atención a los potenciales riesgos asociados a su uso, el Convenio Marco previsto la necesidad de atajar estos riesgos y se ha incorporado en el texto un precepto que obliga a las partes a garantizar que la IA no perjudique la integridad, independencia y eficacia de las instituciones y procesos democráticos, incluyendo el principio de separación de poderes, el respeto a la independencia judicial y el acceso a la justicia.

[123] GÓMEZ COLOMER, *El Juez-robot. La independencia judicial en peligro*, Tirant lo Blanch, Valencia, 2023, pp. 137-143.

matizar que el examen de estas posibilidades se efectúa desde el plano de la fiabilidad de la prueba en cuestión, y no circunscrito al uso de la IA en el concreto desarrollo de la cadena de custodia.

En primer lugar y por lo que se refiere al terreno de la investigación criminal, en la actualidad ciertos usos de la IA están destinados a la localización de indicios mediante el uso de sistemas de minería de datos o *Data Mining*. En concreto, la finalidad es delimitar los lugares en los que, en base a los datos extraídos de experiencias pasadas, sea más probable localizar los indicios del caso investigado (en definitiva, se trata de una herramienta de previsión de posibilidades)[124]. En materia de cadena de custodia, únicamente tiene el objetivo de situar estadísticamente el lugar en que se iniciará la cadena de custodia en atención al primer acto de su vertiente material –la localización y obtención de las fuentes de prueba materiales–, por lo que, en realidad, su relevancia se circunscribe estrictamente al ámbito de la investigación. Mayor conexión con la figura de la cadena de custodia encontramos en la posibilidad de ejecutar diligencias de investigación asistidas por sistemas de IA en el uso de datos biométricos de identificación. Las posibilidades existentes son diversas y pueden sintetizarse en las siguientes: reconocimiento facial, reconocimiento de voz, reconocimiento de emociones, reconocimiento de huellas dactilares, reconocimiento de ADN y reconocimiento de firma y de escritura[125]. El uso de sistemas de IA en tales supuestos no solo puede favorecer la eficacia de la investigación, sino que además ofrece la posibilidad de que los sistemas de IA garanticen el correcto desarrollo de los análisis y fortalezcan la confianza en su autenticidad o, en materia de cadena de custodia, en su mismidad.

En segundo lugar y en relación con la aplicación de la IA en algunos aspectos de la actividad probatoria, uno de los principales supuestos es el de la valoración de la prueba mediante el auxilio de sistemas basados en IA. Es importante subrayar que únicamente hablamos de auxilio en este ámbito, en cuanto la prueba ha de ser valorada por los jueces en virtud del sistema de valoración libre[126]. Dejando a un lado las otras opciones, aquí nos centraremos en la valoración de la prueba pericial con el auxilio de la IA, en tanto que es el supuesto de mayor interés en materia de cadena de custodia. Lo cierto es que la tarea del juez de valorar los informes periciales presenta como principal obstáculo que la persona que va a valorar los resultados contenidos en el informe pericial es una persona lega en la ciencia empleada en el concreto análisis que da origen al informe pericial[127]. En tal sentido, es fundamental en este punto

[124] A este tipo de herramientas se le atribuye una efectividad del 68% que, si bien pudiera parecer un porcentaje bajo, tal y como expone NIEVA FENOLL, hay que tener en cuenta que la alternativa es depender de la intuición y experiencia de los investigadores, con una ratio de efectividad inferior al de la máquina. NIEVA FENOLL, *Inteligencia artificial y proceso judicial,* Marcial Pons, Madrid, 2018, pp. 26 ss.

[125] Para mayor información, *vid.* CUATRECASAS MONFORTE, *La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*, La Ley, Madrid, 2022, pp. 225 ss.; ETXEBERRIA GURIDI, «Datos biométricos y reconocimiento facial en el proceso penal», en MARTÍN RÍOS/VILLEGAS DELGADO (dirs.), *La tecnología y la Inteligencia Artificial al servicio del proceso,* Colex, A Coruña, 2023, pp. 112 ss.

[126] Expone NIEVA FENOLL que el sistema de valoración libre se basa en muchos datos objetivables, de modo que es factible la asistencia de la IA en este campo. *Vid.* NIEVA FENOLL, *Inteligencia artificial y proceso judicial,* Marcial Pons, Madrid, 2018, pp. 79 ss.

[127] Especialmente crítico en este punto se ha manifestado NIEVA FENOLL, *La valoración de la prueba,* Marcial Pons, Madrid, 2010, p. 285, al exponer el problema que se deriva de la ausencia de conocimientos del juez sobre el informe pericial que está valorando. El autor expone que esta circunstancia concluye, en muchos casos, en la asunción directa y acrítica del dictamen en la sentencia, sin que exista realmente motivación al respecto.

plantearnos si los criterios *Daubert* pueden ser automatizables. Concebidos inicialmente como criterios de admisibilidad de la prueba científica, los estándares *Daubert* se convirtieron con el paso del tiempo en criterios de determinación de la fiabilidad técnica de las pruebas periciales. Para ello, se basa en la observancia de una serie de criterios dirigidos a garantizar el rigor de la técnica científica. Son los siguientes: en primer lugar, se requiere que la técnica empleada haya sido testada frente a la posibilidad de cometer errores; en segundo lugar, se exige que la técnica haya sido revisada por otros científicos y, en su caso, publicada; en tercer lugar, se impone la indicación en el informe el grado de acierto de la técnica; en cuarto lugar, se insiste en el deber de justificar el mantenimiento de estándares de calidad en el empleo de la técnica; y, finalmente, se establece el criterio del consenso de la comunidad científica sobre la técnica empleada[128].

Afirma NIEVA FENOLL que «los criterios parecen haber sido configurados realmente para construir un algoritmo sobre ellos». Señala el autor que la creación de una herramienta basada en IA capaz de automatizar estos criterios ofrecería al juzgador la posibilidad de obtener una valoración, en cuestión de segundos, sobre la calidad de la técnica empleada por el perito. De modo que el sistema de IA validará –o no– la fiabilidad técnica del informe pericial[129]. La materialización de esta posibilidad podría contribuir positivamente en la actividad probatoria, toda vez que –tal y como nos recuerda TARUFFO– el uso de metodologías científicas en la producción de la prueba es cada vez más habitual y, con frecuencia, los hechos son «determinados científicamente en el proceso»[130]. Así las cosas, la automatización de los estándares *Daubert* obtendría claros beneficios en pro de una eficaz fijación del grado de fiabilidad técnica de la prueba científica[131], muy en particular desterrando la duda respecto a la posibilidad de que, al efectuar los debidos análisis, se haya contaminado la prueba analizada.

En palabras de ALCOCEBA GIL, con frecuencia «el juzgador se sitúa frente a la ciencia en posición pasiva», de modo que los jueces acogen sin reservas el conocimiento reflejado en el informe pericial y lo incorporan en su razonamiento probatorio. *Vid.* ALCOCEBA GIL, «Los estándares de cientificidad como criterio de admisibilidad de la prueba científica», *Revista Brasileira de Direito Processual Penal,* vol. 4, núm. 1, 2018, p. 220. En este punto, también PAULESU pone de manifiesto la problemática de confiar a ciegas en la prueba científica, afirmando que «la justicia penal recurre hoy ampliamente a los hallazgos científicos, aun a riesgo de enfrentarse a su manifiesta imperfección». *Vid.* PAULESU, «Inteligencia Artificial y proceso penal italiano: una panorámica», en MARTÍN RÍOS y VILLEGAS DELGADO, *La tecnología y la inteligencia artificial al servicio del proceso,* Colex, A Coruña, 2023, p. 724; BONET NAVARRO, «Valoración de la prueba y resolución mediante inteligencia artificial», en BUJOSA VADELL, *Derecho Procesal: retos y transformaciones*, Atelier, Barcelona, 2021, pp. 329-330, expone la posibilidad del empleo de IA para valorar la fiabilidad técnica de la pericia, afirmando que la valoración del perito podría ser una opción para ello, matizando, no obstante, que el análisis de esa cuestión no ofrece una solución enteramente objetiva de cara a determinar la fiabilidad técnica del perito, afirmando que mayor interés tendría que el informe pericial en sí mismo cumpla con los estándares científicos al respecto.

[128] NIEVA FENOLL, "Repensando Daubert: la paradoja de la prueba pericial", *Civil Procedure Review,* Vol. 9, núm.1, 2018, pp. 13 ss.

[129] NIEVA FENOLL, *Inteligencia artificial y proceso judicial*, Marcial Pons, Madrid, 2018, pp. 96 ss.

[130] TARUFFO, *La prueba de los hechos* (trad. Ferrer Beltrán), Trotta, Madrid, 2002, pp. 333 ss.

[131] La doctrina viene considerando que verdaderamente relevante de la doctrina *Daubert*, en los sistemas jurídicos del *Civil Law*, es la exigencia de «una efectiva validez científica de la prueba» (TARUFFO, «La aplicación de estándares científicos a las ciencias sociales y forense», en VÁZQUEZ ROJAS (dir.), *Estándares de prueba y prueba científica. Ensayos de epistemología jurídica*, Marcial Pons, Madrid, 2013, pp. 203 ss.). dicho de otro modo, la transcendencia de lo expuesto se observa en que la formulación de estos criterios en su conjunto se pervive como el primer estándar de cientificidad establecido jurisprudencialmente (ALCOCEBA GIL, «Los estándares de cientificidad como criterio de admisibilidad de la prueba científica», *Revista Brasileira de Direito Processual Penal*, vol. 4, núm. 1, 2018, pp. 230 ss.).

5. Análisis prospectivo-legal de la figura de la cadena de custodia a la luz de la regulación proyectada en los anteproyectos de Ley de Enjuiciamiento Criminal de los años 2011 y 2020

5.1. Valoración crítica

En un claro afán modernizador del proceso penal, en los últimos años se han ido sucediendo hasta tres iniciativas prelegislativas distintas con vistas a la promulgación de una nueva ley procesal penal (y sin que hasta la fecha ningunos de los textos presentados haya finalizado su *iter* legislativo). A pesar de lo anterior, únicamente dos de estas propuestas proyectaban una regulación expresa y unitaria de la cadena de custodia: los ALECrim de 2011 y 2020. En cambio, el Borrador de Código Procesal Penal del año 2013 no incorporaba la tan anhelada regulación procesal de la cadena de custodia[132].

Poniendo el acento en la regulación de la cadena de custodia proyectada en el ALECrim de 2020, sorprende el hecho de que, a pesar de los años transcurridos desde la propuesta anterior (la del 2011), el más reciente mantiene una propuesta esencialmente idéntica[133] a la contenida en su predecesor, sin que el nuevo texto refleje alguna de las novedosas cuestiones que se han ido construyendo a lo largo de estos casi diez años de evolución jurisprudencial[134]. Resulta evidente que, en ambos casos, el primer acierto en la regulación proyectada en materia de cadena de custodia es, precisamente, la propia incorporación de ésta. Y es que, a pesar de las carencias o puntos débiles que puedan reflejarse en los distintos preceptos dedicados al efecto, la inclusión de una regulación expresa merece ser aplaudida en línea de principio, en vista del escenario procesal de partida. Ahora bien, habrá que analizar el texto de cara a ofrecer una valoración crítica sobre el contenido de la regulación proyectada.

---

[132] Con la redacción del Borrador de 2013 se diluía notablemente el interés mostrado en el plano legislativo. A pesar de la presencia de algunas previsiones que otorgaban cierta relevancia, mayoritariamente indirecta, a la institución de la cadena de custodia, este borrador presentaba la gran desventaja de no contar con una regulación unitaria y explícita. El único contacto directo con la cadena de custodia se proyectaba sobre el precepto dedicado a regular el atestado policial (art. 84 Borrador 2013), aludiendo a la misma en los siguientes términos «especialmente se relacionarán los instrumentos, efectos y fuentes de prueba recogidos y las salvaguardas adoptadas para asegurar la integridad de la cadena de custodia». No se puede negar la relevancia de ello, no obstante, cubrir las necesidades legislativas de la cadena de custodia demanda una regulación expresa de la misma como institución procesal autónoma, y no meras referencias en preceptos aislados. Adicionalmente, el borrador refleja una regulación indirecta a propósito de ciertas garantías que han de mantenerse en la práctica de algunas diligencias de investigación, muy especialmente en relación tanto con la conservación de las fuentes de prueba como con el deber de documentar el modo en que se llevaron a cabo las distintas actuaciones (arts. 342; 356 y 287 Borrador 2013).

A pesar de las diferencias obvias que inspiran la redacción de los textos del 2011 y 2013, resulta curioso el distinto enfoque ofrecido a esta figura en estos años. Lo curioso se infiere del diferente reconocimiento otorgado a la cadena de custodia habida cuenta la trascendencia práctica de esta figura y, en particular, considerando que ésta ya había sido expuesta en el año 2013 y no sólo por el prelegislador del 2011, sino también por la doctrina científica y, desde luego, por nuestros juzgados y tribunales.

[133] Teniendo en cuenta que la única diferencia responde a un ajuste terminológico (la sustitución de una palabra por otra sinónima), no existe modificación real entre las regulaciones proyectadas en ambos.

[134] Entre otras, véase las STS 587/2014, de 18 de julio, ECLI:ES.TS:2014:2086; STS714/2016, de 26 de septiembre, ECLI:ES:TS:2016:4171; STS 726/2017, de 8 de noviembre, ECLI:ES:TS:2017:3957; STS 679/2019, de 23 de enero, ECLI:ES:TS:2020:166; STS 46/2021, de 3 de febrero; ECLI:ES:TS:2021:38; STS 90/2021, de 3 de febrero, ECLI:ES:TS:2021:319; STS 201/2022, de 3 de marzo, ECLI:ES:TS:2022:918; STS 241/2024, de 13 de marzo, ECLI:ES:TS:2024:1342.

En primer lugar, resulta cuestionable la ubicación que el prelegislador decide otorgar al capítulo de la cadena de custodia, pues la incardina dentro de las diligencias de investigación y, en particular, en relación con los medios de investigación relativos al cuerpo del delito[135]; lo que parece indicar que la cadena de custodia se concibe como una diligencia de investigación (siendo esto, por supuesto, un error), cuando en realidad, tal y como se sostiene a lo largo de este trabajo, la cadena de custodia debe ser entendida como una garantía de la mismidad de la prueba.

Continuamos el análisis sobre la base del precepto de partida, rubricado *Garantías de las fuentes de prueba*, el cual establece lo siguiente:

> «1. Todas las actuaciones tendentes a la localización, recogida, obtención, análisis, depósito y custodia de las fuentes de prueba deberán realizarse en la forma prevista en esta ley y en las demás disposiciones que resulten aplicables.
>
> 2. Todas las fuentes de prueba obtenidas durante la investigación de los hechos delictivos serán debidamente custodiadas, a fin de asegurar su disponibilidad en el acto del juicio oral con los efectos que esta ley establece».

Dos son los elementos a destacar positivamente: en primer lugar, la inclusión de una enumeración de las actuaciones que conforman la cadena de custodia, teniendo en cuenta que todas ellas participan del recorrido de la prueba desde su obtención hasta su incorporación al proceso; y, en segundo lugar, la identificación de su finalidad. Sin embargo, es el propio título del precepto el que aporta el aspecto de mayor interés: reconoce el carácter garantista de la cadena de custodia.

El siguiente precepto, bajo la rúbrica *Cadena de custodia,* precisa el momento en que se inicia la cadena de custodia entendiendo que «(···) se inicia en el lugar y momento en los que se obtiene o encuentra la fuente de prueba». Seguidamente establece la obligación, frente a todos los intervinientes, de constituir, aplicar y mantener la cadena de custodia, en aras de garantizar la inalterabilidad de la fuente de prueba. Y, finalmente, expone la necesidad de dejar constancia de las posibles alteraciones que pudieran producirse en el estado original de las evidencias. Continúa la regulación proyectada con un precepto dedicado al *procedimiento de gestión de muestras,* incorporando algunas reglas procedimentales cuyo fin es asegurar el buen desarrollo de la cadena de custodia. Además, reconoce la conveniencia de establecer reglamentariamente los procedimientos a seguir y enumera una serie de circunstancias que, en todo caso, habrán de ser documentadas.

El último precepto, *efectos de la cadena de custodia*, regula tres aspectos fundamentales:

[135] A pesar de la sorpresa que nos produce la equiparación de la cadena de custodia con las diligencias de investigación, es preciso señalar que esta igualación no es exclusiva del prelegislador español, sino que en algunos ordenamientos jurídicos ha sido regulada previamente en modo similar. Un ejemplo de ello es el sistema jurídico mexicano, en el cual la cadena de custodia es regulada en el Código Nacional de Procedimientos Penales dentro de un capítulo dedicado a las técnicas de investigación. El sistema jurídico colombiano, en cambio, a pesar de que la regulación de la cadena de custodia en el Código de Procedimiento Penal se contiene en el Libro II –técnicas de indagación e investigación de la prueba y sistema probatorio–, Título I –la indagación y la investigación–, en el Capítulo V –dedicado específicamente a la cadena de custodia– no parece contener la cadena de custodia en el contexto exclusivo de las técnicas de investigación.

> «1. El cumplimiento de los procedimientos de gestión y custodia determinará la autenticidad de la fuente de prueba llevada al juicio oral y, en su caso, justificará sus alteraciones o modificaciones.
>
> 2. El quebrantamiento de la cadena de custodia será valorado por el tribunal a los efectos de determinar la fiabilidad de la fuente de prueba.
>
> 3. La cadena de custodia podrá ser impugnada en el trámite de admisión de la prueba alegando el incumplimiento de los procedimientos de gestión y custodia de las muestras».

En suma, el ALECrim 2020 pretende introducir en nuestro ordenamiento procesal una regulación en la que se establecen unas características y principios mínimos y generales que orienten el correcto desarrollo de la cadena de custodia. Es obvio que la regulación proyectada refleja, en parte, la doctrina elaborada por el TS, configurando la cadena de custodia como una garantía formal de la autenticidad de la prueba. Sin embargo, son también apreciables las ausencias, debiendo destacar muy especialmente la ausencia de concepto. Además, se omite, por un lado, referencia alguna a los términos corrección de la cadena de custodia y mismidad de la prueba, tan sumamente significativos en su construcción jurídica; por otro, las previsiones relativas a la impugnación de la cadena de custodia y las consecuencias jurídicas derivadas tanto de su ruptura como de su corrección continúan siendo deficientes. En cuanto a la delimitación de la cadena de custodia, si bien su planteamiento es suficientemente positivo en general, tampoco es enteramente satisfactorio.

En definitiva, la regulación de la cadena de custodia proyectada en el ALECrim 2020 no satisface las necesidades actuales de una regulación adecuada[136]. Distinta valoración merece, en cambio, el ALECrim 2011. Esto ocurre porque, al tiempo de pronunciar una opinión sobre las regulaciones proyectadas, es preciso atender al marco temporal en el que se encuadran. Con contenido sustancialmente idéntico en ambas propuestas, ciertamente merecen valoraciones dispares a consecuencia, justamente, del marco temporal. En el año 2011, la regulación proyectada merecía una valoración especialmente positiva, no obstante, la misma propuesta a finales del 2020 es poco satisfactoria. De uno a otro año el avance en materia de cadena de custodia es notorio, con consolidación de algunos de los elementos esenciales que siguen sin verse reflejados en la propuesta. En base a tales consideraciones, puede afirmarse que la regulación proyectada en el ALECrim 2020 es susceptible de múltiples mejoras.

5.2. Algunas propuestas de *lege ferenda*

No podemos finalizar el presente trabajo sin abordar, siquiera someramente, la exposición de algunas propuestas de *lege ferenda*, a fin de auxiliar al legislador en la complejidad de su tarea. Y ello teniendo en cuenta, en primer lugar, la urgente necesidad de que se incorpore una regulación procesal de la cadena de custodia en nuestro ordenamiento jurídico y, en segundo lugar, teniendo en cuenta que la regulación proyectada en 2020 no responde a las necesidades actuales de regulación de la cadena de custodia.

[136] Aun cuando parte de la doctrina otorga una valoración positiva a la misma. *Vid.* ORTEGO PÉREZ, «Los medios de investigación relativos al cuerpo del delito», en JIMÉNEZ CONDE/FUENTES SORIANO (dirs.), *Reflexiones en torno al Anteproyecto de Ley de Enjuiciamiento Criminal de 2020,* Tirant lo Blanch, Valencia, 2022, pp. 744 ss.

Un primer precepto, en mi opinión, habrá de ocuparse de la delimitación de la cadena de custodia, siendo conveniente establecer que la cadena de custodia constituye una garantía de la prueba y su corrección acredita la mismidad de la prueba material. Habrá de ser ésta, sin duda, la base sobre la que se sustente una regulación apropiada de la cadena de custodia. Es conveniente que la LECrim refleje el significado del término mismidad de la prueba en este primer precepto, pudiendo incorporar un segundo inciso en el que se indique que la mismidad de la prueba se corresponde con la identidad procesal de la fuente de prueba obtenida y el medio de prueba incorporado al juicio oral, sin que las alteraciones sufridas a consecuencia del devenir de las actuaciones procesales pertinentes sean un impedimento a la misma.

Otro aspecto indispensable es el relativo a la identificación del inicio y el fin de la cadena de custodia, entendiendo que la cadena de custodia se inicia con la obtención de la fuente de prueba material y concluye con su incorporación al juicio oral mediante el medio de prueba oportuno. No debemos olvidar que todas las actuaciones que transcurren desde la obtención de la prueba hasta su incorporación al proceso constituyen los actos que integran la vertiente material de la cadena de custodia.

Además, se ha de incorporar un precepto que establezca las obligaciones de los intervinientes en la cadena de custodia. A este respecto, debemos tener en cuenta que corresponde a quienes tengan contacto con la fuente de prueba material las siguientes funciones: constituir, aplicar y mantener la cadena de custodia de cara a garantizar la mismidad de la prueba.

Por otra parte, y a pesar de lo que se ha venido defendiendo a lo largo del presente trabajo, es necesario incorporar algunas precisiones en relación con el alcance de la vertiente material de la cadena de custodia. En primer lugar, es importante señalar que las actuaciones derivadas de la vertiente material se realizarán en la forma prevista en las disposiciones normativas que resulten aplicables en atención al organismo encargado de las distintas actuaciones, sin que la estricta obediencia de estos protocolos pueda condicionar la corrección de la cadena de custodia, todo ello siguiendo el criterio del TS de que la excesiva burocratización de la cadena de custodia no puede ser impedimento a que despliegue todos sus efectos. En segundo lugar, la LECrim habrá de aludir al deber de documentación de la cadena de custodia, siendo oportuno que se establezcan como necesarios de documentar los siguientes extremos:

1. La persona y el lugar en que se localizó la fuente de prueba, debiendo documentarse el hallazgo.

2. Identificación de las personas que hayan tenido la fuente de prueba a su cargo, los lugares en que haya estado guardada, depositada o almacenada, así como el tiempo que haya permanecido en cada uno de estos lugares y las decisiones que han motivado los traslados.

3. Identificación de las personas que hayan accedido a las fuentes de prueba, con detalle en su caso de las técnicas empleadas sobres las mismas, así como el estado inicial y final de las muestras.

Además, dos de los aspectos de mayor relevancia de cara a una regulación apropiada de la cadena de custodia son la impugnación y los efectos jurídicos. Y es aquí, justamente, donde

mayor cuidado se ha de poner a la hora de redactar la regulación en cuestión. A propósito de la regulación de los cauces y procedimientos de impugnación de la cadena de custodia, habrá de especificarse –en primer lugar– que se presume la corrección de la cadena de custodia en tanto que no se haya acreditado su ruptura. A continuación, es crucial tener en cuenta que la cadena de custodia habrá de impugnarse ante el órgano correspondiente desde el momento en que se tenga conocimiento de las irregularidades en su desarrollo. A tal efecto, la cadena de custodia podrá ser impugnada en el trámite de admisión de la prueba aun cuando su ruptura no determine la inadmisión de la prueba.

Por último y en cuanto a los efectos jurídicos derivados de la cadena de custodia, dos son los extremos que han de quedar necesariamente reflejados en la LECrim. Primero, la corrección de la cadena de custodia determina el cumplimiento de los procedimientos y garantiza la mismidad de la prueba, circunstancia que otorga a la prueba un grado de fiabilidad alto, si bien su verosimilitud deberá ser determinada por el juez o tribunal sentenciador en sede de valoración de la prueba. Segundo, la ruptura de la cadena de custodia será valorada por el tribunal sentenciador a los efectos de determinar el grado de fiabilidad de la prueba.

6. A modo de conclusión

Antes de concluir el trabajo presentado, considero oportuno exponer sintéticamente y a modo de conclusión algunas de las claves fundamentales en la formulación de la cadena de custodia tecnológica.

I.- La configuración de la cadena de custodia tecnológica debe tomar como base necesariamente la noción tradicional de cadena de custodia, en tanto que la cadena de custodia tecnológica es, en puridad, una particularidad de la cadena de custodia en sí misma. Por tanto, también en el contexto tecnológico, la cadena de custodia ha de ser entendida, como una garantía de la prueba que, desde su vertiente formal, constituye la garantía de la mismidad de la prueba 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.

II.- Es fundamental la diferenciación entre ambas vertientes (formal y material) para comprender la cadena de custodia en toda su amplitud. Con esta clasificación se pretende poner el acento en la delimitación de los elementos que integran el contenido procesal de la cadena de custodia como figura jurídica autónoma. Así, integran la vertiente formal aquellos elementos que condiciona su significado (el de la cadena de custodia) en el proceso, mientras que la vertiente material implica la individualización de los actos materiales que se producen desde la obtención de la prueba y hasta su incorporación.

III.- Destaca especialmente la matización de la presunción de veracidad de la cadena de custodia tecnológica. Al contrario de lo que ocurría en la cadena de custodia de una prueba más tradicional, la impugnación de la prueba tecnológica conlleva la necesidad de acreditar su autenticidad. Teniendo en cuenta, por tanto, que la autenticidad es uno de los elementos que integran el concepto de mismidad de la prueba, se produce entonces una matización a la presunción de veracidad de la cadena de custodia

tecnológica y que responde, en todo caso, a una cuestión de fiabilidad sobre la prueba tecnológica. Muy importante esto, teniendo en cuenta que la cadena de custodia rige, en efecto, en el terreno de la fiabilidad de la prueba.

IV.- Al hilo de lo anterior, una de las claves fundamentales del estudio de la cadena de custodia tecnológica se manifiesta en la necesidad de examinar los diferentes modos de acreditar la mismidad de la prueba tecnológica. La más extendida de las soluciones se prevé en la incorporación de un informe pericial, informático, que acredite la autenticidad de la prueba tecnológica y rechace posibles alteraciones en los datos contenidos en los dispositivos tecnológicos.

V.- En el terreno de las tecnologías disruptivas, una solución muy extendida en la actualidad alude a la posibilidad de acreditar la mismidad de la prueba mediante tecnología *blockchain* que, en concreto, implica un mecanismo de encriptación de datos mediante el uso encadenado de códigos *hash*. Esta posibilidad implica una actuación de carácter preventivo. Esto es, la encriptación de los datos como método de prevención frente a la eventual impugnación de la autenticidad de la prueba tecnológica, de modo que una posible alteración de los datos sería perfectamente verificable por un perito informático.

7. Bibliografía

ABEL LLUCH, Xavier, *La prueba electrónica,* J. M. Bosch, Barcelona, 2011.

ALCOCEBA GIL, Juan Manuel, «Los estándares de cientificidad como criterio de admisibilidad de la prueba científica», *Revista Brasileira de Direito Processual Penal,* vol. 4, núm. 1, 2018, pp. 215-242.

ÁLVAREZ DE NEYRA KAPPLER, Susana «La cadena de custodia en materia de tráfico de drogas», en FIGUEROA NAVARRO, Carmen (dir.), *La cadena de custodia en el proceso penal,* Edisofer, Madrid, 2015, pp. 81-106.

ARELLANO, Luis Enrique/CASTAÑEDA, Carlos Mario, «La cadena de custodia informático-forense», *Cuadernos informático-forense*, núm. 3, 2012, pp. 67-81.

ARRABAL PLATERO, Paloma, *La prueba tecnológica: aportación, práctica y valoración*, Tirant lo Blanch, Valencia, 2019.

ARRABAL PLATERO, Paloma, «El valor probatorio de la información contenida en un dispositivo tecnológico», en BUJOSA VADELL, Lorenzo (dir.), *Derecho procesal: retos y transformaciones,* Atelier, Barcelona, 2021, pp. 521-539.

ARROYO GUARDEÑO, David/DÍAZ VICO, Jesús/HERNÁNDEZ ENCINAS, Luis, *Blockchain*, Editorial CSIC, Madrid, 2019.

BAENA PEDROSA, Manuel, *Aplicación de la Inteligencia Artificial por los Tribunales Europeos,* Tirant lo Blanch, Valencia, 2022.

BARONA VILAR, Silvia, «La sociedad post coronavirus con *big data,* algoritmos y vigilancia digital, ¿excusa por motivos sanitarios?, ¿y los derechos dónde quedan?», *Revista Bolivariana de Derecho,* núm. 30, 2020, pp. 14-39.

BARONA VILAR, Silvia, *Algoritmización del Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice,* Tirant lo Blanch, Valencia, 2021.

BARONA VILAR, Silvia, «Algoritmización de la prueba y la decisión judicial en el proceso penal: ¿utopía o distopia?», en ARANGÜENA FANEGO, Coral/DE HOYOS SANCHO, Montserrat/PILLADO GONZÁLEZ, Esther (dirs.), *El proceso penal ante una nueva realidad europea*, Aranzadi, Navarra, 2023, pp. 133-161.

BARRIA NUEVAS, Sebastián, «Introducción al *Blockchain*: análisis del *play to earn*», *Revista Blockchain e Inteligencia Artificial*, vol. 3, núm. 4, 2022, pp. 1-28.

BARRIO ANDRÉS, Moisés, *Manual de Derecho Digital,* 2ª ed., Tirant lo Blanch, Valencia, 2022.

BARRIO ANDRÉS, Moisés, «Objeto, ámbito de aplicación y sentido del Reglamento Europeo de Inteligencia Artificial», en BARRIO ANDRÉS, Moisés (dir.), *El Reglamento Europeo de Inteligencia Artificial,* Tirant lo Blanch, Valencia, 2024, pp. 21-47.

BELHADJ BEN GÓMEZ, Celia, «La prueba digital. Aspectos procesales», *Revista Derecho y Proceso,* núm. 3, 2023, pp. 29-45.

BONET NAVARRO, José, «Valoración de la prueba y resolución mediante inteligencia artificial», en BUJOSA VADELL, Lorenzo (dir.), *Derecho Procesal: retos y transformaciones*, Atelier, Barcelona, 2021, pp. 315-337.

BORGES BLÁZQUEZ, Raquel, *Inteligencia Artificial y proceso penal,* Aranzadi, Navarra, 2021.

BUENO DE MATA, Federico, *Las diligencias de investigación penal en la cuarta revolución industrial: principios teóricos y problemas prácticos*, Aranzadi, Navarra, 2019.

BUENO DE MATA, Federico, «El derecho probatorio en la cuarta revolución industrial», en ASENCIO MELLADO, José María (dir.), *Derecho probatorio y otros estudios procesales. Liber Amicorum: Vicente Gimeno Sendra,* Ediciones Jurídicas Castillo de Luna, Madrid, 2020, pp. 299-314.

BUENO DE MATA, Federico «La necesidad de regular la Inteligencia Artificial y su impacto como tecnología disruptiva en el proceso: de desafío utópico a cuestión de urgente necesidad», en BUENO DE MATA, Federico (dir.), *El impacto de las tecnologías disruptivas en el derecho procesal,* Aranzadi, Navarra, 2022, pp. 15-41.

BUENO DE MATA, Federico, «Blockchain, identidad autosoberana y prueba electrónica transfronteriza», en HERNÁNDEZ LÓPEZ, Alejandro/LARO GONZÁLEZ, María Elena (coords.), *Proceso penal europeo: últimas tendencias, análisis y perspectivas*, Aranzadi, Navarra, 2023, pp. 71-86.

CABEZUDO BAJO, María José, *Propuestas para una regulación armonizada de la obtención de la prueba de ADN como prueba científica-tecnológica de probabilidad en el proceso penal,* Aranzadi, Navarra, 2017.

CALAZA LÓPEZ, Sonia/MUINELO COBO, Juan Carlos, «La digitalización y custodia de la prueba pericial electrónica sobre evidencias virtuales», en PICÓ I JUNOY, Joan (dir.), *La prueba pericial a examen: propuestas de lege ferenda*, J. M. Bosch, Barcelona, 2020, pp. 471-481.

CALAZA LÓPEZ, Sonia, «Cadena de custodia y prueba tecnológica», en VILLEGAS DELGADO, César/MARTÍN RÍOS, Pilar (dirs.), *El derecho en la encrucijada tecnológica: estudios sobre derechos fundamentales, nuevas tecnologías e inteligencia artificial,* Tirant lo Blanch, Valencia, 2022, pp. 39-61.

CAMPOS, Federico, «La relevancia de la cadena de custodia en la investigación judicial», *Medicina legal de Costa Rica*, vol. 19, núm. 1, 2022, pp. 75-87.

CASTILLEJO MANZANARES, Raquel, «La prueba en el proceso penal: el documento electrónico», *Revista de Derecho Penal,* núm. 29, 2010, pp. 11-43.

CASTILLEJO MANZANARES, Raquel «Nuevas tecnologías y prueba en el proceso penal. Especial incidencia en inteligencia artificial», *Derecho digital e innovación,* núm. 11, 2022.

CASTILLEJO MANZANARES, Raquel, «Cuáles son las razones que obstaculizan la introducción de la IA en el proceso judicial. Especial referencia al proceso penal», en MARTÍN RÍOS, Pilar/VILLEGAS DELGADO, César (dirs.), *La tecnología y la inteligencia artificial al servicio del proceso,* Colex, A Coruña, 2023, pp. 83-106.

COLOMER HERNÁNDEZ, Ignacio, «Prueba tecnológica», en GONZÁLEZ CANO, María Isabel (dir.), *La prueba en el proceso civil*, Tirant lo Blanch, Valencia, 2017, pp. 579-361.

COLOMER HERNÁNDEZ, Ignacio, «Limitaciones en el uso de la información y los datos personales en un proceso penal digital», en ARANGÜENA FANEGO, Coral/DE HOYOS SANCHO, Montserrat/PILLADO GONZÁLEZ, Esther (dirs.), *El proceso penal ante una nueva realidad tecnológica europea*, Aranzadi, Navarra, 2023, pp. 39-74.

CUADRADO SALINAS, Carmen, «La obtención de pruebas electrónicas transfronterizas: nuevos retos y nuevas consideraciones desde la perspectiva de la Unión Europea», en ASENCIO MELLADO, José María (dir.), *Derecho probatorio y otros estudios procesales. Liber Amicorum: Vicente Gimeno Sendra*, Ediciones Jurídicas Castillo de Luna, Madrid, 2020, pp. 517-534.

CUATRECASAS MONFORTE, Carlota, *La Inteligencia Artificial como herramienta de investigación criminal. Utilidades y riesgos potenciales de su uso jurisdiccional*, La Ley, Madrid, 2022.

DE HOYOS SANCHO, Montserrat, «El Libro Blanco sobre inteligencia artificial de la Comisión Europea: reflexiones desde las garantías esenciales del proceso penal como 'sector de riesgo'», *REDE: Revista Española de Derecho Europeo,* núm. 76, 2020, pp. 9-43.

DE URBANO CASTRILLO, Eduardo, *La valoración de la prueba electrónica,* Tirant lo Blanch, Valencia, 2009.

DEL POZO PÉREZ, Marta, *Diligencias de investigación y cadena de custodia,* Sepín, Madrid, 2014.

DELGADO MARTÍN, Joaquín, *Investigación tecnológica y prueba digital en todas las jurisdicciones*, 2ª ed., La Ley, Madrid, 2018.

DOMÍNGUEZ PADILLA, Carlos, «Aspectos relevantes de la implementación de la Inteligencia Artificial en el proceso judicial», en FONTESTAD PORTALÉS, Leticia (dir.), *La justicia en la sociedad 4.0: nuevos retos para el siglo XXI,* Colex, A Coruña, 2023, pp. 483-498.

ESPÍN LÓPEZ, Isidoro, «La cadena de custodia en el proceso penal. Propuestas en relación con el análisis y custodia de la prueba digital», *La Ley penal*, núm. 151, 2021.

ESPÍN LÓPEZ, Isidoro, *Investigación sobre equipos informáticos y su prueba en el proceso penal,* Aranzadi, Navarra, 2021.

ETXEBBERIA GURIDI, José Francisco, «Datos biométricos y reconocimiento facial en el proceso penal», en MARTÍN RÍOS, Pilar/VILLEGAS DELGADO, César (dirs.), *La tecnología y la Inteligencia Artificial al servicio del proceso,* Colex, A Coruña, 2023, pp. 107-126.

FALCIANI, Hervé, «La prueba digital en el proceso civil: la cadena de la prueba», en FUENTES SORIANO, Olga (dir.), *Era digital, sociedad y Derecho,* Tirant lo Blanch, Valencia, 2020, pp. 365-371.

FIGUEROA NAVARRO, Carmen, «El aseguramiento de las pruebas y cadena de custodia», *La Ley Penal,* núm. 84, 2011.

FUENTES SORIANO, Olga, «La intervención de las comunicaciones tecnológicas tras la reforma de 2015», en ALONSO-CUEVILLAS SAYROL, Jaime (dir.), *El nuevo proceso penal tras las reformas de 2015*, Atelier, Barcelona, 2016 pp. 261-285.

FUENTES SORIANO, Olga, «El valor probatorio de los correos electrónicos», en ASENCIO MELLADO, José María (dir.), *Justicia penal y nuevas formas de delincuencia*, Tirant lo Blanch, Valencia, 2017, pp. 183-210.

GARCÍA DE YÉBENES, Pilar/GASCÓ ALBERCHI, Pilar, «La cadena de custodia de muestras relacionadas con presuntos ilícitos contra el medio ambiente», en FIGUEROA NAVARRO, Carmen (dir.), *La cadena de custodia en el proceso penal,* Edisofer, Madrid, 2015, pp. 129-137.

GARCÍA MATEOS, José Aurelio, «Cadena de custodia vs. mismidad», en OLIVA LEÓN, Ricardo/VALERO BARCELÓ, Sonsoles (coords.), *La prueba electrónica: validez y eficacia procesal,* Editorial Juristas con futuro, Madrid, 2016, pp. 130-136.

GARCIMARTÍN MONTERO, Regina, *Los medios de investigación tecnológicos en el Proceso Penal*, Aranzadi, Navarra, 2018.

GIMENO BEVIÁ, Jordi, «Blockchain y resolución de conflictos: algunas reflexiones», en MARTÍN PASTOR, Juan/JUAN SÁNCHEZ, Ricardo (dirs.), *El Derecho Procesal: entre la Academia y el Foro,* Atelier, Barcelona, 2022, pp. 607-613.

GÓMEZ COLOMER, Juan Luis, «Problemas legales del juez robot desde una perspectiva procesal y orgánica», en ARANGÜENA FANEGO, Coral/DE HOYOS SANCHO, Montserrat/PILLADO GONZÁLEZ, Esther (dirs.), *El proceso penal ante una nueva realidad tecnológica europea,* Aranzadi, Navarra, 2023, pp. 163-193.

GÓMEZ COLOMER, Juan Luis, *El juez-robot. La independencia judicial en peligro,* Tirant lo Blanch, Valencia, 2023.

GONZÁLEZ GRANDA, Piedad, «Órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento criminal: próximo avance en materia de prueba penal transfronteriza», en MORENO CATENA, Víctor/ROMERO PRADAS, María Isabel (dirs.), *Nuevos postulados de la cooperación judicial en la Unión Europea. Libro homenaje a la Profª. Isabel González Cano,* Tirant lo Blanch, Valencia, 2021, pp. 1083-1109.

GONZÁLEZ GRANDA, Piedad/ARIZA COLMENAREJO, María Jesús, *Justicia y proceso: una revisión procesal contemporánea bajo el prisma constitucional,* Dykinson, Madrid, 2021.

GONZÁLEZ GRANDA, Piedad/JAMARDO LORENZO, Andrea, «Medios tecnológicos y uso de la Inteligencia Artificial en el ámbito judicial: una mirada desde el análisis de la ética judicial», *Derecho Digital e Innovación,* núm. 18, 2023.

GRAHAM, Michael H., *Federal Rules of Evidence in a nutshell,* 11ª ed., West Academic Publishing, Saint Paul, 2021.

GUTIÉRREZ SANZ, María Rosa, *La cadena de custodia en el proceso penal español,* Civitas, Navarra, 2016.

GUZMÁN FLUJA, Vicente Carlos, *Anticipación y preconstitución de la prueba en el proceso penal*, Tirant lo Blanch, Valencia, 2006.

IBÁÑEZ JIMÉNEZ, Javier Wenceslao, *Blockchain: primeras cuestiones en el ordenamiento español,* Dykinson, Madrid, 2018.

JAMARDO LORENZO, Andrea, «La cadena de custodia: configuración jurídica y estado actual de la cuestión», *Justicia: revista de derecho procesal*, núm. 1, 2024, pp. 299-398.

JAMARDO LORENZO, Andrea, *Construcción jurisprudencial y evolución de la cadena de custodia: análisis sistemático*, Colex, A Coruña, 2024.

KAPLAN, Jerry, *Artificial Intelligence. What everyone needs to know*, Oxford University Press, Nueva York, 2016.

LEMUS SOLER, Diana Julieth, «Cadena de custodia en el ordenamiento jurídico colombiano a la luz de la Ley 906, ¿ficción o realidad?», *Revista Iter ad Veritatem,* núm. 12, 2014.

LARO GONZÁLEZ, Elena, *La Orden Europea de Investigación en el Espacio Europeo de Justicia,* Tirant lo Blanch, Valencia, 2021.

LÓPEZ VALERA, Manuel, «Localización, hallazgo y recogida de muestras de ADN en la cadena de custodia», *Revista de Derecho UNED*, núm. 19, 2016, pp. 777-808.

MAGRO SERVET, Vicente, «¿Cómo aportar la prueba digital en el proceso penal?», *Diario la Ley,* núm. 9824, 2021.

MANSILLA MOYA, Mario Moisés/MANSILLA MOYA, Mateo, «Cadena de custodia 2.0», *Revista Mexicana de Ciencias Penales,* vol. 5, núm. 8, 2022, pp. 47-61.

MARÍN GONZÁLEZ, Juan Carlos/GARCÍA SÁNCHEZ, Guillermo, «Problemas que enfrenta la prueba digital en los Estados Unidos de América», *Revista de Estudios de Justicia*, núm. 21, 2014, pp. 75-91.

MARTÍN DIZ, Fernando, «Inteligencia artificial y derecho procesal: luces, sombras y cábalas en clave de derechos fundamentales», en MORENO CATENA, Víctor/ROMERO PRADAS, María Isabel (dirs.), *Nuevos postulados de la cooperación judicial en la Unión Europea. Libro homenaje a la Prof[a]. Isabel González Cano*, Tirant lo Blanch, Valencia, 2021, pp. 969-1006.

MARTÍN RÍOS, Pilar, «Problemas de admisibilidad de la prueba obtenida de dispositivos de almacenamiento digital», *Revista General de Derecho Procesal,* núm. 51, 2020.

MARTÍNEZ GALINDO, Gema, «Problemática jurídica de la prueba digital y sus implicaciones en los principios penales», *Revista Electrónica de Ciencia Penal y Criminología*, núm. 24, 2022.

MCCARTHY, John/MINKSKY, Marvin L./ROCHESTER, Nathaniel/SHANNON, Claude E., «A proposal for the Dart-mouth Summer Research Project on Artificial Intelligence, August 31, 1955», Al Magazine, Vol. 27, núm. 4, 2006, pp. 12-14.

MERKEL, Laura, *Derechos humanos e investigaciones policiales. Una tensión constante*, Marcial Pons, Madrid, 2022.

MESTRE DELGADO, Esteban «La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos», en FIGUEROA NAVARRO, Carmen (dir.), *La cadena de custodia en el proceso penal*, Edisofer, Madrid, 2015, pp. 39-79.

MIRÓ LLINARES, Fernando, *El cibercrimen: fenomenología y criminología de la ciberdelincuencia en el ciberespacio*, Marcial Pons, Madrid, 2012.

MORENO CATENA, Víctor/CORTÉS DOMÍNGUEZ, Valentín, *Derecho Procesal Penal*, Tirant lo Blanch, Valencia, 2004.

NIEVA FENOLL, Jordi, *La valoración de la prueba,* Marcial Pons, Madrid, 2010.

NIEVA FENOLL, Jordi, *Inteligencia artificial y proceso judicial*, Marcial Pons, Madrid, 2018.

NIEVA FENOLL, Jordi, «La prueba preconstituida: un concepto erróneo e imposible», *Diario la Ley,* núm. 10532, 2024.

NILSSON, Nils, *The Quest for Artificial Intelligence: A History of Ideas and Achievements*, Cambridge University Press, Nueva York, 2010.

ORTEGO PÉREZ, Francisco, «Los medios de investigación relativos al cuerpo del delito», en JIMÉNEZ CONDE, Francisco/FUENTES SORIANO, Olga (dirs.), *Reflexiones en torno al Anteproyecto de Ley de Enjuiciamiento Criminal de 2020,* Tirant lo Blanch, Valencia, 2022, pp. 733-756.

ORTIZ PADRILLO, Juan Carlos, *Problemas procesales de la ciberdelincuencia*, Colex, A Coruña, 2013.

PAULESU, Pier Paolo, «Inteligencia Artificial y proceso penal italiano: una panorámica», en MARTÍN RÍOS, Pilar/VILLEGAS DELGADO, César (dirs.), *La tecnología y la inteligencia artificial al servicio del proceso,* Colex, A Coruña, 2023, pp. 261-281.

PEREIRA PUIGVERT, Silvia, «Sistema de hash y aseguramiento de la prueba informática. Especial referencia a las medidas de aseguramiento adoptadas inaudita parte», en BUENO DE MATA, Federico (dir.), *Fodertics II: hacia una justicia 2.0,* 2014, Comares, Granada, pp. 75-83.

PÉREZ CAMPILLO, Lorena, «Blockchain: ¿amenaza o solución en la protección de datos y privacidad?», en BUENO DE MATA, Federico (dir.), *Fodertics 7.0: estudios sobre derecho digital,* Comares, Granada, 2019, pp. 261-268.

PÉREZ DAUDÍ, Vicente, «La prueba electrónica: naturaleza jurídica e impugnación», en ASENCIO MELLADO, José María (dir.), *Derecho probatorio y otros estudios procesales. Liber Amicorum: Vicente Gimeno Sendra*, Ediciones Jurídicas Castillo de Luna, Madrid, 2020, pp. 1557-1576.

PÉREZ GIL, Julio, «Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal», en JIMÉNEZ CONDE, Francisco/BELLIDO PENADÉS, Rafael (dirs.), *Justicia: ¿garantías versus eficiencia?*, Tirant lo Blanch, Valencia, 2019, pp. 399-441.

RICHARD GONZÁLEZ, Manuel, «La cadena de custodia en el proceso penal», *Diario la Ley,* núm. 8187, 2013.

RICHARD GONZÁLEZ, Manuel, «La investigación y prueba de hechos y dispositivos electrónicos», *Revista General de Derecho Procesal,* núm. 43, 2017.

ROCA MARTÍNEZ, José María, «Nuevas tecnologías e investigación penal: garantías ante injerencias y motivación de su autorización», en FERNÁNDEZ VILLALÓN, Luis Antonio (coord.), *Derecho y nuevas tecnologías*, Civitas, Navarra, 2020, pp. 71-92.

ROTHSTEIN, Paul F., *Federal Rules of Evidence*, 3ª ed., Thomson Reuters, Eagan, 2021.

RUBIO ALAMILLO, Javier, «Conservación de la cadena de custodia de una evidencia informática», *Diario la Ley*, núm. 8859, 2016.

RUBIO ALAMILLO, Javier, «Cadena de custodia y análisis forense de smartphones y otros dispositivos móviles en procesos judiciales», *Diario la Ley*, núm. 9300, 2018.

SÁNCHEZ MELGAR, Julián, «La nueva regulación de las medidas de investigación tecnológica. Estudio de su parte general», *Práctica penal: cuaderno jurídico*, núm. 82, 2016, pp. 20-32.

SÁNCHEZ RUBIO, Ana, «Cadena de custodia y prueba electrónica: la mismidad del hash como requisito para la fiabilidad probatoria», en BUENO DE MATA, Federico (dir.), *FODERTICS 7.0: estudios sobre derecho digital*, Comares, Granada, 2019, pp. 289-299.

SANJURJO RÍOS, Eva Isabel, «Proceso penal y volatilidad/mutabilidad de las fuentes de prueba electrónicas: sobre la conveniencia y el modo de asegurarlas eficazmente», en GONZÁLEZ GRANDA, Piedad (dir.), *Exclusiones probatorias en el entorno de la investigación y prueba electrónicas,* Reus, Madrid, 2020, pp. 195-224.

SANTISTEBAN CASTRO, María, «Algunas consideraciones en torno al valor probatorio de la tecnología blockchain en el ámbito europeo: presente y futuro», *La Ley probática,* núm. 12, 2023.

SCHWAB, Klaus, *La cuarta revolución industrial*, Debate, Barcelona, 2016.

SIMARRO PEDREIRA, Margarita, «La cadena de custodia en la prueba digital: España vs. EEUU», en GONZÁLEZ GRANDA, Piedad (dir.), *Exclusiones probatorias en el entorno de la investigación y prueba electrónica,* Reus, 2020, pp. 225-237.

SOANA, Giulio, «Block-chain y prueba digital. Una oportunidad para la cadena de custodia», en PEREIRA PUIGVERT, Silvia/ORDÓÑEZ PONZ, Francesc (dirs.), *Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos*, Aranzadi, Navarra, 2021, pp. 605-628.

TARUFFO, Michele, *La prueba de los hechos* (trad. Ferrer Beltrán), Trotta, Madrid, 2002.

TARUFFO, Michele, «La aplicación de estándares científicos a las ciencias sociales y forense», en VÁZQUEZ ROJAS, María del Carmen (dir.), *Estándares de prueba y prueba científica. Ensayos de epistemología jurídica*, Marcial Pons, Madrid, 2013, pp. 203-213.

TURING, Alan M., «Computing machine and intelligence», *Mind,* vol. 59, 1950, pp. 433-460.

VEGAS TORRES, Jaime, «Las medidas de investigación tecnológica», en CEDEÑO HERNÁN, Marina (coord.), *Nuevas tecnologías y Derechos Fundamentales en el proceso*, Aranzadi, Navarra, 2017, pp. 21-47.

VELASCO NÚÑEZ, Eloy, *Delitos tecnológicos: definición, investigación y prueba en el proceso penal,* Sepín, Madrid, 2015.

VELASCO NÚÑEZ, Eloy, «Investigación penal y protección de datos», *El cronista social y democrático de Derecho*, núm. 88-89, 2020, pp. 136-151.

XAVIER JANUÁRIO, Túlio Felippe, «Vulnerabilidad e hiposuficiencia 4.0: la protección jurídico-penal de los consumidores en la era de la inteligencia artificial», en FONTESTAD PORTALÉS, Leticia (dir.), *La Justicia en la sociedad 4.0: nuevos retos en el siglo XXI,* Colex, A Coruña, 2023, pp. 187-200.