Revista de Estudios Europeos
Publicación del Instituto Universitario de Estudios Europeos de la Universidad de Valladolid
EDICIONES Universidad Valladolid

Blockchain como medio de prueba electrónico en el marco de un proceso penal transfronterizo frente al ciberdelito*

Blockchain as electronic evidence in cross-border criminal proceedings against cybercrime

JAIME CRIADO ENGUIX
Universidad de Granada
jaimecriado@ugr.es
ORCID: 0000-0003-3894-2610
Recibido:14/10/2024 Aceptado:22/11/2024.
Cómo citar: Criado Enguix, Jaime "Blockchain como medio de prueba electrónico en el marco de un proceso penal transfronterizo frente al ciberdelito", *Revista de Estudios Europeos* 85 (2025): 492-527.

DOI: https://doi.org/10.24197/ree.85.2025.492-527

Resumen: El desarrollo tecnológico actual en Europa ha suscitado nuevas formas de criminalidad, con pautas de actuación novedosas, y una clara dificultad de rastreo, lo que ha mermado la eficacia de los instrumentos procesales para su seguimiento, detección y prueba. El cibercrimen está en auge, y rasgos que le son propios como el fácil acceso, las múltiples jurisdicciones implicadas, la globalización, y el anonimato del infractor, demanda un tratamiento procesal transfronterizo, adaptado a los parámetros de esta nueva técnica. Por ello, en este contexto, se propone ahondar en *blockchain*, tecnología que por sus características – descentralizada y anónima - ha cobrado una importante relevancia para la dogmática probatoria, ya que permite identificar fiablemente su trazabilidad a lo largo del tiempo, obteniendo para el escenario de la actividad procesal penal, una evidencia sólida que permite determinar algún tipo de responsabilidad penal. Se trata de analizar la viabilidad de esta tecnología para la conservación de pruebas electrónicas, que puede ser incorporada al proceso penal por diferentes medios de prueba.
Palabras clave: Cibercrimen, Instrumento Procesal, Prueba, *Blockchain*.

* Este trabajo ha sido realizado en el ámbito del Proyecto: Módulo Jean Monnet "Challenges and strategic profiles of the EU in the fight against organised crime" (Retos y perfiles estratégicos de la Unión Europea en la Lucha contra el Crimen Organizado. (RUECO)) 2023-2026, con referencia Erasmus-Jean Monnet 2023 Module. Ref. 101127315; y Red de Cooperación internacional y de excelencia científica de estudio y análisis "Justicia, Derecho, Constitución y Proceso".

Abstract: The current technological development in Europe has given rise to new forms of criminality, with novel patterns of action, and a clear difficulty in tracing them, which has reduced the effectiveness of procedural instruments for tracking, detecting and proving them. Cybercrime is on the rise, and its own characteristics, such as easy access, the multiple jurisdictions involved, globalisation and the anonymity of the offender, require cross-border procedural treatment, adapted to the parameters of this new technique. Therefore, in this context, it is proposed to delve into blockchain, a technology which, due to its characteristics - decentralised and anonymous - has gained an important relevance for evidential dogmatics, as it allows to reliably identify its traceability over time, obtaining for the scenario of criminal procedural activity, a solid evidence that allows to determine some type of criminal liability. The aim is to analyse the viability of this technology for the preservation of electronic evidence, which can be incorporated into criminal proceedings by different means of evidence.

Keywords: Cybercrime, Procedural Instrument, Evidence, *Blockchain*.

1. EL FENÓMENO DE INTERNET COMO PRINCIPAL ALIADO DEL CIBERCRIMEN

Ya el último informe SOCTA[1], publicado por Europol el 12 de abril de 2021, identificó como una de las amenazas más apremiantes para la UE los ataques cibernéticos, cuestión que ha experimentado un notorio crecimiento no sólo en términos cuantitativos, sino también en cuanto a la sofisticación de sus procedimientos

La delincuencia organizada tradicional atraviesa una especie de transición tecnológica, al servirse de las innumerables prestaciones y facilidades que proporciona Internet para desarrollar acciones delictivas y tener acceso a herramientas más sutiles, indetectables y sofisticadas.

El Secretario General de Interpol, Jürgen Stock, durante la 8ª Conferencia de Interpol y Europol sobre Ciberdelincuencia en 2020, declaró que "*en un mundo en el que más de 4.500 millones de personas están conectadas, más de la mitad de la humanidad corre el peligro de caer víctima de la ciberdelincuencia en cualquier momento*".

El mencionado informe revela que, ante la ausencia de cambios fundamentales, el ciberdelito evoluciona rápidamente. Declara que los

[1] Europol, Informe SOCTA (Serious and Organized Crime Threat Assessment): *La amenaza de la Delincuencia Organizada y Grave en la Unión Europea*, 2021. Gobierno de España. Gabinete de la Presidencia del Gobierno (Departamento de Seguridad Nacional). Disponible en el siguiente enlace: https://www.dsn.gob.es/es/actualidad/sala-prensa/informe-socta-2021-amenaza-delincuencia-organizada-grave-unión-europea [Fecha de consulta: 04/12/2023].

delincuentes están aumentando su seguridad operativa ocultando su actividad en línea y utilizando canales de comunicación más seguros.

Frente a ello, el Consejo de la UE emitió, en mayo de 2021, unas conclusiones en las que establece las prioridades de la UE en la lucha contra la delincuencia grave y organizada para 2022-2025 a través de la plataforma multidisciplinar europea contra las amenazas delictivas (EMPACT - *European Multidisciplinary Platform Against Criminal Threats* -)[2] a saber: redes delictivas de alto riesgo, ciberataques, trata de seres humanos, explotación sexual de menores, tráfico ilícito de migrantes, tráfico de drogas, fraude, delitos económicos y financieros, delincuencia organizada contra la propiedad, delitos contra el medioambiente, y tráfico de armas de fuego.

Por otro lado, conforme establece la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las regiones sobre la Estrategia de la UE contra la Delincuencia Organizada 2021-2025[3], el cuarto objetivo consiste en la necesidad de adaptar a las autoridades policiales y judiciales a la Era Digital, por cuanto "*más del 80 % de los delitos tienen un componente digital*".

Asistimos, además, a una tendencia delictiva al alza, y que, en términos del Consejo Europeo, "*seguirá agravándose en el futuro, ya que se espera que 22.300 millones de dispositivos en todo el mundo estén conectados a la internet de las cosas de aquí a 2024*"[4].

Y es que, en efecto, el crimen organizado se sirve de los avances tecnológicos para perpetrar el delito de forma trasnacional, compleja e "invisible", y que éste resulte provechoso. Se trata, sin duda, de un aliado que se adapta perfectamente a las características propias de este tipo de criminalidad. Como bien apunta RUÍZ RODRÍGUEZ y GONZÁLEZ AGUDELO[5] "*anonimato, distancia, reducción de la prueba documental, ubicuidad, mantenimiento de redes flexibles y complejas, son todas*

[2] Iniciativa emblemática de la UE en la lucha contra la delincuencia organizada.
[3] COM (2021) 170 final. Bruselas, 14.4.2021.
[4] Consejo Europeo/Consejo de la Unión Europea, *Ciberseguridad: cómo combate la UE las amenazas cibernéticas*, 2024. Disponible en el siguiente enlace web: https://www.consilium.europa.eu/es/policies/cybersecurity/ Fecha de consulta: [20/12/2023]
[5] Ruíz Rodríguez, L.R., González Agudelo, G. (2014), "El factor tecnológico en la expansión del crimen organizado" en *Centro de Investigación Interdisciplinaria en Derecho Penal Económico* (CIIDPE), p. 10.

características idóneas que, como cualquier otra organización empresarial, las redes delictivas han asumido de forma inmediata y con clara visión economicista".

En España, a tenor de la Estrategia Nacional contra el Crimen Organizado 2019-2023[6], la delincuencia avanza de forma progresiva hacia nuevas perspectivas cada vez más sofisticadas, y digitalizadas, mediante estructuras y métodos variados[7].

Este fenómeno digital ha suscitado nuevas formas de criminalidad – como estafas, robos de datos personales, suplantación de identidad, *phishing*, o amenazas de la ingeniería social[8] - con diferentes niveles de riesgo, y mayor dificultad de rastreo.

Además, la ciberdelincuencia implica en su mayoría investigaciones transfronterizas, pues las víctimas y los delincuentes, así como los prestadores de servicios, suelen estar localizados en diferentes países. Esto, sin duda, plantea un reto para los investigadores, ya que normalmente los países entre sí tienen una regulación sustantiva y procesal distinta en torno al ciberdelito, lo que la Interpol define como "*complejidad interjurisdiccional*"[9], que desemboca en asimetrías y descoordinaciones. Esta circunstancia ha mermado la eficacia de los instrumentos procesales para su prevención, detección y prueba, erigiéndose su persecución penal en un verdadero desafío para los actores judiciales implicados.

Basta consultar los últimos pronunciamientos judiciales, y titulares de prensa, para comprobar que los casos de ciberataques con impacto transfronterizo han ido *in crescendo* en los últimos años. Por citar los casos más sonados, señálese uno de los más perjudiciales contra la infraestructura petrolera de un país, el caso del oleoducto *Colonial Pipeline* de EEUU, en mayo de 2021, el cual sufrió un ataque de

[6] BOE, núm. 46, Sec. I, p. 17048, 22 de febrero de 2019.

[7] Garrido Carrillo, F.J. (2022), "Prólogo. Retos, amenazas, instrumentos y experiencias en la lucha contra el crimen organizado" en Garrido Carrillo, F.J. (Dir.), *Respuesta Institucional y normativa al Crimen Organizado. Perfiles estratégicos para una lucha eficaz*, Ed. Aranzadi, Navarra, p. 19.

[8] Que son aquellas que tratan de aprovechar un error o comportamiento humanos para obtener acceso a información o servicios. Según informa la UE, el 82% de las violaciones de la seguridad de los datos tuvieron un componente humano. *Vid*. Consejo Europeo, *Infografía – Principales ciberamenazas en la UE*, 2023.

[9] *Vid*., Interpol, *Guía sobre la Estrategia Nacional contra la Ciberdelincuencia*, abril 2021, p. 15. Disponible en el enlace web: https://www.interpol.int/es/Pagina-de-busqueda?search=gu%C3%ADa+sobre+la+estrategia+nacional Fecha de consulta: [25/12/2023].

malware[10], que supuso la paralización del suministro de energía en EEUU, y un gasto público de 4.4 millones de dólares a los ciberdelincuentes para pagar el rescate del programa. O, por ejemplo, la reciente ciberestafa conspirada por *hackers* que aprovecharon la situación de Ucrania para, por vía de técnicas de *phishing*, incitar a los usuarios a "ayudar a Ucrania" mediante donaciones a direcciones de *Bitcoin* y *Ethereum* falsificadas, y no afiliadas al gobierno ucraniano[11]. O, el ciberataque provocado contra la compañía aérea *Air Europa* el pasado octubre de 2023, que alertaba del acceso no autorizado por ciberdelincuentes a datos de las tarjetas para realizar compras en la web de la compañía[12]. O, en el ámbito de la investigación y la cultura, en octubre de 2023, no se puede obviar el ciberataque contra la prestigiosa *British Library* (Biblioteca Británica, en Londres) que fue víctima de un grupo de *ransomware* Rhysida. Este grupo exigió un rescate de setecientos mil euros y, ante la negativa por parte de la institución de pagar el monto exigido, decidió filtrar información sobre los empleados en la *darkweb*[13]. También, con ocasión del auge de los sistemas inteligentes, se vienen lanzando ciberataques por vía de IA, para una perpetración del delito más ingeniosa e indetectable. Sin duda, los ataques más frecuentes son de *phishing* y de suplantación de identidad.

Sin ir más lejos, el pasado 14 de marzo, la Guardia Civil alertó de una estafa de phishing dirigida a los usuarios de Netflix. Según explica INCIBE, "*estos correos emplean mensajes de emergencia titulados como "el último recordatorio antes del cierre de la cuenta", creando una sensación de pánico en el usuario y que de esta manera no piense y quiera*

[10] Este consiste en un programa malicioso, un tipo de software que realiza acciones dañinas en un sistema informática de forma intencionado y sin conocimiento del usuario.
[11] Caso descrito en el reciente Informe IOCTA, *Internet organised crimen threat assessment* – 2023, emitido por Europol. Disponible en: https://www.europol.europa.eu/publications-events/main-reports/iocta-report Fecha de consulta: [01/01/2024].
[12] Nota de prensa, La Sexta, Sección Economía: *¿Qué hacer si eres uno de los clientes afectados por el ciberataque de Air Europea?*, 10 de octubre de 2023. Disponible en línea:https://www.lasexta.com/noticias/economia/que-hacer-eres-uno-clientes-afectados-ciberataque-air-europa_2023101065251ef1b2ab5700016fed89.html [Fecha de consulta: [15/01/2024].
[13]*Vid*. CSO Computer World España: Los sistemas de la *British Library* aún no se recuperan tres meses después de su peor ciberataque, redacción 25 de enero de 2024. Disponible en línea: https://cso.computerworld.es/cibercrimen/los-sistemas-de-la-british-library-aun-no-se-recuperan-tres-meses-despues-de-su-peor-ciberataque [Fecha de consulta: [15/01/2024].

solucionar ese supuesto problema de manera rápida y sin verificar el mensaje". Mediante la técnica phishing, se estafa a los usuarios para conseguir sus datos personales y bancarios[14].

La situación descrita permite extraer una conclusión clara, y es que el ciberdelito puede adoptar múltiples formas, y adentrarse de un modo imperceptible en cualquier sector o industria, lo cual exige por parte de la UE una respuesta eficaz y adaptada, en sede normativa e institucional.

2. REACCIÓN NORMATIVA E INSTITUCIONAL DE LA UE FRENTE AL CIBERDELITO. ESPECIAL ATENCIÓN A LA PRUEBA ELECTRÓNICA

El marco normativo es amplio, y fundamental, para garantizar una armonización europea en la lucha contra el ciberdelito. Por ello, es prolija la producción de normas en el ámbito de la ciberseguridad.

Así pues, ha visto la luz recientemente el Reglamento (UE, Euratom) 2023/2841 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, por el que se establecen medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión[15]. Esta norma jurídica ha implantado medidas específicas - como un marco único de certificación a escala de la UE, o un Consejo Interinstitucional de Ciberseguridad – destinadas a generar confianza, y aumentar el crecimiento del mercado de la ciberseguridad en Europa.

En 2022, la UE adoptó una revisión de la Directiva SRI (SRI 2) para sustituir la Directiva de 2016, que entraría en vigor en 2023, con medidas jurídicas para impulsar el nivel global de ciberseguridad en la UE, exigiendo a los Estados Miembros que estén debidamente equipados. Asimismo, implantó un sistema de trabajo mediante la creación de un Grupo de Cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros.

Por otro lado, también se ha trabajado en el plano estratégico. La Comisión Europea y el Servicio Europeo de Acción Exterior (SEAE) presentaron, a finales de 2020, una nueva Estrategia de Ciberseguridad de la UE, con el objeto de reforzar la resiliencia de Europa frente a las

[14] *Vid*.,Comunicado de prensa en *20 minutos.es* Disponible en: https://www.20minutos.es/tecnologia/ciberseguridad/guardia-civil-alerta-estafa-phishing-netflix-5227381/ Fecha de consulta: [15/01/2024]

[15] DOE núm. 2841, de 18 de diciembre de 2023.

ciberamenazas, y garantizar que todos los ciudadanos y empresas puedan beneficiarse plenamente de servicios y herramientas digitales seguros y fiables.

Por su parte, el 22 de marzo de 2021, el Consejo adoptó unas Conclusiones sobre la Estrategia de Ciberseguridad[16] en las que destacó que la ciberseguridad es esencial para construir una Europa resiliente, ecológica y digital. Los ministros de la UE fijaron como objetivo clave lograr la autonomía estratégica preservando al mismo tiempo una economía abierta, para lo cual es necesario aumentar la capacidad de adoptar decisiones autónomas en el ámbito de la ciberseguridad con el fin de reforzar el liderazgo digital y las capacidades estratégicas de la UE.

A la vista de este marco normativo, y de la línea estratégica de Europa[17], se puede inferir que se está actuando frente a una modalidad delictiva absolutamente globalizada, que ha traído consigo una considerable disrupción en todos los órdenes, a nivel social, político, económico, y jurídico, entre otros.

El anterior contexto trae causa del actual incremento del movimiento de personas, bienes y capitales, tanto a nivel europeo como internacional, que venimos asistiendo. Este fenómeno, como bien indica AUGUSTO DEPETRIS[18], ha superado con creces el desarrollo de los mecanismos estatales para el control de la actividad delictiva, y el intercambio de información, factor que, entre otros, ha favorecido la expansión del ciberdelito.

La tecnología ha evolucionado al mismo ritmo que dicho proceso, propiciando un nuevo paradigma. La evolución de la informática, si bien ha proporcionado utilidades a los usuarios en materia de información y conocimiento, lo cierto es que a su vez ha suscitado nuevas formas de realización de la actividad delictiva. Ello obedece a los aspectos relacionados con la irrupción de Internet como una red de alcance global,

[16] Consejo de la Unión Europea, *Conclusiones del Consejo sobre la Estrategia de Ciberseguridad de la UE para la Década Digital*. Bruselas, 9 de marzo de 2021. 6722/21.
[17] Para un análisis más exhaustivo en torno a la génesis normativa y la evolución de la obtención transnacional de la prueba electrónica en materia penal, se recomienda vivamente la lectura de la obra de Tinoco Pastrana, Á., "Las órdenes europeas de entrega y conservación: la futura obtención transnacional de la prueba electrónica en los procesos penales en la Unión Europea", *Cuadernos de Política Criminal*, núm. 135, III, Época II, diciembre 2021, pp. 205 y ss.
[18] Augusto Depetris, J. (2021), "Organizaciones criminales digitales: conocerlas para enfrentar su desafío" en *Revista del CLAD Reforma y Democracia*, núm. 79, p. 141.

que facilita no sólo una inmediatez en el resultado, sino además la encriptación, el anonimato, la inmediatez de la mensajería y la deslocalización; factores estos que, además, han secundado la aparición de verdaderos problemas de índole procesal si se parte de las previsiones jurídicas tradicionales.

En síntesis, lo que se pretende destacar es que los medios tecnológicos han favorecido la globalización e interconexión entre países, y los criminales han sabido aprovechar las prestaciones que estas técnicas ofrecen para "*ocultar no sólo sus actividades delictivas sino también todos los productos de sus delitos*"[19]. Internet es "*causa y a su vez consecuencia de la globalización*"[20], y ello ha provocado, explica MORILLAS CUEVA, una suerte de "*simbiosis*" entre globalización y delincuencia organizada, por cuanto la "*cada vez más intensa interdependencia entre países (...) propicia un evidente cauce extensivo para la criminalidad organizada y sus actividades, (…) con provecho de los nuevos cauces de actuación que semejantes hipótesis posibilitan para sus objetivos criminales*[21]".

La principal amenaza radica, pues, en que el crimen organizado se viene adaptando a los avances tecnológicos, modificando sus pautas de actuación y logrando ocupar los espacios concretos de impunidad, que la ausencia de una regulación específica, le permite.

GARRIDO CARRILLO sostiene que "*si el crimen organizado trasciende las fronteras de los Estados, no caben únicamente respuestas nacionales, aunque se planteen de forma coordinada, pues esto en definitiva es trasladar los problemas de un país a otro, lo que hay que hacer es plantear una respuesta internacional y global ante este conflicto*"[22].

---

[19] Alarcón-Jiménez, O. (2019), "La aportación del Consejo de Europa en la lucha contra el crimen organizado transnacional" en AA.VV. Galán Muñoz, A., Mendoza Calderón, S. (Dirs.), *Globalización y lucha contra las nuevas formas de criminalidad transnacional*. Ed. Tirant lo Blanch, España, p. 96.

[20] Díaz Gómez, A. (2010), "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest", en *REDUR* 8, p. 171.

[21] Morillas Cueva, L. (2022), "Globalización y delincuencia organizada. Respuestas penales" en AA.VV. Garrido Carrillo, F.J., (Dir.), Faggiani, V. (Coord.), *Respuesta institucional y normativa al crimen organizado. Perfiles estratégicos para una lucha eficaz*, Ed. Aranzadi, España, p. 50.

[22] Garrrido Carrillo, F.J. (2022), "Prólogo. Retos, amenazas, instrumentos y experiencias en la lucha contra el crimen organizado" en AA.VV. Garrido Carrillo, F.J., (Dir.),

En efecto, los esfuerzos normativos y estratégicos adoptados por el momento han resultado ineficientes, prueba de ello es el reciente comunicado del Consejo Europeo, según el cual el coste anual mundial de la ciberdelincuencia asciende a 5,5 billones de euros[23].

Para acometer esta realidad, se considera necesario una visión holística del problema, o como lo define SEGURA SERRANO, "*un estudio omnicomprensivo del fenómeno*"[24] ya que, junto a la amenaza para el ciberespacio, han emergido otras de carácter estrictamente jurídico que no han recibido la necesaria atención, y que concretamente afecta a la eficacia de los instrumentos procesales tradicionales para la investigación, y enjuiciamiento del ciberdelito. Efectivamente, un inconveniente en la lucha contra este tipo de criminalidad estriba en el carácter obsoleto de los actuales mecanismos procesales previstos en la normativa. Apremia incorporar en el marco de una investigación judicial europea, medios de investigación y de prueba tecnológicos, con una utilidad y un peso específico dentro del proceso.

Parece lógico pensar que a medida que aumentan los actos delictivos vía Internet, las autoridades judiciales y policiales dependen cada vez más de las pruebas electrónicas para luchar contra este tipo de delincuencia. Es una cuestión de "*adaptarse al medio delictivo*", para con ello soslayar las grietas de nuestro sistema procesal, y la posibilidad de que el delito quede impune. Una opción para ello es, sin duda, la prueba electrónica, pues este tipo de prueba "*se necesita en cerca del 85% de las investigaciones penales y, en dos tercios de estas investigaciones, es preciso obtener pruebas de proveedores de servicios en línea establecidos en otra jurisdicción*"[25].

Por lo tanto, está claro, afirma DE HOYOS SANCHO[26], que es "*imprescindible disponer de instrumentos normativos que permitan a las*

Faggiani, V. (Coord.), *Respuesta institucional y normativa al crimen organizado. Perfiles estratégicos para una lucha eficaz*, Ed. Aranzadi, España, p. 19.

[23] Información en: https://www.consilium.europa.eu/es/policies/cybersecurity/ Fecha de consulta: [06/02/2024].

[24] Segura Serrano, A. (2023), *El desafío de la ciberseguridad global*, Ed. Tirant lo Blanch, p. 14.

[25] Recomendación de DECISIÓN DEL CONSEJO por la que se autoriza la apertura de negociaciones para un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el acceso transfronterizo a las pruebas electrónicas para la cooperación judicial en materia penal. COM(2019) 70 final, Bruselas, 5.2.2019.

[26] De Hoyos Sancho, M. (2023), "Novedades en materia de obtención transfronteriza de información electrónica necesaria para la investigación y enjuiciamiento penal en el

autoridades competentes esa información electrónica (…) de manera selectiva, rápida y fiable, al tiempo que se asegura el pleno respeto de los derechos esenciales (…)".

En este sentido, ha visto la luz, recientemente, el Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales[27]. Se trata de una medida de cooperación judicial en materia penal, basada en el principio de reconocimiento mutuo, por la cual la autoridad judicial competente de un Estado miembro puede ordenar directamente a un proveedor de servicios que ofrezca sus servicios en la UE que entregue pruebas electrónicas (orden de entrega) o prohibirle que las destruya mientras se tramita la orden de entrega o una orden europea de investigación (orden de conservación).

Asimismo, se viene colaborando con EEUU, como territorio estratégico por cuanto alberga las sedes de los mayores proveedores de servicios, y constituye uno de los principales receptores de solicitudes de asistencia judicial mutua emitidas desde los Estados miembros de la Unión Europea (y desde el resto del mundo) para acceder a las pruebas electrónicas. El marco legal utilizado hasta ahora es el marco general de asistencia judicial penal pero la lentitud de este mecanismo ha motivado que se haya recurrido a la colaboración voluntaria de los proveedores norteamericanos, como vía alternativa a la cooperación judicial[28]. Actualmente, dichas negociaciones siguen abiertas, con miras a que en un futuro escenario las autoridades judiciales europeas puedan dirigirse directamente a las empresas norteamericanas, con las debidas garantías.

En relación a esta misma materia, el Consejo ha autorizado la participación de la UE en las negociaciones del segundo protocolo adicional al Convenio de Budapest sobre Ciberdelincuencia. Se trata de un tratado multilateral que reunirá a Estados con ordenamientos jurídicos muy distintos de los propios de los países miembros de la UE, y que tiene por

ámbito europeo", *Revista de Estudios Europeos*, núm. extraordinario monográfico 1, pp. 100-101.

[27] y de ejecución de penas privativas de libertad a raíz de procesos penales. DOUE núm. 191, de 28 de julio de 2023.

[28] *Vid*., Recomendación de DECISIÓN DEL CONSEJO por la que se autoriza la apertura de negociaciones para un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el acceso transfronterizo a las pruebas electrónicas para la cooperación judicial en materia penal. COM/2019/70 final. Bruselas, 5 de febrero de 2019.

objeto diseñar mecanismos de asistencia mutua más efectivos, en particular, mediante la cooperación directa con los proveedores de internet radicados en otras jurisdicciones.

Retomando el antecitado Reglamento (UE) 2023/1543, parece que el legislador ha acogido las apreciaciones de la doctrina[29], al incorporar en su texto (Capítulo V) los sistemas informáticos descentralizados como canal seguro y fiable para el intercambio de datos provenientes de una orden europea de producción y conservación de pruebas electrónicas.

Esta medida, efectivamente, permite incorporar un sistema informático descentralizado – como podría ser *blockchain* (o cadena de bloques)– para la conservación de evidencias electrónicas obtenidas en el marco de una investigación europea. Avance que si bien resulta oportuno – por cuanto incorpora, como venimos reclamando, medidas tecnológicas al proceso penal europeo– lo cierto es que deja algunos aspectos procesales sin resolver. Concretamente, no responde al interrogante procesal de cuál podría ser el medio de prueba idóneo para que la información almacenada en la cadena de bloques pueda acceder al proceso penal, y hacer prueba plena del hecho, acto o estado de cosas que documenta.

Ante esta laguna procesal en la norma europea[30], nos proponemos analizar, desde la óptica de la legislación procesal española, el medio idóneo a través del cual se podría hacer valer la fuente de prueba *blockchain* recabada en una investigación europea, en un eventual proceso penal español, y servir con ello de verificación fehaciente de los hechos que acredita.

[29] En este sentido, cabe destacar la postura de BUENO DE MATA, quien, en su momento, acertadamente observó que las iniciativas normativas – previas al actual Reglamento (UE) 2023/1543 - sólo se detenían en "*cuestiones vinculadas a la obtención y a la transferencia de pruebas electrónicas, (…) pero nada hasta ahora se ha dicho de la conservación de los datos ni de las técnicas propuestas para el mismo, cuestión crucial donde podría encajar la tecnología blockchain". Vid.,* Bueno de Mata, F. (2023), "Blockchain, identidad autosoberana y prueba electrónica transfronteriza" en AA.VV. Hernández López, A., Laro González, M.E. (Dirs.), *Proceso penal europeo: últimas tendencias, análisis y perspectivas*, Ed. Thomson Reuters Aranzadi, p. 74.

[30] La cual se limita, mínimamente, en el art. 20 Reglamento 2023/1543, a no denegar los efectos jurídicos de los documentos electrónicos, y a considerarlo admisibles en el contexto de los procesos judiciales transfronterizos por el mero hecho de estar en formato electrónico.

3. *BLOCKCHAIN* COMO FUENTE DE PRUEBA ELECTRÓNICA

3.1. Aproximación a la tecnología *blockchain*

Blockchain, como "idea" o "fundamento", se concibe como bastión de la libertad individual, garantizada por unos estándares mínimos, como el anonimato, la privacidad, y, principalmente, la elusión del control estatal. *Blockchain* - a riesgo de caer en un reduccionismo - aboga por una especie de anarquía, sin un ente jerárquicamente superior que centralice el poder sobre la plataforma.

Si se analiza bajo un prisma puramente técnico, el origen de este portento se atribuiría a los investigadores Stuart Haber y W. Scott Stornetta, quienes, en 1991, publicaron "*How to Time-Stamp a Digital Document*", esto es, una invención informática que permite registrar todo tipo de archivos multimedia en Internet, en un registro distribuido, de manera inmutable y confiable.

Tal sistema, si bien resultó novedoso, no desplegaría sus utilidades prácticas hasta transcurridas dos décadas desde su creación, por el 2008, cuando un grupo de personas - bajo el pseudónimo "Satoshi Nakamoto" – decidió emprender un sistema de dinero electrónico descentralizado entre pares - como alternativa al sistema de pago convencional - que permitiría transacciones con criptomonedas, como "Bitcoin"[31].

Actualmente, la cadena de bloques constituye una tecnología de registro distribuido, en la que su estructura almacena datos y a medida que llega una nueva información, la agrupa en un bloque, le asigna un código y la ubica en el orden consecutivo de la cadena, es allí que surge la denominación "cadena de bloques" o en su anglicismo "*blockchain*", para posteriormente ese bloque ser replicado a todos los nodos participantes en la red. Esa transferencia de bloques (o, mejor dicho, transferencia de datos) se denomina "transacciones".

Con el paso del tiempo, se apreció el carácter versátil de esta tecnología por su fácil aplicabilidad en diversos sectores, a saber: i) seguridad en *big data* mediante *blockchain*; ii) sistema de seguimiento de transportes; iii) ejecución automática de los *smart contracts* en *ethereum*; iv) o garantía de la prueba digital, por su carácter inmutable. Esta última

[31] No se tiene constancia clara de quién creó el bitcoin, pero algunos autores lo atribuyen al experto en seguridad informática Craig Steven, ciudadano australiano, que se amparó en el seudónimo "Satoshi Nakamoto", quien lo puso en circulación en 2009.

prestación trae causa de tres atributos fundamentales que hacen de *blockchain* una tecnología fiable y atractiva a efectos probatorios.

En primer lugar, es una plataforma segura. Esta cualidad se atribuye a la utilización de técnicas criptográficas en el momento de crear un nuevo bloque, que resumen su contenido por medio de un código denominado *hash*, el cual contiene el número de bloque creado, el número de transacciones establecidas, el código *hash* del bloque anterior, el nuevo código *hash* asignado y la respectiva firma digital; todo empaquetado bajo un código *hash*. Tal configuración evidencia que cada bloque de la cadena contiene el registro del código *hash* del bloque anterior, lo que imposibilita su alteración debido a que si se pretendiese cambiar la información, la misma debería ser cambiada en retroceso hasta la génesis del primer bloque, y adicional a ello y complicando aún más las cosas, debería hacer lo mismo en cada una de las copias almacenadas por cada uno de los participantes de la red, que en el caso de la red pública, son millones de nodos participantes. Es por ello que esta tecnología ofrece un alto grado de confianza y seguridad, puesto que el atacante requeriría una mayor potencia de cómputo superior a todos los nodos que conservan copia en toda la red.

En segundo lugar, *blockchain* se desenvuelve en un portal transparente, por cuanto todos los usuarios tienen acceso al libro registro, lo cual implica que tienen disponible la información sobre las transacciones que se efectúan por el grupo. Así ocurre, por ejemplo, en las redes *Bitcoin* o *Ethereum*. A esto se añade, además, que se trata de protocolos informáticos de código abierto, por lo que el acceso al diseño de la programación es también libre. Esta transparencia, sin embargo, no significa que podamos conocer al autor de las transacciones en todo caso. En algunos tipos de redes los usuarios no necesitan identificarse de forma personal para acceder y operar en la correspondiente red *blockchain*. Las transacciones son visibles, pero vinculadas a un código. Esta característica ha ocasionado que se hayan vinculado algunas de estas redes a actividades ilícitas por el crimen organizado debido el carácter anónimo en la actuación que permiten en ciertos casos.

Y, en tercero, la cadena de bloques almacena información, de forma irrevocable e inmutable. Irrevocable por cuanto una vez la información ha sido consensuada y verificada, se incorpora a una red *blockchain*, y ello no admite rectificación ni marcha atrás, pues cada usuario posee una copia de la información, lo que dificulta su alteración y eliminación de la red sin previo consenso de todos. E inmutable porque si un nodo decide cambiar

el contenido de la cadena de bloques alterando una transacción ya realizada e incluida en un bloque, provocará que el contenido de su versión del libro registro varíe, un cambio que será fácilmente identificable por el resto de los nodos. Por tanto, a la hora de someter a aprobación una nueva transacción, estos no aceptarán su versión del registro, puesto que el contenido será distinto. Esta última propiedad, "*sin equivalente en el mundo digital ni en el mundo real, tiene obvias aplicaciones*"[32] en el ámbito de la prueba digital.

3.2. Hacia la digitalización de la prueba mediante *blockchain*

La prueba como instrumento básico en la búsqueda de la verdad, y en la conformación de la verdad judicial, que es el soporte de la decisión jurisdiccional que adopta el órgano juzgador resolviendo los asuntos que se someten a su conocimiento, ha sido una cuestión a la que se le ha prestado la máxima atención, siendo múltiples y variados los análisis que sobre este tema se han llevado a cabo.

SENTÍS MELENDO[33] explica que, en su origen etimológico, prueba proviene del término latín *"probatio", "probationis"*, que, a su vez, procede del vocablo *probus*, que significa bueno. Por tanto, lo que resulta probado es bueno, fiel a la realidad. Por extensión, la acción de probar consiste en corroborar y verificar la autenticidad de una cosa.

Esta acción tiene aplicabilidad no sólo en el campo jurídico, sino también en otras disciplinas, como las ciencias experimentales, cuya metodología requiere de ensayos para probar hipótesis. También se aplica el término "prueba" en contextos de la vida cotidiana del ser humano.

Como explica CARNELUTTI[34], las fuentes de prueba son infinitas y los medios, finitos, de tal manera que cualquier fuente de prueba para su efectiva incorporación al proceso ha de hacerlo mediante un medio de prueba de los que están establecidos en nuestra normativa sustantiva y procesal.

Para este autor, la fuente de prueba es un concepto extraprocesal, que alude a una realidad anterior, exterior e independiente del proceso;

[32] Dolader Retamal, C., Bel Roig, J., Muñoz Tapia, J.L. (2017), "La blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas" en *Economía Industrial*, núm. 405, p. 39.

[33] Sentís Melendo, S., (1973), "Qué es la prueba (Naturaleza de la prueba)", *Revista de Derecho Procesal Iberoamericana*, núm. 2-3, pp. 259-260.

[34] Carnelutti, F. (1955), *La prueba civil*, Arayu, Buenos Aires, pp. 67 y ss

mientras que el medio de prueba es el instrumento de que se valen las partes para incorporar la fuente de prueba al proceso, de tal manera que se haga posible la apreciación judicial de dicho objeto[35].

En el concreto ámbito jurídico, la prueba adquiere una dimensión muy relevante en el terreno de la administración de justicia; DEVIS ECHANDÍA[36] afirmaba que básicamente ésta no sería posible sin la prueba.

La prueba es el eje central de un litigio, ya que permite al Juez conformar su convicción judicial, en un sentido o en otro.

Sobre esta materia, se han arrojado en el área procesal tantas definiciones como estudios se han llevado a cabo; en nuestro caso, tomaremos como referencia, por su claridad y precisión, la definición que aporta CORTES DOMINGUEZ[37], quien la define como aquella *"actividad encaminada a convencer al juez de la veracidad de unos hechos que se afirman existentes en la realidad"*.

Esta actividad, sin embargo, adquiere un cariz más complejo cuando se trata del cibercrimen transfronterizo, caracterizado por el anonimato del infractor, y la fugacidad del contenido *online* – extremos estos indispensables para conformar cualquier tipo de prueba-.

En el punto de la globalización en que nos encontramos, el intercambio de datos electrónicos entre las autoridades judiciales para recabar evidencias digitales se presenta como una necesidad para combatir la criminalidad *online*. Es obligado aproximar a los actores judiciales implicados en la persecución y demostración del cibercrimen; y una vía para ello, sin duda, es la propia causa que ha facilitado esta realidad delictiva: la tecnología. Como bien señala FAGGIANI "*a la digitalización del crimen hay que responder con la digitalización de los sistemas de justicia*"[38].

---

[35] Carnelutti, F. (1973), *Institituciones de Derecho Procesal Civil*, Buenos Aires, Ejea,t.I, p. 331.

[36] Devis Echandía, H. (1981), *Teoría General de la Prueba Judicial*, Tomo I, 5.a edición, Buenos Aires, p. 13.

[37] Cortés Domínguez, V., Moreno Catena, V. (2019), *Derecho Procesal Civil. Parte General*, Ed. Tirant lo Blanch, 10ª Edición, p. 197.

[38] Faggiani, V. (2022), "Cooperación judicial vs. Criminalidad organizado en el marco de la *rule of law backsliding.* ¿Hacia dónde vamos?" en AA.VV. Garrido Carrillo, F.J., (Dir.), *Lucha contra la criminalidad organizada y cooperación judicial en la UE: instrumento, límites y perspectivas en la era digital*, Ed. Thomson Reuters Aranzadi, 2022, p. 27.

Los medios tecnológicos no sólo están incidiendo en las nuevas formas del crimen, sino que también están alterando los instrumentos procesales para su investigación, y demostración. Por ello, inaplazablemente, se ha de recurrir aquí a la fuente de prueba electrónica, cuyo acceso, explica GRANDE SEARA[39], "*se ha convertido en un factor esencial en la investigación y enjuiciamiento de actividades delictivas muy graves*", como los ciberdelitos. En este campo, resulta preciso ser muy cuidadosos en el modo de su obtención, sin vulneraciones de derechos ni de garantías constitucionales, pues de lo contrario estaremos abocados a la posible ilicitud de la misma. GARRIDO CARRILLO[40] explica que esto no se puede relativizar o excepcionar, debiendo operar como límite ineludible en los Estados de Derecho en su lucha contra la delincuencia organizada.

El concepto de prueba electrónica no es uniforme en el panorama europeo, empleándose por los países diferentes términos para hacer alusión a este medio[41]. A esta conclusión se llegó en un Proyecto Europeo sobre "*Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad*", donde se afirmaba que *"los investigadores no hallaron una definición específica de "prueba electrónica", pero sí referencias legislativas a "prueba tradicional", "documento electrónico", "firma electrónica" y "medios de prueba", todas aplicables por analogía a la prueba electrónica, pero con las debidas matizaciones"*[42].

En el ámbito europeo, el reciente Reglamento (UE) 2023/1543 sobre órdenes europeas de producción y órdenes europeas de conservación a efectos de prueba electrónica en procesos penales, define prueba

[39] Grande Seara, P. (2022), "Las órdenes europeas de entrega y conservación de pruebas penales en el marco de la lucha contra la delincuencia organizada" en AA.VV. Garrido Carrillo, F.J., (Dir.), *Lucha contra la criminalidad organizada y cooperación judicial en la UE: instrumentos, límites y perspectivas en la era digital*. Ed. Thomson Reuters Aranzadi, p. 64.

[40] Garrido Carrillo, F.J. (2021), "Estudio preliminar-prólogo" en AA.VV. Garrido Carrillo, F.J. (Dir.), *Retos en la lucha contra la delincuencia organizada. Un estudio multidisciplinar: garantías, instrumentos y control de los beneficios económicos*, Ed. Thomson Reuters Aranzadi, p. 19.

[41] *Vid.* en profundidad este debate en Abel Lluch, X. y Picó i Junoy, J. (2011), *La prueba electrónica*, Ed. JB Bosch Formación, Barcelona, pp. 21 y ss.

[42] En este Proyecto Europeo se analizaron las legislaciones de dieciséis países, *Vid*. Insa Mérida, F., Lázaro Herrero, C., García González, N. (2008), "Pruebas electrónicas ante los tribunales en la lucha contra la ciberdelincuencia. Un proyecto europeo", en *Revista Venezolana de Información, Tecnología y Conocimiento*, Año 5, nº 2, pp. 142 y ss.

electrónica como aquellas evidencias almacenadas en formato electrónico por un proveedor de servicios en el momento de recibir el certificado de la orden europea, consistentes en datos de los abonados, datos relativos al acceso, datos de transacciones y datos de contenido almacenados.

En el ámbito nacional, no obstante, no disponemos por el momento de una norma jurídica que defina de manera unívoca este concepto, por lo que habría que recurrir a diferentes referencias legislativas. Por citar una, a modo de ejemplo, la legislación procesal civil, en sus arts. 382-384 LEC, admite la prueba electrónica al incorporar los medios de prueba audiovisuales, y la prueba por instrumentos informáticos. El carácter genérico de estos preceptos parece admitir el material probatorio almacenado, y aportado, en un soporte electrónico. Cuestión distinta es la validez, fiabilidad o autenticidad del contenido probatorio; razón por la cual esta ha de rodearse de las máximas garantías, como un dictamen pericial.

Por su lado, desde la doctrina, también se ha trabajado en esta labor definitoria. DELGADO MARTÍN[43] entiende por prueba electrónica toda "*información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio*". BUENO DE MATA[44] señala, básicamente, que "*desde un punto de vista técnico procesal, la prueba electrónica no es diferente de la prueba tradicional, pues sigue siendo material probatorio (…), la diferencia es que se expresa mediante un soporte electrónico creado por los modernos instrumentos tecnológicos de la información*".

Por otra parte, también se ha previsto y regulado la prueba electrónica en la Constitución Española, por cuanto su art. 24.2 establece el derecho a utilizar los medios de prueba pertinentes para nuestra defensa, para la defensa de aquello que afirmamos y que queremos probar en el marco del proceso judicial, por lo que tenemos derecho a proponer prueba, que sea practicada, y que sea valorada por el Tribunal, así como derecho a recurrir para el caso de que sea inadmitida[45].

Por lo tanto, las partes tienen derecho a respaldar sus afirmaciones con los medios probatorios admitidos en derecho, siempre que se respeten las

[43] Delgado Martín, J. (2017), "La prueba digital. Concepto, clases y aportación al proceso y valoración" en *Diario La Ley*, nº6, Sección Ciberderecho.
[44] Bueno de Mata, F. (2018), "Prueba electrónica: problemas del presente y retos del futuro. España" en AA.VV. Bujosa Vadell, L-M. (Dir.) *La prueba en el proceso. Perspectivas nacionales*, Ed. Tirant lo Blanch, Valencia, p. 574.
[45] *Vid*. Pérez Palací, J.E. (2014), *La prueba electrónica: Consideraciones*, Universitat Oberta de Catalunya, p. 4.

reglas procesales sobre la aportación, práctica y valoración; ahora bien, en el contexto actual en el que irrumpen en el mundo del derecho las llamadas nuevas tecnologías (TIC), y se consolida el cibercrimen en el panorama delictivo, es lógico que se barajen nuevas fuentes de prueba en forma de nuevos soportes y dispositivos electrónicos. De todas maneras, el fin que se persigue continúa siendo el mismo: que adquiera el juzgador el convencimiento de un hecho controvertido, ya sea mediante el convencimiento psicológico, ya sea fijando este hecho como cierto atendiendo a unas normas legales. La diferencia básicamente estriba en que, con la llegada de las nuevas tecnologías, las relaciones humanas y la información se encuentran ahora en soportes informáticos, como un DVD, una hoja de cálculo, o una tecnología *blockchain*, que esto último, como ya se ha visto, no es otra cosa que un registro dentro de una base de datos distribuida en un sistema *p2p*.

En el caso que nos ocupa, *blockchain*, sirve como tecnología descentralizada capaz de verificar y cotejar información sobre tres extremos relevantes en la persecución del cibercrimen, a saber:

- Los datos, negocios y transacciones que se han llevado a cabo y registrado en la base de datos distribuida.
- La identidad de los usuarios que han intervenido en las operaciones (si está previamente definida).
- Y el sellado de tiempo, o momento temporal en el que cada transacción queda sellada de forma auténtica e inmutable en el bloque.

Esta información que almacena *blockchain* – y que opera, a tenor del Cap. V del Reglamento 2023/1543, como sistema informático descentralizado que conserva pruebas electrónicas recabadas bajo una previa investigación europea - resulta valiosa para avanzar en la averiguación y enjuiciamiento del presunto ciberdelito transfronterizo, y constituye fuente de prueba. Recabada esta, la cuestión que ahora procedería sería cómo accede y se incorpora al proceso penal la información almacenada en *blockchain*[46]. Recuérdese que una cosa es la

[46] Como explica PÉREZ-CRUZ MARTÍN, realmente, no existe un "numerus clausus" de medios de prueba en el sistema actual de enjuiciamiento penal; a los medios de pruebas tradicionales (como la pericial, la testifical o la documental) hay que añadir, de acuerdo a lo establecido en el art. 230 LOPJ, "*los medios técnicos de documentación y reproducción y las innovaciones científicas siempre que ofrezcan las debidas garantías (…)*", por lo que cabría incorporar *blockchain* como fuente de prueba al proceso penal, la cuestión es cómo. *Vid*., Pérez-Cruz Martín, A-J. (2023), "La prueba. Concepto; objeto;

fuente de prueba – que es extraprocesal, e ilimitada – y otra distinta el medio de prueba – que sería el cauce por el que la fuente accede al proceso, y los cauces, como sabemos, están tasados en la normativa-. GARRIDO CARRILLO[47] facilita la comprensión de cada término, señalando que "*la fuente de prueba electrónica recoge información intangible y precisa de un aparato de almacenamiento para su práctica en el acto del juicio, siendo su reproducción ante el órgano judicial la forma de práctica de la prueba electrónica, no el medio*".

La prueba electrónica, por tanto, abarca cualquier clase de información, intangible – ya sea sobre hechos físicos, o virtuales – producida, almacenada o transmitida por medios electrónicos. Con las debidas garantías, esta información acceder al proceso por vía de una actividad probatoria, y surtir, eventualmente, los efectos probatorios pretendidos.

La cuestión radica en determinar, a la luz de la legislación procesal española, y de las actuales reformas, el medio idóneo a través del cual hacer valer la fuente de prueba *blockchain* recabada en Europa, en un eventual proceso penal español, y servir con ello de verificación fehaciente de los hechos que acredita.

4. MEDIOS DE PRUEBA ELECTRÓNICA *BLOCKCHAIN*

La información contenida en un equipo informático, o dispositivo de almacenamiento de datos, puede acceder al proceso penal a través del uso de distintos medios de prueba, como son: declaraciones personales (ya sea de testigos, o confesiones del presunto culpable), un informe pericial, un reconocimiento judicial, o una impresión en papel y posterior exhibición del documento *blockchain*.

En este estudio, por motivos de extensión, nos centraremos en la documental, y la pericial, por constituir, como se argumentará, dos medios

medios de prueba. Proposición, admisión o denegación; prueba anticipada; proposición en el acto del juicio; prueba acordada "ex oficio". Las pruebas obtenidas con violación de los derechos fundamentales (prueba prohibida). La prueba producida irregularmente", en Pérez-Cruz Martín, A-J (dir.), *Derecho procesal penal*, Tirant lo Blanch, Valencia, p. 560.

[47] Garrido Carrillo, F.J. (2017), "La prueba electrónica en los procesos civiles y penales" en AA.VV. Pérez-Serrabona González, J.L. (Dir.), *Crisis y Estado de Bienestar. In memoriam Prof. Nicolás María López Calera*, 3ª. Época, núm. 16/17/18, 2013-2014-2015, ISSN: 0212-8217, Ed. Tirant lo Blanch, Valencia, p. 559.

de prueba perfectamente complementarios y suficientes para disuadir al Juez tanto de la validez como de la autenticidad de la prueba electrónica conservada en *blockchain*.

Previo a entrar en esta cuestión, nos parece oportuno indagar siquiera brevemente en el estado de la cuestión en el derecho comparado.

En primer lugar, en EEUU, en 2017, el actual gobernador del Estado de Delaware, John C. Carney Jr., legalizó el uso de *blockchain* para el intercambio de acciones y registros contables, por vía de la Ley "*Delaware Blockchain Initiative (DBI)*". Con esta iniciativa se anticipaba por aquel entonces a las iniciativas de regulación que empezaban a promoverse en los estados de Nevada, Vermont, New Hamsphire y Arizona sobre la tecnología *blockchain*[48].

En China, la última reforma de la Ley Procesal de China, de 1 de julio de 2017, ya incluyó un apdo. 5º en su art. 63 que expresamente reconoce "los datos electrónicos" como una variante de evidencia admitida por los tribunales. Ello, rápidamente, tuvo repercusión en la *praxis* judicial, concretamente, a partir del caso del tribunal de internet de Hangzhou (2018), el cual, en el marco de un litigio sobre derechos de propiedad intelectual, consideró admisible, y confiable, el contenido y sello de tiempo aportado por la demandante mediante *blockchain*. Así pues, dentro de este contexto normativo y judicial, el Tribunal Popular Supremo de China, publicó, recientemente, el 25 de mayo de 2022, un dictamen titulado "*Opiniones del Tribunal Popular Supremo sobre el Fortalecimiento de la Aplicación Blockchain en el Campo Judicial*" (versión española), en el que, entre otros avances tecnológicos, propugna la incorporación de la tecnología *blockchain* para que las partes y jueces puedan verificar las pruebas electrónicas almacenadas en esta plataforma.

Reino Unido, por su lado, publicó, en 2018, por voz de Balaji Anbil[49], un proyecto *blockchain*, como elemento estratégico y parte de un proceso global de digitalización de los procesos judiciales. Anbil explicó la importancia de la tecnología distribuida para ayudar en el manejo de la evidencia digital al crear una "*pista de auditoría que rastrea la custodia y*

[48] *Vid*., Comunicado de prensa en Criptonoticas, por José Rafael Peña, en https://www.criptonoticias.com/regulacion/delaware-legaliza-uso-blockchain intercambio-acciones-registros-contables/ Fecha de consulta: [15/02/2024]

[49] Jefe de Arquitectura Digital y Seguridad Cibernética en el Servicio de Cortes y Tribunales de Su Majestad (HMCTS) dependiente del Ministerio de Justicia.

previene la manipulación"[50]. El proyecto, bautizado como "*Archangel*"[51], fusiona tecnologías IA y *blockchain*, con la finalidad de proporcionar garantías para la integridad y sostenibilidad futura de los datos electrónicos.

En Italia, se incorpora la regulación de la tecnología *blockchain* por medio de una enmienda del Senado al art. 8 de la Ley de Conversión del Decreto-Ley de simplificación (D.l.n. 135/2018), que introduce la definición de la tecnología de registros distribuidos, y regula el valor probatorio de un documento con el sello de tiempo *blockchain* (art. 8-bis 3)[52].

En definitiva, este paréntesis de derecho comparado nos permite concluir que la prueba electrónica *blockchain* es una realidad consolidada en las legislaciones, y tribunales del extranjero, lo cual refuerza las garantías de una investigación y enjuiciamiento europeo e internacional del ciberdelito, ya que las pruebas electrónicas recabadas y conservadas en *blockchain*, podrían, en principio, acceder al proceso, y surtir los efectos oportunos frente a cualquiera de los tribunales citados. Esto ayudaría a evitar disfunciones propias de países con asimetrías regulatorias entre sí. Cuestión distinta, claro está, es el valor probatorio que se le otorga a la prueba en cada caso, o jurisdicción, lo cual se reserva ya a la amplia casuística propia de los juzgados.

Ya centrándonos en nuestra circunscripción territorial, ciertamente, cabe reconocer que la tecnología *blockchain* se encuentra en auge, y que empieza a encontrar acomodo en diversos nichos.

En el ámbito judicial, por ejemplo, los juzgados de lo mercantil de Barcelona presentaron en 2020 un proyecto piloto, en el marco de los litigios sobre protección del secreto empresarial. Se propuso un protocolo de actuación que plantea el uso de *blockchain* como un sistema de almacenaje o libro registro de información reservada o confidencial.

---

[50] Nota disponible en *Diario Bitcoin*, editado el 10 de diciembre de 2022. Disponible en: https://www.diariobitcoin.com/tecnologia/blockchain/reino-unido-revela-piloto-para-almacenar-evidencia-digital-en-un-blockchain/ Fecha de consulta: [15/02/2024]

[51] *Vid*., Archangel – *Trusted Digital Archives – Securing our National Archives for Future Generations*, disponible en: https://www.archangel.ac.uk/ Fecha de consulta: [15/02/2024]

[52] Senato della Repubblica, *Proposta di modifica n. 8.0.3 al DDL n. 989*. Consultado en: https://www.senato.it/japp/bgt/showdoc/frame.jsp?tipodoc=Emendc&leg=18&id=1096791&idoggetto=1095835 Fecha de consulta: [15/02/2024]

Por otro lado, *blockchain* también ha despertado el interés del Colegio de Registradores de España, y entre ellos el Registro de la Propiedad, que recalcan su viabilidad para dar mayor seguridad y trazabilidad a las anotaciones.

En el ámbito delictivo, España, en respuesta a las exigencias de Europa para regular eficazmente el mercado interior, traspuso la V Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, dando lugar a la actualización de la Ley 10/2010 a través del Real Decreto-ley 7/2021, de 27 de abril[53]. *Blockchain* - al funcionar como un libro de contabilidad digital que facilita el seguimiento de los movimientos de la criptomoneda - se ha incorporado como herramienta para detectar y prevenir numerosos delitos financieros, incluido el lavado de activos y otras actividades delictivas relacionadas.

Dicho esto, lo cierto es que, pese al interés por las diversas instituciones, a día de hoy, nuestra legislación interna carece de un marco regulatorio completo que ofrezca garantías técnicas y legales suficientes para incorporar *blockchain* con normalidad jurídica en un proceso penal. En consecuencia, el análisis de su encaje como medio de prueba suscita aún cierto desasosiego, y, por ello, de momento, conviene recurrir a lo que sientan los tribunales.

4.1. *Blockchain* como documento electrónico

La jurisprudencia española ha trabajado en este asunto, y, por vez primera, por vía de la sentencia 326/2019, de 20 de junio[54], nos da ya una

[53] de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores. BOE núm. 101, de 28 de abril de 2021.

[54] Lo cual se deduce del Fundamento de Derecho Primero, que establece que "el artículo 726 LECrim previene la valoración directa por el Tribunal de los libros, documentos y demás piezas de convicción que pueden contribuir al esclarecimiento de los hechos. En un sentido parecido, el art. 899 de la Ley procesal propone el examen de las actuaciones, que podrían ser reclamadas por el Tribunal de la revisión, para un mayor esclarecimiento de los hechos. Desde esta escasa indicación sobre su valoración, hemos destacado que siempre y cuando los documentos se hayan incorporado a la causa de forma legítima, y con cabal conocimiento de las partes y el Tribunal, corresponde a este examinar de manera directa los documentos, debiendo motivar la convicción o el rechazo de lo que encierran en función de su coherencia o compatibilidad con el resto del material acreditativo presentado". *Vid*., STS núm. 326/2019, de 20 de junio.

primera pista, al admitir como válido la documental *blockchain* aportada en un proceso, siempre que se hayan observado las debidas garantías.

Se trata de una cuestión que ha sido desarrollada de un modo escaso en vía jurisprudencial, por lo que conviene ahondar en este asunto.

Blockchain proporciona un registro contable, en el que la autenticidad de su contenido se atribuye a su naturaleza electrónica, pues la información que se agrega a cada bloque pasa por un previo proceso de validación y consenso entre todos los ordenadores o nodos interconectados entre sí. Esta innovación tecnológica, que almacena información veraz, inmutable y transparente acerca de la realidad de la transacción, el sujeto titular de la misma, y el sellado de tiempo, debe incorporarse al acervo jurídico procesal en la medida en que expresa una "realidad", y sirve de instrumento para ayudar al Juez en el esclarecimiento de los hechos y la búsqueda de la verdad material.

En base a esto se considera, en primer lugar, que la forma de enlazar la tecnología *blockchain* y la prueba electrónica es a través del documento electrónico.

Desde el punto de vista de la jurisdicción penal, art. 26 CP, se considera documento *"todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica"*. Desde la óptica procesal, el art. 743 apdo. 1º LECrim define documento electrónico al establecer que *"el desarrollo de las sesiones del juicio oral se registrará en soporte apto para la grabación y reproducción del sonido y de la imagen"*.

Para la Real Academia Española[55], el término "soporte" alude al material en cuya superficie se registra información, pudiendo ser ese material: el papel, la cinta de video, un CD, un lápiz de memoria (Pendrive), una cinta magnética, un disco duro (*Hard Disk Drive*), entre otros; estos soportes son medios de almacenamiento de datos.

Todo lo anteriormente expuesto tiene un denominador común: el "soporte material" habrá de contener "datos, hechos o narraciones" o, dicho de otra manera, habrá de contener información relativa a una transacción, dato o declaración de voluntad atribuible a algún sujeto en particular. Esta, como se ha señalado más arriba, es precisamente la función que desempeña *blockchain*: registrar y certificar información sobre un hecho, su autoría (si está previamente definida), y el sellado de

[55] *Vid*. Concepto en el siguiente enlace: https://dle.rae.es/soporte Fecha de consulta: 22/02/2024].

tiempo, o momento temporal en el que cada transacción queda registrada de forma auténtica e inmutable en el bloque.

Por tanto, nos preguntamos si, en términos de prueba, *blockchain* hace las veces de documento electrónico, y, por tanto, puede ser considerado prueba documental en el proceso penal.

Señálese que toda información registrada en el bloque no deja de conformar un documento, con la singularidad de que aparece plasmado en un soporte informático. Por lo que se aportará el soporte electrónico en el que se hallan registrados, así como la copia impresa del *hash* de la transacción, y de los bloques afectados, junto a las claves criptográficas que permiten su descodificación. Recuérdese que *blockchain*, si bien no es responsable por el contenido de los hechos, lo es por el hecho de validar y registrar la información, por lo que constituye una evidencia y prueba manifiesta de las transacciones que han tenido lugar, de forma transparente e irrevocable, a lo largo del tiempo.

En otras palabras, constituye pues documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico, según un formato determinado y susceptible de identificación y tratamiento diferenciado, pudiendo ser soporte de documentos públicos y documentos privados. Respecto a la eficacia jurídica de los documentos electrónicos (públicos, privados o administrativos) será aquélla que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable (art. 3 Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza).

4.1.1. *Bockchain* como documento privado

En el supuesto de la cadena de bloques, la cuestión es si procede aportar al proceso como prueba documental privada la impresión del "hash ", es decir, la clave alfanumérica asociada a un determinado contenido, así como la correspondiente pericial informática que descifre estos dígitos y los "traduzca" a un lenguaje inteligible, haciendo así las veces de un documento escrito tradicional en soporte papel. Esta eficacia probatoria se aprecia con mayor intensidad en el ámbito de la contratación, ya que los arts. 23 y 24 de la Ley 34/2002, de 11 de Julio, de Servicios de la Información y del Comercio Electrónico (en adelante, LSSICE), enfatizan una clara equivalencia entre el soporte electrónico y el soporte papel como

fuente de prueba que puede acceder a cualquier proceso. En concreto, el art. 23.3 LSSICE establece que la forma electrónica equivale a la forma escrita, por lo que es claro que la base de datos que configura la cadena de bloques constituye un documento a los efectos probatorios. Añade el artículo 24.2 LSSICE que el soporte electrónico en el que se halle registrado un contrato electrónico será admisible en juicio como prueba documental.

En torno a su valor probatorio, al no prever la LECrim disposiciones relativas al documento público y privado, hemos de aplicar por técnica remisoria - prevista en el art. 4 LEC - la legislación procesal civil[56]. En atención a este texto, el artículo 326.1 LEC dispone que los documentos privados harán prueba plena en el proceso siempre que su autenticidad no sea impugnada por la parte perjudicada. Por tanto, la regla es que, en caso de que no resulte impugnada la autenticidad, el registro en *blockchain* impreso en un documento privado despliega la fuerza probatoria plena. Solo la impugnación de la autenticidad de dicho soporte provocará que el aportante deba pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente con el fin de acreditar su autenticidad. Cuando no se pudiere deducir su autenticidad o no se hubiere propuesto prueba alguna, el tribunal lo valorará conforme a las reglas de la sana crítica (art. 348 LEC).

Países de la órbita del *Civil Law* como Italia se colocan a la vanguardia de la tecnología *blockchain* como libro contable y medio de prueba, y es por ello que, a través del ya referido D.l.g. 135/2018, reconoce que "*el almacenamiento de un documento informático a través del uso de tecnologías basadas en registros distribuidos, produce los efectos legales de la validación electrónica del tiempo, de conformidad con el art. 41 del Reglamento de la UE no. 910/2014*"[57]. Es decir, la normativa italiana

[56] La cual, en aras a la digitalización y eficiencia del servicio de justicia, ha sido objeto de reforma parcial por el Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo. BOE núm. 303, de 20 de diciembre de 2023.

[57] Este art. 41 del Reglamento de la UE nº. 910/2014 establece que:

"*1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello de tiempo electrónico por el mero hecho de estar en formato electrónico o de no cumplir los requisitos de sello cualificado de tiempo electrónico.*

2. Los sellos cualificados de tiempo electrónicos disfrutarán de una presunción de exactitud de la fecha y hora que indican y de la integridad de los datos a los que la fecha y hora estén vinculadas.

reconoce los efectos de la validación electrónica del tiempo a los documentos electrónicos almacenados en *blockchain* de conformidad con el art. 41 del Reglamento de la UE núm. 910/2014. Esto significa que tiene valor y fuerza probatoria la fecha y hora de existencia de una transacción en un momento dado. Esta es la función típica de los registros, que permiten documentar con precisión un hecho concreto en un momento determinado, como por ejemplo en el registro público de automóviles, los registros catastrales o el registro de empresas.

En el concreto ámbito de la firma electrónica, el soporte en que se hallen los datos firmados electrónicamente es admisible como prueba documental, por lo que el art. 326.3 LEC dispone que si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico, se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.

La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros (art. 320.3 LEC). Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apdo. 2 del art. 326 de la LEC.

Una cuestión problemática es que, en el actual sistema procesal, el documento privado aportado al proceso se acompañe de un dictamen pericial elaborado por un técnico informático experto en "*blockchain*" que certifique la autenticidad de los datos insertos en la cadena de bloques, en particular los aspectos criptográficos, así como la equivalencia entre la huella digital y el dato que pervive en el mundo exterior.

---

3. Un sello cualificado de tiempo electrónico emitido en un Estado miembro será reconocido como sello cualificado de tiempo electrónico en todos los Estados miembros".

Ahora bien, la conveniencia de aportar dicho dictamen no excluye la posibilidad del juez de valorar el medio de prueba documental por sí mismo, al amparo del art. 326.2 LEC, sin necesidad de acompañarlo de exámenes adicionales.

4.1.2. *Blockchain* como documento público

Uno de los retos principales que plantea el uso de la cadena de bloques es la posibilidad de otorgar a la misma el valor probatorio que la legislación procesal asigna exclusivamente al documento público.

De *lege lata*, el listado *numerus clausus* de documentos públicos que recoge el art. 317 LEC se refiere a aquellos documentos expedidos por autoridades judiciales, notariales o registrales, legitimadas para certificar, en el ámbito de sus competencias, la autenticidad de dichos contenidos. Por tanto, al no constar la cadena de bloques certificada por fedatario alguno[58], ello impide afirmar que la *blockchain* puede ser equiparada a un documento público, por no hallar expreso encaje en la legislación procesal. Por tal razón, en principio, el medio idóneo para incorporar *blockchain* al proceso penal es mediante un documento privado. En todo caso, si se pretendiera aportar como documento público, sería conveniente antes una reforma de *lege ferenda* en la que el legislador equiparara expresamente las certificaciones extraídas de la cadena de bloques con los documentos validados por fedatario público.

Cuestión distinta es si, con base en sus rasgos tecnológicos, la cadena de bloques permite la emisión de certificados que podamos considerar a efectos procesales como "auténticos". A la vista de las características enumeradas *supra*, parece que solo la realidad de la transacción registrada y el momento temporal del sellado son elementos verdaderamente fiables.

[58] La utilización de servicios de notaría dentro de *blockchain*, mediante plataformas *Stampery* y *Blockverify*, permitiendo crear registros inmutables, con verificación de autoría y autenticidad del documento, y sin necesidad de un tercero que lo certifique, generó en su momento un intenso debate sobre la viabilidad de reemplazar la figura del notario por estas plataformas. Miembros del gremio, como GONZÁLEZ GRANADO, sostuvieron que Blockchain, si bien constituye un medio descentralizado de sellado de tiempo de archivos digitales, lo cierto es que no añade ningún valor al documento verificado". *Vid*. González Granado, J. "¿Enviará Blockchain de vacaciones a los notarios? en *Notaría Abierta*, disponible en el siguiente enlace: https://notariabierta.es/enviara-blockchain- vacaciones-los-notarios/. Fecha de consulta: [01/03/2024]

En cuanto al modo de aportación de los documentos públicos al proceso, el art. 318.1 LEC dispone que estos deberán aportarse al proceso en original o por copia o certificación fehaciente, bien en soporte papel o mediante documento electrónico, o si, habiendo sido aportado por copia simple, en soporte papel o imagen digitalizada, cuando no se hubiere impugnado su autenticidad (art. 267 LEC). Según la reforma introducida por el Real Decreto-ley 6/2023, de 19 de diciembre, de eficiencia digital y procesal[59] "*si se impugnara su autenticidad, podrá llevarse a los autos original, copia o certificación del documento con los requisitos necesarios para que surta sus efectos probatorios*". Por tanto, de atribuir al registro en la cadena de bloques valor probatorio pleno, bastaría la aportación al proceso de la copia digitalizada del mismo, siendo necesaria la aportación del original en el supuesto en que el contrario impugnara aquélla.

Sin duda, en cualquiera de los hipotéticos escenarios, la necesidad de complementar la documental mediante la aportación de un dictamen pericial sigue siendo el caballo de batalla. Su utilidad en orden a garantizar al juez la correspondencia entre el código encriptado y el lenguaje humano es indudable.

4.2. Prueba pericial de *blockchain*

En este proceso de transición de fuente a medio de prueba, *blockchain* plantea un desafío ya que la integridad y autenticidad del contenido de la cadena de bloques se pone en entredicho si en vez de acceder al registro el documento completo, lo hace el denominado "*hash*", es decir, la huella digital del mismo, ya que la autenticidad parece ceñida a dicha clave alfanumérica, procedente de la criptografía.

En este caso, se debe considerar la intervención y análisis pericial de un informático experto en la lectura y descodificación de contenidos archivados en la tecnología *blockchain*. Dicho dictamen, emitido por el perito bajo previo juramento o promesa de actuar con objetividad, y bajo previo apercibimiento de las sanciones penales en las que podría incurrir si incumpliese dicho deber, se centraría en la fuente de prueba y su objeto se centraría, en primer lugar, en garantizar la autenticidad de la misma, y, en segundo, en garantizar su integridad, es decir, que la misma no ha sido manipulada ni alterada.

[59] El art. 267 LEC se modificó por el art. 103.47 del Real Decreto-ley 6/2023, de 19 de diciembre citado *supra*.

En relación a lo anterior, GARRIDO CARRILLO[60] señala que coexisten dos tipos de prueba pericial, una pericial autónoma y una pericial instrumental. En el primer caso, cabría que la prueba documental operara de modo independiente, y pudiera ser valorada judicialmente, en tanto en cuanto no sea impugnada su autenticidad (art. 326.1 LEC). Esto último, no obstante, no es el escenario habitual, por lo que, en tales casos, como explica GONZÁLEZ REYES[61], la pericial informática devendrá "*indispensable (…) así como cuando se requiera el acceso a la información contenida en un dispositivo y la misma haya sido encriptada o eliminada o, simplemente, cuando el acceso a dicha información sea difícil y se requiera por ello conocimientos técnicos*".

Se está en presencia de una tecnología disruptiva, compleja, y configurada por unos parámetros que aún desconoce la mayoría de la sociedad; por tanto, y a fin de evitar un proceso sin las debidas garantías, nos parece a todas luces necesario acompañar la documental de *blockchain*, con el debido informe pericial informático, que acredite la autenticidad, e integridad de la cadena de bloques, así como su inalterabilidad. Esto no sólo refuerza las garantías del proceso, sino que además robustece la prueba electrónica.

Por ello, a nuestro criterio, debe insistirse en el carácter instrumental de esta pericial, al operar como medio o vehículo para incrementar el poder de convicción de la prueba documental electrónica sobre el tribunal.

Este dictamen, complementario de la documental, en definitiva, ayudará al Juez a valorar, conforme a los principios de la sana crítica (art. 348 LEC), si, de un lado, el *blockchain* que operó como técnica de conservación de pruebas electrónicas en el marco de una cooperación procesal europea, es auténtico y no se ha actuado y ocultado la información en una especie de *software* maliciosa, y, de otro, si la información almacenada y registrada es auténtica y no ha sido objeto de manipulación ni alteración. En definitiva, se trata de verificar que se respeta la cadena de custodia.

[60] Garrido Carrillo, F.J. (2017), "La prueba electrónica en los procesos civiles y penales" en *Crisis y Estado de Bienestar. In memoriam Prof. Nicolás María López Calera, op.cit…,* p. 571.

[61] González Reyes, J.M., (2021), "La prueba pericial digital y la cadena de custodia" en *Anales de la Facultad de Derecho*, nº 38, 2021, p. 64.

A MODO DE CONCLUSIÓN

Consideramos que, a la vista de la actual tendencia alcista del cibercrimen, urge adoptar e incorporar medidas de investigación y prueba tecnológicas al proceso penal europeo. Cabe reconocer que la UE viene trabajando de un modo profuso para tratar de paliar y prevenir los efectos de la cibercriminalidad; no obstante, las cifras revelan que los esfuerzos implementados, en cierto modo, han resultado baldíos.

En este estudio, se ha considerado esencial digitalizar los mecanismos procesales como respuesta eficaz, y adaptada, a las nuevas características del delito. Se ha hablado de la necesidad de "*adaptarse al medio delictivo*", por cuanto es un hecho, afirma la Comisión Europea, que el 80% de los delitos tiene un componente digital, por lo que es necesario, para una comprensión óptima del problema, emplear este enfoque. En consecuencia, hemos incidido sobre una institución procesal específica, la prueba electrónica, pues, como ya se ha constatado, este tipo de prueba *se necesita en cerca del 85% de las investigaciones penales y, en dos tercios de estas investigaciones, es preciso obtener pruebas de proveedores de servicios en línea establecidos en otra jurisdicción*.

El reciente Reglamento 2023/1543 representa un avance significativo en esta dirección, por cuanto incorpora, en su articulado, la viabilidad de incorporar sistemas informáticos descentralizados coma vía o canal para la conservación de pruebas digitales recabadas bajo una previa orden europea de investigación[62]. *Blockchain*, por sus características, encaja perfectamente en este tipo de sistemas. Su estructura y configuración

[62] FUENTES SORIANO afirmó que "*internet no conoce fronteras, estos servicios pueden prestarse desde cualquier lugar del mundo y no exigen necesariamente una infraestructura física (…). Tampoco requieren una ubicación específica para el almacenamiento de datos, que a menudo es elegida por el proveedor de servicios (…). En consecuencia, en un número creciente de casos penales relativos a todo tipo de delitos (…) ha comenzado a pensarse en la conveniencia de que las autoridades competentes de los Estados miembros puedan dirigir – con carácter vinculante – sus solicitudes de entrega o conservación de datos electrónicos directamente a los proveedores de servicios en el ámbito de la Unión*". Con este avance, señala la autora, "*se inaugura un nuevo escenario de actuación procesal que (…) permite una actuación procesal directa y vinculante de un Estado en relación con sujetos asentados (o con vinculaciones estables) en otro*". *Vid*., Fuentes Soriano, O. (2020), "Europa ante el reto de la prueba digital. el establecimiento de instrumentos probatorios comunes: las órdenes europeas de entrega y conservación de pruebas electrónicas" en Fuentes Soriano, O. (Dir.), *Era digital, sociedad y derecho*, Ed. Tirant lo Blanch, Valencia, pp. 292-293.

resultan idóneas para almacenar información relativa al cibercrimen de un modo seguro, fiable, y transparente, lo cual tiene sus obvias implicaciones en materia de prueba electrónica. En este preciso aspecto, se ha detectado una laguna, o deficiencia de la norma europea, al no dispensar un tratamiento procesal de mínimos en torno al medio probatorio idóneo para incorporar la fuente de prueba *blockchain* al proceso penal español.

La normativa, como se ha señalado, es muy parca en este sentido, y se limita tan sólo a indicar que "*no se denegarán los efectos jurídicos de los documentos transmitidos como parte de la comunicación electrónica ni se considerarán inadmisibles en el contexto de los procesos judiciales transfronterizos contemplados en el presente Reglamento por el mero hecho de estar en formato electrónico*" (art. 20 Reglamento 2023/1543).

Esto es insuficiente para superar los posibles interrogantes procesales que pueden surgir en el curso de un proceso judicial español a la hora de incorporar *blockchain* como prueba electrónica. Por ello, en esta investigación se ha procurado, bajo la óptica de la legislación procesal, y las recientes reformas, analizar los posibles medios de prueba que podrían, de un modo suficiente y completo, certificar la validez y autenticidad de la evidencia digital conservada en *blockchain*.

Así pues, en primer lugar, se ha concluido que *blockchain*, como soporte electrónico que plasma la información de la investigación, es responsable por el hecho de validar y registrar la información, y, por tanto, hace las veces de prueba documental.

Ex art. 326.1 LEC, el registro en *blockchain* impreso en un documento privado despliega la fuerza probatoria plena, siempre que no se impugne en el proceso; de ser así, provocará que el aportante deba proponer cualquier otro medio de prueba que resulte útil y pertinente con el fin de acreditar su autenticidad.

En el caso de la documental pública, *blockchain* no figura en la lista *numerus clausus* (art. 317 LEC) de documentos públicos expedidos por autoridades, ya sean judiciales, notariales o registrales, legitimadas para certificar, en el ámbito de sus competencias, la autenticidad de dichos contenidos.

Por tanto, *blockchain* no puede ser considerado documento público. Para posibilitar este medio de prueba, se sugiere una reforma de *lege ferenda* en la que el legislador equiparara expresamente las certificaciones extraídas de la cadena de bloques con los documentos validados por fedatario público. Para llegar a este punto, habría que pasar primero por un

proceso de maduración y concienciación que discurra entre los agentes jurídicos, y la sociedad.

En cuanto al modo de aportación de los documentos públicos al proceso, *ex* art. 267 LEC, bastaría con la aportación al proceso de la copia digitalizada del mismo, siendo necesaria la aportación del original en el supuesto en que el contrario impugnara aquélla.

En cualquiera de los casos, el proceso de transición de la fuente al medio de prueba *blockchain*, plantea el óbice de la integridad y autenticidad del contenido de la cadena de bloques. Por ello, se considera, de todo punto necesario, la intervención y análisis pericial de un informático experto en la lectura y descodificación de contenidos archivados en la tecnología *blockchain*, en orden a garantizar al juez la correspondencia entre el código encriptado y el lenguaje humano. En este contexto, imprime un carácter muy importante la pericial informática, como prueba instrumental, complementaria de la documental, cuyo cometido no es otro que garantizar la autenticidad de la misma, y su integridad, es decir, que la misma no ha sido manipulada ni alterada.

BIBLIOGRAFÍA

Abel Lluch, X., Picó i Junoy, J. (2011), *La prueba electrónica*, Ed. JB Bosch Formación, Barcelona.

Alarcón-Jiménez, O. (2019), "La aportación del Consejo de Europa en la lucha contra el crimen organizado transnacional" en AA.VV. Galán Muñoz, A. Mendoza Calderón, S. (Dirs.), *Globalización y lucha contra las nuevas formas de criminalidad transnacional*. Ed. Tirant lo Blanch, España, pp. 96-107.

Augusto Depetris, J. (2021), "Organizaciones criminales digitales: conocerlas para enfrentar su desafío" en *Revista del CLAD Reforma y Democracia*, núm. 79, Mar., pp. 117-154.

Bueno de Mata, F. (2023), "Blockchain, identidad autosoberana y prueba electrónica transfronteriza" en AA.VV. Hernández López, A., Laro González, M.E. (Dirs.), *Proceso penal europeo: últimas tendencias, análisis y perspectivas*, Ed. Thomson Reuters Aranzadi, pp. 71-86.

Bueno de Mata, F. (2018), "Prueba electrónica: problemas del presente y retos del futuro. España" en AA.VV. Bujosa Vadell, L-M. (Dir.) *La prueba en el proceso. Perspectivas nacionales*, Ed. Tirant lo Blanch, Valencia, pp. 573-581.

Carnelutti, F. (1973), *Institituciones de Derecho Procesal Civil*, Buenos Aires, Ejea,t.I.

Carnelutti, F. (1955), *La prueba civil*, Arayu, Buenos Aires.

Cortés Domínguez, V., Moreno Catena, V. (2019), *Derecho Procesal Civil. Parte General*, Ed. Tirant lo Blanch, 10ª Edición.

Delgado Martín, J. (2017), "La prueba digital. Concepto, clases y aportación al proceso y valoración" en *Diario La Ley*, nº6, Sección Ciberderecho.

De Hoyos Sancho, M., "Novedades en materia de obtención transfronteriza de información electrónica necesaria para la investigación y enjuiciamiento penal en el ámbito europeo", *Revista de Estudios Europeos*, núm. extraordinario monográfico 1, 2023, pp. 99-128.

Delgado Martín, J. (2017), "La prueba digital. Concepto, clases y aportación al proceso y valoración" en *Diario La Ley*, nº6, Sección Ciberderecho.

Devis Echandía, H. (1981), *Teoría General de la Prueba Judicial*, Tomo I, 5.a edición, 1981, Buenos Aires.

Díaz Gómez, A. (2010), "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest", en *REDUR* 8, diciembre, pp. 169-203.

Dolader Retamal, C., Bel Roig, J., Muñoz Tapia, J.L. (2017), "La blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas" en *Economía Industrial*, núm. 405, pp. 33-40.

Faggiani, V. (2022), "Cooperación judicial vs. Criminalidad organizado en el marco de la *rule of law backsliding*. ¿Hacia dónde vamos?" en

AA.VV. Garrido Cariilo, F.J. (Dir.), *Lucha contra la criminalidad organizada y cooperación judicial en la UE: instrumento, límites y perspectivas en la era digital*, Ed. Thomson Reuters Aranzadi, pp. 1-29.

Fuentes Soriano, O. (2020), "Europa ante el reto de la prueba digital. el establecimiento de instrumentos probatorios comunes: las órdenes europeas de entrega y conservación de pruebas electrónicas" en Fuentes Soriano, O. (Dir.), *Era digital, sociedad y derecho*, Ed. Tirant lo Blanch, Valencia, pp. 281-319.

Garrido Carrilo, F.J. (2021), "Estudio preliminar-prólogo" en AA.VV. Garrido Carrillo, F.J. (Dir.), Retos en la lucha contra la delincuencia organizada. Un estudio multidisciplinar: garantías, instrumentos y control de los beneficios económicos, Ed. Thomson Reuters Aranzadi, p. 19.

Garrido Carrillo, F.J. (2022), "Prólogo. Retos, amenazas, instrumentos y experiencias en la lucha contra el crimen organizado" en GARRIDO CARRILLO, F.J. (Dir.), *Respuesta Institucional y normativa al Crimen Organizado. Perfiles estratégicos para una lucha eficaz*, Ed. Aranzadi, Navarra, pp. 19-35.

Garrido Carrillo, F.J. (2017), "La prueba electrónica en los procesos civiles y penales" en AA.VV. PÉREZ-SERRABONA GONZÁLEZ, J.L. (Dir.), *Crisis y Estado de Bienestar. In memoriam Prof. Nicolás María López Calera*, 3ª. Época, núm. 16/17/18, 2013-2014-2015, ISSN: 0212-8217, Ed. Tirant lo Blanch, Valencia, pp. 553-590.

González Reyes, J.M. (2021), "La prueba pericial digital y la cadena de custodia" en *Anales de la Facultad de Derecho*, nº 38, pp. 43-79.

Grande Seara, P. (2022), "Las órdenes europeas de entrega y conservación de pruebas penales en el marco de la lucha contra la delincuencia organizada" en AA.VV. Garrido Carrillo, F.J. (Dir.), *Lucha contra la criminalidad organizada y cooperación judicial en la UE: instrumentos, límites y perspectivas en la era digital*. Ed. Thomson Reuters Aranzadi, pp. 63-92.

Insa Mérida, F., Lázaro Herrero, C., García González, N. (2008), "Pruebas electrónicas ante los tribunales en la lucha contra la ciberdelincuencia. Un

proyecto europeo", en *Revista Venezolana de Información, Tecnología y Conocimiento,* Año 5, nº 2, pp. 139-152.

Morillas Cueva, L. (2022), "Globalización y delincuencia organizada. Respuestas penales" en AA.VV. Garrido Carrillo, F.J. (Dir.), Faggiani, V. (Coord.), *Respuesta institucional y normativa al crimen organizado. Perfiles estratégicos para una lucha eficaz,* Ed. Aranzadi, España, pp. 39-75.

Pérez Palací, J.E. (2014), *La prueba electrónica: Consideraciones*, Universitat Oberta de Catalunya.

Pérez-Cruz Martín, A-J., "La prueba. Concepto; objeto; medios de prueba. Proposición, admisión o denegación; prueba anticipada; proposición en el acto del juicio; prueba acordada "ex oficio". Las pruebas obtenidas con violación de los derechos fundamentales (prueba prohibida). La prueba producida irregularmente", en J. A. Pérez-Cruz Marín (dir.), *Derecho procesal penal*, Tirant lo Blanch, Valencia, 2023, pp. 553 – 584.

Ruíz Rodríguez, L.R., González Agudelo, G. (2014), "El factor tecnológico en la expansión del crimen organizado" en *Centro de Investigación Interdisciplinaria en Derecho Penal Económico* (CIIDPE), pp. 1-42.

Segura Serrano, A. (2023), *El desafío de la ciberseguridad global*, Ed. Tirant lo Blanch.

Sentís Melendo, S. (1973), "Qué es la prueba (Naturaleza de la prueba)", *Revista de Derecho Procesal Iberoamericana*, núm. 2-3.

Tinoco Pastrana, Á., "Las órdenes europeas de entrega y conservación: la futura obtención transnacional de la prueba electrónica en los procesos penales en la Unión Europea", *Cuadernos de Política Criminal*, núm. 135, III, Época II, diciembre 2021, pp. 203-246.