Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en el Ejercicio de la Abogacía

Aplicación de la tecnología *blockchain* en el sistema judicial español

Trabajo fin de estudio presentado por:	Ana Moreno Toro
Tipo de trabajo:	Trabajo de Investigación Teórica
Área jurídica:	Derecho Civil
Director/a:	Joaquín David Rodríguez Álvarez
Fecha:	1 de febrero de 2023

Resumen

El surgimiento de la tecnología *blockchain* está articulando una nueva realidad desde un punto de vista jurídico-normativo y procesal. La Administración de Justicia está sumergida en tres profundas reflexiones fruto de las características disruptivas del *blockchain:* por un lado, el valor probatorio y los efectos jurídicos de las transacciones nacidas en una red *blockchain,* entre las que se incluye el registro y almacenamiento de contratos automatizados o *smart contracts;* por otro lado, la seguridad jurídica y los riesgos inherentes a la protección de datos personales; y, finalmente, la eficiencia en los procesos que esta tecnología podría aportar a la estructura judicial actual como herramienta digital. A través de una revisión aproximada de esta tecnología, se pretende que el lector comprenda el *blockchain* como una oportunidad en lugar de como una amenaza, capaz de ofrecer una respuesta jurídica conforme al sistema normativo actual y un servicio más seguro y transparente.

Palabras clave: *blockchain*, tecnología, administración de justicia, efectos jurídicos y *smart contracts*.

Abstract

The emergence of blockchain technology is articulating a new reality from a legal-regulatory and procedural perspective". The Administration of Justice is immersed in three deep reflections resulting from the disruptive characteristics of blockchain: on the one hand, the probative value and legal effects of transactions originating in a blockchain network, including the registration and storage of automated contracts or smart contracts. On the other hand, the legal security and the risks inherent to the protection of personal data; and, finally, the efficiency in the processes that this technology could bring to the current judicial structure as a digital tool. Through an approximate review of this technology, it is intended that the reader understands the blockchain as an opportunity instead of a threat, capable of offering a legal response in accordance with the current regulatory system and a more secure and transparent service.

Keywords: blockchain, technology, justice administration, legal effects and smart contracts.

Índice de contenidos

Índice de tablas

1. Introducción

La presente investigación ha sido fruto del auge de la tecnología *blockchain* en los distintos sectores socio-económicos, principalmente en el ámbito financiero y de los seguros. La incertidumbre y la desconfianza arrolladora que han provocado los acontecimientos acaecidos alrededor de las monedas virtuales frente a los defensores de su seguridad y transferencia, supusieron el punto de arranque a la actual obra con el fin de conocer, analizar y aportar un visión compatible entre lo jurídico y lo tecnológico.

1.1. Justificación del tema elegido

Los esfuerzo europeos de construir un mercado único digital, de crear infraestructuras y redes que permitan compartir información entre las distintas autoridades, así como proteger y garantizar el cumplimiento de todos los derechos inherentes a entidades físicas y jurídicas en un mercado cada vez más globalizado y deslocalizado, comenzaron a ser un punto de inflexión para investigar y profundizar en aquellas tecnologías que había detrás de estos objetivos europeos. Y entre estas tecnologías, aparecían términos como descentralización, confianza, inmutabilidad, transparencia y evidentemente, bitcóin, provocando cierta curiosidad en la tecnología *blockchain.* Sobre todo, en cómo estas novedades podían confluir en el sistema jurídico español y cómo podrían tener cabida un sistema sin intermediarios en el ámbito de los servicios públicos.

La aplicación de las redes públicas y descentralizadas, así como las privadas o permisionadas, como alternativa estas últimas a algunos riesgos adherentes a las primeras, han sido objeto de prueba y posterior implementación por el ámbito privado. Este sector ha ido experimentado los beneficios y oportunidades que otorgan este tipo de redes basadas en *blockchain.* Sin embargo, actualmente, la comunidad científica y jurídica continúan indagando con la finalidad de establecer un sistema de gobernanza, una arquitectura sólida y sobre todo, un marco jurídico capaz de amparar estas nuevas transacciones y proteger las situaciones de vulnerabilidad que el uso del *blockchain* pueda desembocar tanto en las esferas privadas como públicas.

La labor de los jueces de interpretar y valorar las pruebas digitales aportadas a un procedimiento judicial, en relación a una red *blockchain*, aún no cuenta con criterios unificados ni con una doctrina que permita delimitar con precisión los efectos jurídicos de

una relación contractual registrada en una red descentralizada. Es por ello, que la presente obra ha sido reflejo de la cohesión de diversas fuentes para así ser capaz de integrar el *blockchain* y sus interpretaciones, en la función jurisdiccional encomendada a los Juzgados y Tribunales.

1.2. Problema y finalidad del trabajo

Los avances normativos que hasta ahora se han experimentado en la justicia a causa de la tecnología y sus herramientas funcionales, técnicas y organizativas, son fruto de haber logrado una mayor eficacia y calidad en los sistemas judiciales de todos los estados miembros de la Unión Europea. Sin embargo, frente a la pausada actualización normativa, la tecnología sigue avanzando a un ritmo incontrolable, no existiendo una asincronía entre la tecnología y el derecho. Por esa razón y ante las deficiencias tecnológicas que acaecen en la justicia española, los procesos se ralentizan, la seguridad se debilita y la transparencia e independencia se cuestionan. Ello, deriva a su vez, en los señalamientos tardíos y que han sido objeto de recurso de amparo por vulnerar la tutela judicial efectiva (*vid*. STC 125/2022, de 10 de octubre de 2022); en ciberataques a los sistemas informáticos como el sufrido por el Punto Neutro Judicial en octubre de 2022 y en ocasiones, «la falta de compatibilidad entre los sistemas de gestión procesal, que puede originar, como ha sucedido, la falta de la imagen en las videoconferencias celebradas entre tribunales situados en diferentes comunidades autónomas» (CABRERA et al. 2022, p. 26).

La tecnología disruptiva que ha motivado esta investigación, se contempla como una herramienta cualificada y competente para salvaguardar las grietas que actualmente, el sistema judicial tiene en su arquitectura procesal. A pesar de lo anterior, se requiere de una especial cautela en cuanto a los riesgos que surgen de una tecnología inmadura en su aplicación al ámbito judicial.

La carga de trabajo que jueces y fiscales en reiteradas ocasiones han pronunciado, también se podría mermar mediante el empleo de sistemas de consultas de expedientes, resoluciones o cualquier información de manera inmediata y segura. Además, la interoperabilidad entre administraciones públicas, privadas, nacionales e internacionales no siempre queda garantizada ante un ecosistema protagonizado por la delegación de competencias a las Comunidades Autónoma y por los distintos marcos de gobernanza

judicial existentes en los países. *Blockchain* puede ayudar, incentivar o mejorar la concepción de la justicia en España, como servicio público lento, arcaico, politizado y deficiente.

1.3. Objetivos

Objetivo General

Determinar el potencial impacto de la tecnología *blockchain* sobre el sistema judicial español.

Objetivos Específicos

- Estudiar las particularidades de la tecnología *blockchain,* los derechos procesales afectados y las distintas alternativas ofrecidas por expertos en materia jurídica ante la irrupción de esta tecnología.
- Revisar el marco regulatorio europeo, las iniciativas en marcha sobre la cadena de bloques y la jurisprudencia de aplicación a esta materia.
- Realizar una aproximación sobre los riesgos y perjuicios que se pueden derivar del uso de esta tecnología y conjuntamente, delimitar el modelo de gobernanza adecuado para práctica judicial.
- Analizar las aplicaciones desarrolladas en el sector privado, así como en las Administración Pública.
- Conceptuar la evolución de la justicia digital en España e identificar las utilidades y beneficios que esta tecnología es capaz de aportar al sistema judicial y desde una perspectiva de eficacia procesal.
- Profundizar en el marco normativo actual, con el fin de delimitar los efectos jurídicos de las relaciones creadas y registradas en *blockchain.*
- Concienciar sobre la escasa regulación normativa sobre la materia objeto de investigación.
- Evaluar el potencial impacto de la tecnología *blockchain* sobre los procedimientos judiciales.

2. Marco teórico y desarrollo

La tecnología *blockchain* o cadena de bloques nace, entre otras, con la finalidad de crear un registro de datos descentralizado, transparente e independiente a las decisiones adoptadas por los poderes públicos. Lejos de la base técnica y matemática que rodea a esta nueva tecnología, resulta determinante conocer cómo una red blockchain condiciona, complementa y revoluciona las relaciones personales, sociales o profesionales en una esfera caracterizada por la rigidez normativa y por la pausada adaptación a los cambios tecnológicos (ALI et al. 2021).

2.1. Concepto y características de la cadena de bloques

A pesar de que la tecnología *blockchain* empezó a ser desarrollada hace décadas por especialistas en programación informática, su primera aplicación definitiva se vincula directamente al nacimiento del Bitcóin y a su uso como libro mayor abierto donde únicamente se almacenaban las transacciones con monedas digitales. El nacimiento de esta tecnología, irrumpiendo en la revolución digital, supuso la transformación de las relaciones económicas, sociales, jurídicas y políticas pero al margen de todo el engranaje jurídico que regula actualmente estas relaciones.

En este sentido, la teoría formulada por Satoshi Nakamoto en el conocido *paper*, publicado en 2008 y titulado *Bitcoin: A Peer-to-peer Electronic Cash System*, fue el punto de partida para el lanzamiento de esta tecnología y de la primera criptomoneda. La cadena de bloques surgió con la finalidad de ser la alternativa al sistema financiero que subyace en esta década, regulando la toma de decisiones directamente entre particulares, de forma transparente y segura. De esta forma, «nace un sistema para transacciones electrónicas» sin depender de la confianza depositada en los intermediarios y lejos de ser un sistema sometido o supervisado por ninguna autoridad estatal o central.

En consonancia con lo anterior, comienzan a prosperar las tecnologías de registro distribuido o *Distributed Ledger Technology* (DLT, según el término anglosajón), y entre ellas, el *blockchain,* como un *software,* un libro mayor de contabilidad o una base de datos generadora de confianza a través de mecanismos de consenso y de un registro secuencial en forma de cadena (TAN, MAHULA Y CROMPVOETS 2022). La arquitectura empleada por una red distribuida es la que se conoce como *Peer-to-Peer,* en virtud de la cual, las transacciones

se ejecutan directamente de particular a particular, sin intermediarios o terceros que sustenten o validen esta operación. En este sentido, un mismo participante (*peer* o nodo) podría actuar en un momento determinado como servidor y posteriormente, como cliente (NASIR *et al.* 2021, p. 3). El término nodo se configura como cada uno de los equipos informáticos que están conectados a una red *blockchain*, almacenando y distribuyendo una copia actualizada en tiempo real de la cadena de bloques.

Los nodos constituyen un eslabón fundamental en este tipo de tecnología, por tener la función, entre otras, de decidir y validar la información que se puede incorporar a la red. Estas validaciones se realizan a través de los mecanismos de consenso, principalmente, a través del conocido *Proof-of -Work* (*PoW*, por sus siglas en inglés), utilizado principalmente en redes públicas y sin permisos (como son, Bitcóin y Ethereum). Este mecanismo de consenso, se sustenta en la resolución de un complejo trabajo computacional (también denominados, protocolos de consenso) que acarrea un elevado coste de energía, pero que sin embargo, otorga una mayor seguridad ante un ataque cibernético. Desde un punto de vista energético, estas pruebas de trabajo suponen una auténtica amenaza para el clima global debido a las emisiones de efecto invernadero. Las instituciones europeas en línea con los objetivos para reducir las emisiones de gases de efecto invernadero marcados por la política de la UE para 2030, están instando nuevas propuestas e iniciativas para mitigar los efectos sobre el medio ambiente y la preocupante huella de carbono que provocan las criptoactivos (ESTELLER 2022).

Para tener una perspectiva objetiva sobre la huella ambiental, en este caso de Bitcoin, se recogen las estimaciones obtenidas, a fecha 21 de septiembre de 2022, por el Índice de Consumo de Electricidad del Centro de Finanzas Alternativas de la Universidad de Cambrigde: *actualmente, se estiman 48,35 MtCO 2 e (millones de toneladas de dióxido de carbono equivalente) y representa aproximadamente el 0,10 % de las emisiones mundiales de gases de efecto invernadero y es similar a la de países como Nepal (48,37 MtCO 2 e) y la República Centroafricana (46,58 MtCO 2 e), o aproximadamente la mitad de la minería de oro (100,4 MtCO 2 e)*[1].

[1] Texto de traducción propia. Fuente: https://www.jbs.cam.ac.uk/insight/2022/a-deep-dive-into-bitcoins-environmental-impact/

En relación con lo anteriormente expuesto y para incentivar la participación continua de los mineros (usuarios que resuelven complejos problemas matemáticos), surgieron los sistemas de incentivos o recompensas, principalmente monetarias. Estos incentivos económicos colisionan con los principios y valores de los servicios públicos, siendo más acertado aplicar, en el seno del sector público, otros mecanismos de recompensas como pueden ser la asignación de *tokens* (TAN *et al*. 2022) o implementar otros mecanismos de consensos conforme a lo expuesto seguidamente.

Por las deficiencias que suponen las técnicas de minería basadas en la prueba de trabajo, surgieron nuevos mecanismos de consenso, como la prueba de participación (PoS, por sus siglas en inglés, *proof-of-stake*) y de autoridad (PoA, por sus siglas en inglés, *proof-of-authority*); ésta última, ampliamente implantada tanto en redes públicas como privadas, permite conocer la identidad de los participantes, alejándose asimismo, de la finalidad intrínseca de los mecanismos de consenso descentralizados en la que se otorga a los usuarios un papel protagonista, en detrimento de los modelos de gobernanza tradicionales. En líneas generales, en la PoS para poder *participar* en la validación de las transacciones, se tienen que aportar o apostar una cantidad de criptoactivos, por lo que el poder de cómputo cede frente a la capacidad de garantizar un número determinado de criptoactivos (NASIR *et al.* 2021); por otro lado, en la PoA, las transacciones están garantizadas y autorizadas por los validadores previamente seleccionados, diluyendo así los esfuerzos competitivos entre los mineros.

La preocupación del Banco Central por la huella de carbono que consumen los criptoactivos basados en el PoW, no ha cesado como es comprensible. El pasado 11 de julio de 2022, publicó un informe titulado *Mining the environment - ¿is climate risk priced into crypto-assets?*, según el cual, aseguraba que «la cadena de bloques PoS reduce drásticamente el consumo de energía al tiempo que garantiza la misma funcionalidad[2]», al igual que las estimaciones realizadas por la Fundación Ethereum. Esta última compañía adquirió el compromiso de actualizar la red a prueba de participación durante el 2023, para conseguir una moneda más sostenible. Pese a esta actualización, cabe precisar que el mecanismo de

[2] Texto de traducción propia. Fuente: https://www.ecb.europa.eu/pub/financial-stability/macroprudential-bulletin/html/ecb.mpbu202207_3~d9614ea8e6.es.html

consenso PoA es el más eficiente respecto a los dos anteriores, puesto que es capaz de procesar más transacciones por segundo y además, el mantenimiento de estas redes se realiza únicamente a través de los validadores (es decir, la autoridad participante) y no de los mineros. Sin embargo, esta ventaja relacionada con la escalabilidad puede desnaturalizar en cierta medida la transparencia de la red *blockchain.*

Puntualizar que, tras el consenso alcanzado entre los dispositivos mineros o validadores, la transacción se incorpora a la cadena de bloques y automáticamente se genera una copia en cada uno de esos ordenadores (nodos). Por ello, cuántos más nodos haya en una red distribuida y descentralizada, más segura será la misma a efectos de detectar una manipulación por un hacker.

La identificación de la identidad, la protección de los datos personales y la normativa procesal aplicable constituyen las principales vicisitudes a las que nos enfrentamos en la presente obra. En este sentido y en aras de determinar cómo y bajo qué premisas una red de estas características puede tener cabida en nuestro ordenamiento jurídico, se conceptualizarán de forma sintetizada las principales características de una red *blockchain:*

- Descentralización: se ha puesto de manifiesto cómo la información se incorpora a una red *entre iguales,* donde todos los participantes tienen los mismos derechos y obligaciones, sin la necesidad de autoridades centrales, de intermediarios o de terceros de confianza (NASIR *et al.* 2021, p. 4).
- Inmutabilidad: la inmodificabilidad de los datos en una red *blockchain* es consecuencia del sistema de encriptación que se ha desarrollado a través del conocido *hash*. De manera muy simplificada, un *hash* es el resultado de cifrar una transacción, que tras incorporarse a un bloque con un *hash* inicial*,* vuelve a generar otro *hash* final, cerrando el bloque y siendo la copia cifrada de todas las transacciones que componen ese bloque y que supondrá el *hash* inicial del siguiente bloque cronológicamente. En este sentido, si se modifica un dato, recordemos ya encriptado, «generará una discrepancia en el sistema con el resto de bloques que invalidarían la transacción» (NESPRAL *et al*. 2021, p. 33). Se puede afirmar por ende, que la red goza de integridad en los datos, manteniéndose inalterables desde que se incorporan a un bloque.

- Transparencia: esta característica, predominante en las redes públicas, permite conocer las transacciones que se ejecutan o se agregan al registro cronológicamente. Este elemento está estrechamente vinculado con el principio de publicidad de las actuaciones judiciales, inherente a los Estados de Derecho y el cuál, debe ser garantizado mediante el uso de toda herramienta tecnológica al servicio de la Administración de Justicia. A lo largo de la presente obra, profundizaremos sobre este principio constitucional, amparado potencialmente por una red *blockchain.*
- Trazabilidad: fruto de la inmutabilidad, las operaciones que entran en la cadena de bloques pueden ser rastreadas, comprobándose su origen, su evolución, así como las incidencias que puedan derivarse de una transacción. La trazabilidad ha tenido un fuerte impacto en las cadenas de suministro y las redes de transportes. Se puede establecer del mismo modo, un historial de transacciones jurídico-económicas, conociendo en todo momento aquello que se ha pactado y el grado de cumplimiento de las obligaciones asumidas (MASHOUF 2022, p. 3).
- Seguridad: a través de la criptografía asimétrica estos sistemas son inherentemente seguros. Este tipo de criptografía se define por emplear dos claves, una pública, visible para todos los usuarios y otra privada, únicamente accesible por su propietario.
- Anonimato: la identificación de los sujetos que operan en las redes creadas con tecnología *blockchain,* es un elemento opcional e innecesario en una transacción electrónica; al contrario de lo que sería para un jurista. En las redes públicas, los usuarios no se conocen entre sí, pudiendo operar de forma anónima. Cada persona se identificará con una dirección expresada en números y letras (VALPUESTA, HERNÁNDEZ 2022, p. 34), a diferencia, por ejemplo, de cómo podemos identificarnos cuando entramos a nuestra cuenta corriente *online* de una entidad financiera o accedemos a un registro electrónico, es decir, con nuestro *DNI,* si somos personas físicas o *CIF*, en caso de persona jurídica. Siendo conscientes de la complejidad que en nuestro sistema de protección de datos supone esta casuística, se analiza e investiga en profundidad el impacto que el *blockchain* tiene en la privacidad y protección de los datos de la ciudadanía *(vid.* p. 29*).*

Conocedores de los elementos más diferenciadores de esta tecnología, la integridad e inmutabilidad de los datos almacenados en la cadena de bloques, no debería dejarnos indiferentes ante las consecuencias y utilidades que podría promover en el ámbito de las Administraciones Públicas; ello, por permitir registrar información en tiempo real y a su vez, sellada o bloqueada por su sistema técnico de claves criptográficas. La autenticidad de la información aportada por un ciudadano a la Administración Pública, se podría alcanzar en apenas unos instantes si se confía en este tipo de herramienta, que por su arquitectura, es capaz de certificar la información de manera segura y transparente, principalmente sobre tres aspectos relevantes: en primer lugar, sobre el hecho o acto que se registra en un bloque; en segundo lugar, sobre la identidad de las partes implicadas (esto, propio de las redes privadas y permisionadas); y por último, sobre el momento temporal en el que la transacción o información ha quedado sellada por el *hash* de cierre o final de cada bloque (RÍOS 2021).

2.2. Tipos de redes *blockchain*

La tecnología de registro distribuido (DLT) como el *blockchain,* posee características diferenciadoras entre sí según la red en la que se participe. A tal efecto, se distinguen principalmente, tres redes *blockchain,* siendo el punto de partida la red pública o sin permisos. En esta red, cualquier persona con acceso a internet y sin ostentar una clave privada o permiso específico, puede descargarse una copia de la cadena de bloques, enviar transacciones a otros usuarios y validar a través de las técnicas de minería y bajo un mismo protocolo, entendido éste como el lenguaje de comunicación informático que todos los miembros de una red tienen que utilizar para comunicarse entre sí. En este tipo de redes, se puede llegar a concebir que una mayor seguridad, se contrarresta con una menor privacidad de la información almacenada.

El fin innato de estas redes, de garantizar las transacciones al alcance de cualquiera (sin intermediarios) y mediante un código abierto disponible para todos, ha desembocado en una problemática jurídica en cuanto a garantías y protección de derechos, tanto individuales como colectivos. Las redes públicas han evolucionado hacia las redes privadas, satisfaciendo en cierta medida los problemas de seguridad y distribución que acontecen en las redes públicas.

En este sentido, las redes privadas se configuran para ser usadas por una comunidad de usuarios limitada y restringida, los cuales determinarán los permisos de cada integrante (*permissioned)*. Los usuarios deberán ser identificados o identificables para poder otorgarle un permiso de lectura o de escritura. Este tipo de redes privadas y permisionadas, son las que se están comenzando a implantar en organizaciones privadas o en Administraciones Públicas y que, en virtud de la cual se pueden garantizar las operaciones a nivel interno sin exponerlas a usuarios ajenos. Como se puede intuir, tal y como afirmó PEREA (2020), «resulta obvio que en esta segunda categoría las notas esenciales de *Blockchain* —la descentralización de la confianza…— se diluyen parcialmente por cuanto el sistema opera en una suerte de circuito cerrado y mediante la autorización de actuaciones por una autoridad central. Sin embargo, no podemos desconocer que este dato en realidad no desnaturaliza lo que es propiamente la técnica de cadena de bloques, sino que atañe únicamente al acceso a la participación de la misma». Y es por ello, por lo que no dejan de florecer las ventajas que, sobre la gestión de recursos y optimización de procesos, promueven este tipo de redes.

En tercer lugar, una combinación entre las redes públicas y privadas, confluyen en las conocidas como redes híbridas y federadas. Las redes híbridas nacen con el fin de otorgar una mayor seguridad a las redes privadas, en tanto que las transacciones o registros de *hash* se almacenan en una red pública, continuando no obstante, el acceso privado a la red (SANCHEZ 2020, p. 73). Por otro lado, las redes federadas afloran para salvaguardar la característica de la descentralización propia de una red originariamente basada en *blockchain,* no existiendo una única autoridad u organización que controle o administre la red sino que son grupos de entidades públicas o privadas quienes administran conjuntamente los permisos y las validaciones y además, mantienen copias públicas para todos los usuarios de la red y sincronizadas. En este tipo de redes, «el acceso suele establecerse mediante una interfaz web que los administradores ponen a disposición del usuario, en lugar de compartirles una copia de la cadena como en las redes públicas» (ESPUGA 2021, p. 4).

2.3. Los oráculos como fuentes externas de información

Los oráculos en la cadena de bloques es un elemento de confianza y posiblemente el más vulnerable, por no regirse por los mecanismos de consenso ni protocolo como el resto de los participantes en la cadena *on chain.* Esta figura despliega sus funciones en paralelo a la

ejecución de un contrato inteligente. En este sentido, los oráculos se pueden entender como aquel tercero de confianza (ajeno a la red *blockchain)* sobre el que las partes encomiendan la función de informar sobre los hechos acontecidos en el mundo exterior y que pueden determinar el devenir del *smart contract* registrado (MASHOUF 2022, p. 5).

Por tanto, los oráculos como fuente de información indirecta y como intermediario entre la red *blockchain* y el mundo exterior, pueden ser altamente vulnerables y por ende, el contrato inteligente. Esto supone una limitación inherente a los contratos inteligentes registrados en base a un código matemático y encomendados a que el algoritmo predefinido se ejecute. Este tipo de contratos son ajenos e independiente a cualquier acontecimiento que tenga lugar en el mundo real, por lo que se busca una figura híbrida a través de los oráculos para mejorar este defecto (UE BLOCKCHAIN OBSERVATORY AND FORUM 2022, p. 9).

El empleo de los oráculos también se ha concebido como un factor de conexión que salvaguarda la cuestión de la territorialidad y su difícil aplicación en un entorno digital. De acuerdo con CASTELLÓ (2021, p. 464), «la detección de factores de vinculación es clave para la adaptación de nuestras soluciones tradicionales», constituyendo los oráculos un factor en aras de mejorar la seguridad jurídica que se produce cuando un contrato inteligente pierde su territorialidad.

Como más adelante se expondrá, los contratos inteligentes se podrían implementar en el sistema judicial, agilizando procedimientos estandarizados y por unas reglas bien delimitadas y sin margen de interpretación; en el supuesto que ahora nos incumbe, identificaríamos los oráculos como aquellos funcionarios que tras una notificación sobre consignación de cantidad por ejemplo, informaría a la cadena de bloques para que ejecute la orden de pago o más bien, si no se realiza en el plazo concedido la consignación sobre la cantidad adeudada, se informaría para que ponga en marcha el proceso de ejecución. Lógicamente, este mecanismo está lejos de la realidad procesal y del sistema digital que actualmente está implementado, siendo necesario afrontar muchos de los retos expuestos en el *apartado 5.*

3. Marco normativo de la tecnología *blockchain*

Supondría un elevado esfuerzo, comprender la evolución, utilidades, aplicaciones, así como sus riesgos y desafíos de la tecnología *blockchain* si no retrotraemos nuestra posición inicial al marco normativo europeo. Así, un futuro lector de esta investigación será capaz de reflexionar y concienciarse sobre el "camino" que aún nos queda por trazar, desde el punto de vista normativo y procesal, en el sistema jurídico español.

3.1. Desde una perspectiva europea

Esta breve pero imprescindible aproximación al marco europeo podrá sensibilizarnos sobre cómo la tecnología disruptiva objeto del presente, es capaz de aunar las necesidades de los ciudadanos en sus relaciones con las Administraciones Públicas, de una forma más satisfactoria, ágil y segura, aunque no exenta de determinados riesgos. Sobre todo, en el ámbito de la protección de datos personales en relación a las posibles intromisiones que como en cualquier sistema tecnológico puede existir, por mínimo que sea.

La tecnología *blockchain* forma parte de los objetivos de la Unión Europea como un eslabón más del futuro digital, examinando las posibilidades, entre otras, que la tecnología de registro distribuido y descentralizada podría tener en la prestación de servicios públicos a los ciudadanos. Prueba de ello, encontramos instrumentos normativos con expresas referencias a esta tecnología disruptiva, como el reciente Reglamento UE 2022/858, de 30 de mayo de 2022 sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado, aplicable a los servicios financieros así como iniciativas y aplicaciones que evidencian que es posible avanzar hacia una mayor simplificación administrativa, siendo a su vez conscientes de la cautela que, *de facto*, esta tecnología exige y de las garantías que a cada sujeto de Derecho le corresponden y que no se pueden traspasar.

Los instrumentos normativos que la UE aprueba y desarrolla, son el punto de partida para que los Estados Miembros normalicen e implementen esta tecnología en las relaciones jurídico-públicas. En relación a la iniciativa de la Comisión Europea, el Comité Económico y Social Europeo (en adelante, CESCE) emitió el Dictamen sobre «La tecnología de cadena de bloques y de registros distribuidos: una infraestructura ideal para la economía social», publicado el 18 de node 2019 y en virtud del cual, se recomendaba y solicitaba a las

autoridades públicas garantizar «que la tecnología de cadena de bloques se desarrolle dentro del respeto de las normas en materia de tratamiento de datos personales y de ciberseguridad, prestando atención a los riesgos de acaparamiento o uso indebido de los datos de los ciudadanos y las empresas».

Bajo una conceptualización de la cadena de bloques como un protocolo informático y de comunicación sobre un registro público y basado en la confianza mutua de los distintos actores, resulta necesario atender previamente a la implementación en el seno de las Administraciones Públicas, al marco regulatorio sobre el que puedan operar los principios de buena fe y confianza legítima inherentes al normal funcionamiento de las Administraciones Públicas; ¿se podría corresponder este marco regulatorio con las normas de consenso o protocolos de confianza, en las cuáles se basa el funcionamiento de la cadena de bloques? (GARCÍA-VALDECASAS 2022, p. 164). Y ello, no resulta un objeto inalcanzable si nos trasladamos a otros países europeos y a los avances en ellos producidos, tal y como se expondrá a lo largo de la presente investigación.

En consonancia a las pautas, objetivos y recomendaciones emitidas por las distintas Resoluciones del Parlamento Europeo, se hacen visibles los avances que favorecerían la implantación de la tecnología *blockchain* ámbito de las Administraciones Públicas:

- En primer lugar, facilitaría a los ciudadanos elegir aquellos datos que desean compartir con un registro distribuido público y además, otorgar distintos permisos de acceso a esos datos. Esta forma revolucionaria del tratamiento y compartimentación de datos, unido a la premisa de inmutabilidad de la información registrada, ha estimulado la confianza de los ciudadanos sobre las transacciones y los datos almacenados en una replicada cadena de bloques.
- En segundo lugar, el poder de la automatización de la que presume esta tecnología, incentivaría una mayor eficiencia y simplificación administrativa.
- En tercer, como herramienta que mejora la interoperabilidad y la armonización entre los sistemas de los Estados miembros.

Tal es la inquietud de la Unión Europea de otorgar una mayor seguridad jurídica, así como de reforzar la aplicación de la tecnología *blockchain,* que en febrero 2018, la Comisión Europea puso en marcha el proyecto piloto «EU Blockchain Observatory and Forum», con la finalidad

de acercar a las naciones y a la ciudanía el concepto de la cadena de bloques, crear sinergias entre expertos sobre esta tecnología, identificar obstáculos y encontrar futuras soluciones que aceleren el ecosistema de desarrollo en *blockchain*. Actualmente, lo forman los 27 Estados miembros de la Unión Europea, Noruega y Liechtenstein, creándose una comunidad para incentivar el diálogo y el conocimiento con el objeto de arrojar resultados que otorguen transparencia y rigor en los casos de uso de esta tecnología. Para consolidar la posición de Europa como líder mundial y fruto del compromiso de los socios europeos junto con Noruega y Liechtenstein, nació la «European Blockchain Partnership (EBP)», con el fin de desarrollar una Infraestructura Europea de Servicios de Blockchain (EBSI, por sus siglas en inglés), que «mejore la provisión de servicios transfronterizos para el ciudadano y favorecer la movilidad ciudadana y empresarial, garantizando el cumplimiento de la normativa de la UE» (MERCHAN Y MARTIN 2020, p. 6).

Esta infraestructura está implantando una red de nodos distribuidos en toda Europa, completamente descentralizada, pública, permisionada, sostenible, interoperable, escalable y abierta, cumpliéndose en cada caso las prioridades claves marcadas por la Comisión Europea, como son, «la sostenibilidad ambiental, la protección de datos, la identidad digital, la ciberseguridad y la interoperabilidad» (EBSI 2018). Además, bajo una arquitectura de tres niveles implementada en la red EBSI, se establecen un conjunto de servicios centrales, es decir, interfaces estandarizadas que capacitan a terceros el desarrollo de sus aplicaciones. Al margen de las cuestiones puramente técnicas, estas interfaces se pueden concebir, desde la perspectiva adoptada en la presente investigación, como un servicio de certificación que garantiza que todo proyecto en desarrollo, cumpla los principios esenciales marcados por la EBP (CEF CONNECTING EUROPE, 2021):

- Que identifique una necesidad pública y sea capaz de aportar valor a los ciudadanos y a los Estados Miembros.
- Que las decisiones se establezcan a través de un sistema de gobernanza fruto del consenso entre las partes interesadas.
- Que, a su vez, esas decisiones estén en armonía con la arquitectura EBSI.
- Que, el código-base a emplear, siempre que sea posible, sea abierto.

- Y finalmente, que toda la infraestructura EBSI esté en consonancia con los valores del sistema jurídico europeo.

En aras de instaurar una red EBSI, la Comisión Europea y la *Asociación Europea de Blockchain* (EBP, por sus siglas en inglés), en 2020, lanzaron el «Programa Early Adopter», con el fin de impulsar los primeros casos de uso en un entorno real y a través de la implementación de varios tipos de credenciales verificables. A día de hoy, aún sigue siendo un reto la verificación de información de manera rápida y segura, de manera que el uso de una red o tecnología *blockchain* puede ser impedimento para la falsificación de documentos. En este sentido, las credenciales verificables de EBSI, se definen como patrones de intercambio de información autónomos en el que los usuarios de las credenciales controlan cómo, cuándo y quién verifica su información a través de una billetera conforme a EBSI.

Este proyecto piloto cuenta actualmente con diferentes familias de casos de uso (credenciales verificables, intercambio de datos de confianza, seguimiento y localización), y dentro de los mismos, existen sectores o dominios sobre los que se pueden aplicar una arquitectura EBSI para crear servicios transfronterizos. Al respecto, encontramos el caso de éxito aplicado al sector de la educación: el proyecto «multiuniversitario» que desembocó en 6 escenarios transfronterizos y que se pueden conocer en la página web de la Comisión Europea; y además, el proyecto usuario conocido como «Viaje de Eva», a través del cual una institución autorizada expedía una credencial verificable sobre su titulación oficial, y Eva a través de su *Wallet EBSI* y la creación de su identidad descentralizada (DID, por sus siglas en inglés) podía presentar esa credencial verificable en cualquier universidad europea.

A continuación, se expondrán algunas apreciaciones, que a mi juicio, han sido determinantes para que los proyectos se hayan podido desarrollar de manera consciente y comprometida con la normativa actual.

En primer lugar, todos estos casos de uso, comparten los servicios técnicos básicos de EBSI, formados por las APIS, los contratos inteligentes y un libro mayor. Los *smart contracts* se encuentran rigurosamente controlados, y no se pueden crear por cualquier usuario, únicamente aquellos que tenga ese permiso específico. El libro mayor característico de esta tecnología, persiste en su funcionalidad de ser un registro de todas las transacciones que operan bajo esta infraestructura, criptográficamente protegidas y a su vez,

implementándose registros específicos y de confianza que velan por una información veraz y acreditada.

En segundo lugar, el papel de los nodos EBSI, sumergidos en una red pública y abierta, se encuentra sujeta a estrictos estándares de seguridad, así como a una previa autorización del Estado EBP representante del Operador que pretende unirse a la red de nodos, favoreciendo así una infraestructura robusta, sin grietas y capaz de garantizar la integridad y protección de la información registrada. En relación con ello, se establecen también las conocidas «pruebas de autoridad» (en contraposición a las pruebas de trabajo) como sistemas de consenso en el cual, los validadores tiene una identidad real y garante sobre las operaciones transfronterizas (CEF DIGITAL 2021).

Como se ha puesto de manifiesto, bajo el nuevo paradigma de Europa Digital, destacamos iniciativas que, a través, de los *building block* o «bloques de construcción» proporcionados por la CE, como soluciones digitales abiertas y reutilizables, han sido capaces de logar un impulso a los proyectos, otorgando soluciones ante problemas que puedan surgir en una transacción entre organismos públicos. Se trae a colación, la Comunicación realizada el 2 de diciembre de 2020 por la Comisión Europea sobre la *Digitalización de la justicia en la UE.* Un abanico de oportunidades*,* en virtud de la cual y a través de los programas de *Justicia* y *Europa digital*, se pretende incentivar la creación de soluciones interoperables y brindar «iniciativas tecnológicas innovadoras basadas en la inteligencia artificial y las tecnologías de registro distribuido».

El primer caso de uso, fue el proyecto European Self-Sovereign Identity Framework Laboratory (eSSIF-Lab), es decir, la creación de una «Identidad Europea auto-gestionada o soberana», financiada con fondos europeos bajo el Programa Horizonte 2020 y teniendo prevista su fecha de fin el 31 de diciembre de 2022 por lo que los resultados definitivos no serán objeto de análisis por esta investigación (CORDIS 2022).

Tomaremos como punto de partida, el derecho de todas las personas a ser identificadas, recogido implícitamente en la Declaración Universal de Derechos Humanos. Este derecho abarca todas las características físicas, género, estudios universitarios, experiencia laboral y multitud de atributos más que, lógicamente no podían ser en sus inicios verificados, todos ellos en un mismo momento o lugar. A su vez, el derecho a ser identificado tiene que estar en equilibro con los derechos fundamentales recogidos en la Carta de los Derechos

Fundamentales de la Unión Europea y en su Tratado de Funcionamiento, principalmente, el derecho fundamental a la protección de los datos personales. Para lograr ser identificados frente a terceros, las autoridades centrales o públicas emiten certificados o documentos validados a su vez por sí mismos. Esta manera de identificarnos, evolucionó hacia lo que conocemos como identidad digital, permitiendo a las personas sobrepasar las limitaciones espaciales y de conectividad y logrando que los consumidores y prestadores de servicios digitales sean identificados de manera confiable y segura. Para ello, los niveles de seguridad adoptados por una cartera europea de identidad digital, constituye uno de los principales retos a afrontar por la UE (CONSEJO DE LA UNIÓN EUROPEA 2022).

Recientemente, se ha adoptado la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital[3], suponiendo un punto de inflexión para la protección de los valores y derechos fundamentales reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea. Tal y como se pone de manifiesto en la Declaración citada, la transformación digital «no debe implicar un retroceso en los derechos» (Preámbulo, Considerando 3), por lo que, la implementación de la tecnología *blockchain* en las relaciones económico-sociales tienen que tener cabida bajo el sistema normativo europeo. Entre los derechos fundamentales que deben ser respetados, se destacan la protección de datos, el derecho a la privacidad, la ausencia de discriminación, la igualdad de género, y de principios como la protección de los consumidores y la neutralidad tecnológica. Por su relación con la presente investigación, se destaca el compromiso manifiesto en la Declaración, hacia los servicios públicos digitales en línea, velando por ofrecer una identidad digital accesible, voluntaria, segura y fiable, garantizando la accesibilidad y la compartición de la información a gran escala y facilitando un acceso a los servicios públicos, fluido, seguro e interoperable.

Frente a la administración de la identidad por autoridades públicas, se pretende conseguir que sea el individuo quien gestione y administre su identidad frente a terceros, sin necesidad de que la identidad sea validada por un proveedor de identidad o de servicios. Este objetivo se alcanzará con el modelo de identidad auto-gestionada y a través de los registros de información descentralizada (como son las redes *blockchain*) y las billeteras

[3] Esta Declaración ha sido publicada en el Boletín Oficial de la Unión Europea el 23 de enero de 2023. Fuente: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32023C0123(01)&qid=1674487975230&from=ES

digitales (esto es, un archivo digital y personal donde se podrán almacenar y administrar todas nuestras claves privadas, nuestras credenciales verificables, etc.). En este modelo se «elimina la necesidad de que la entidad tercera a la que se le presente un activo digital tenga que acudir directamente al emisor para comprobar su veracidad o validez, pues puede hacerlo contra un registro público y descentralizado como son las redes *blockchain*» (ALLENDE LÓPEZ 2020).

El desarrollo de una identidad soberana (SSI, por sus siglas en inglés), segura, abierta y de confianza, exige dar cumplimiento al marco normativo europeo actual. Esto es, por un lado, Reglamento eIDAS (Reglamento nº. 910/2014) relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior; y por otro, el Reglamento General de Protección de Datos (Reglamento nº. 2016/679). Sin embargo, este marco normativo, no es capaz de amparar todas las demandas del mercado que actualmente los organismos públicos y privados consideran más adecuadas, como son las carteras digitales.

En relación a lo anterior, y en aras de avanzar hacia una mayor implementación de las identidades digitales y donde también tengan cabida las credenciales verificables, en junio de 2021, la Comisión Europea adoptó una propuesta de Reglamento eIDAS para respaldar que los ciudadanos cuenten con una identidad digital en todo el territorio europeo y que se consoliden los sistema de identificación electrónica descentralizada en las administraciones públicas. Tal y como se expone en el texto de la propuesta de reforma precitada, «se consideró que las identidades digitales basadas en carteras digitales almacenadas de forma segura en dispositivos móviles representan un activo fundamental que puede ofrecer una solución con perspectivas de futuro. Tanto el mercado privado (por ejemplo, Apple, Google o Thales) como los gobiernos están avanzando ya en esta dirección».

Asimismo, la UE considera esencial la cooperación jurídico-privada, colaborando a tal fin con la International Association for Trusted Blockchain Applications (INATBA), un consorcio formado por entidades públicas y privadas que promueven la adopción global del *blockchain* en diversas áreas, evitando que surjan enfoques fragmentados entre las distintas aplicaciones (MERCHAN Y MARTIN 2020, p. 10).

Acertadamente, la UE se ha esforzado en comprobar tanto la viabilidad técnica de esta tecnología como la jurídica en aras de otorgar una completa protección a las garantías de

todos los ciudadanos en los procedimientos para con la Administración Pública. Consecuencia de numerosas iniciativas, proyectos europeos y grupos de trabajo, la Comisión Europea publicó con fecha de 14 de enero de 2021, lo que se denomina como «Estrategia Europea de Blockchain», en adelante EEB, un folleto de regulación «soft» y de contenido inspirador para los Estados Miembros. Esta propuesta, no es óbice para restarle importancia, no pudiendo negar que la Unión Europea considera el *blockchain* como tecnología emergente y transformadora, esencial para construir un mercado europeo digital, justo, seguro y democrático. Es por ello, que la política de la cadena de bloques de la UE se alinea con los valores europeos, incentiva la innovación y a través de sus distintas iniciativas, desea «acelerar la adopción de tecnologías *blockchain* y crear un marco legal equilibrado y coherente» (EEB, 2021).

3.2. Evolución de la tecnología en el seno del sistema judicial español

No se puede negar que nos encontramos ante un nuevo paradigma del que se derivan, inquietudes, debilidades y retos a los que habrá que enfrentarse con el fin de construir un sistema judicial cada vez más garante, eficaz y dinámico. En aras de alcanzar los objetivos de esta investigación, reflexionaremos y descubriremos cómo el *blockchain* puede incidir positivamente en la actividad judicial, siendo capaz de irrumpir en los procesos como herramienta de eficiencia y agilidad, así como en las materias que pueden ser objeto de un litigio. Todo ello, debiendo adoptar las cautelas necesarias para respetar los derechos de todo justiciable y sin dejar atrás el cometido constitucional encomendado a la Administración de Justicia.

3.2.1. Situación actual de la Justicia Digital

A fin de justificar una escasez regulatoria en torno a los nuevos avances tecnológicos y su implementación en la Justicia como medidas de eficiencia, transparencia y seguridad, resulta proporcionado conocer, en líneas generales, los instrumentos normativos que regulan esta nueva era de la justicia digital. Como uno de los hitos más notorios alcanzados en el ámbito de la Administración de Justicia, se destaca la Ley 18/2011, de de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, por la que se introdujeron conceptos como el Punto de Acceso General de la Administración de Justicia, la Sede Judicial Electrónica, el Expediente Judicial Electrónico o las

comunicaciones por medios electrónicos, así como organismos como el Comité Técnico Estatal de la Administración Judicial Electrónica (CTEAJE), que ostenta competencias en orden a la interoperabilidad de las distintas aplicaciones que se empleen en la Administración de Justicia (CABRERA et al. 2022).

Desde este momento, se aprecia la importancia de lograr la interoperabilidad entre las distintas administraciones y facilitar la comunicación e integración entre ellas (*vid.* artículo 230. 6 Ley 18/2011); un reto que sigue subsistiendo a día de hoy y que, a los efectos de ofrecer múltiples oportunidades de mejora, la tecnología *blockchain* podría ser un buen caso de uso.

El conocido *Punto Neutro Judicial,* constituye «actualmente una red de servicios que ofrece a los órganos judiciales los datos necesarios en la tramitación judicial mediante accesos directos a aplicaciones y bases de datos del propio Consejo, de organismos de la Administración General del Estado y de otras instituciones con objeto de facilitar y reducir los tiempos de tramitación, de aumentar la seguridad, y de mejorar la satisfacción de los usuarios», según se define en la web del Poder Judicial en España. Haciendo una lectura de lo anterior, podríamos pensar que los objetos de interoperabilidad entre Administraciones y otro instituciones ha logrado su máxima efectividad pero, en realidad, queda mucho que mejorar, sobre todo en cuestiones de acceso y compartición de información, en tanto en cuento, existen supuestos en los que los ciudadanos no tienen obligación de comunicarse o dirigirse a la Administración por vía electrónica (CABRERA et al. 2022).

A posteriori y también de suma importancia, se aprobó Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET, en fin de dar cumplimiento a las directrices marcadas por la UE en cuanto a la identificación electrónica y los servicios de confianza (Reglamento n.º 910/2014). Esta plataforma permite el intercambio de información entre los Sistemas de Gestión Procesal de los Juzgados y Tribunales y el resto de operadores jurídicos que se relacionan con ellos, «para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por vía telemática, garantizando los requisitos exigidos en las leyes procesales» (DELGADO 2020, p. 288).

En los últimos años, a causa de la crisis del COVID-19, las deficiencias procesales en la Administración de Justicia, han florecido y por ende, las necesidades de ofrecer una solución rápida a la paralización de la Justicia ante las medidas restrictivas interpuestas por las autoridades sanitarias. De ahí, que la Ley 3/2020, de 18 de septiembre, de medidas procesales y organizativas para hacer frente al COVID-19, estableciera en su artículo 14, la preferencia de las vistas o distintos actos procesales por vía telemática. Sin embargo y no entrando en el fondo del asunto, la cuestión más problemática reside en la escasez de medios técnicos, ágiles y eficientes, para realizar este tipo de actuaciones judiciales.

Llegados a este punto y ante los intentos de mejorar la digitalización de la justicia y solventar sus deficiencias, el 22 de abril de 2022, se han aprobado, por un lado, el Proyecto de Ley de medidas de eficiencia procesal del servicio público de Justicia (PLMEPSPJ) y por otro, el Proyecto de Ley Orgánica de eficiencia organizativa del servicio público de Justicia. Entre las medidas más significativas (PLOEOSPJ), se destacan brevemente las siguientes:

- Sistema de notificaciones entre las personas jurídicas, a través de la Dirección Electrónica Habilitada (DEH), ya implementada en otras administraciones públicas, como la Agencia Tributaria. Tal y como se recoge en la exposición de motivos del PLMEPSPJ, esta medida promueve los emplazamientos de forma más segura, rápida y eficaz. Los mecanismos de cifrado que la tecnología *blockchain* emplea podría ser una herramienta capaz de lograr los objetos de esta futura Ley.
- Generalizar la celebración de vistas telemáticas y promover nuevas herramientas tecnológicas que se adapten a los nuevos cambios sociales y normativos.
- Implementar el expediente electrónico desde su inicio hasta su fin en todas las Administraciones Públicas. Aún se siguen remitiendo a los Juzgados, expedientes escaneados y tramitados por un organismo autonómico, por ejemplo.

En definitiva y a pesar de que paulatinamente se están produciendo avances en la digitalización de toda la arquitectura judicial, los esfuerzos legislativos capaces de amparar y respaldas nuevas tecnologías, como el *blockchain,* constituyen un reto aún en trámites.

3.2.2. Un nuevo marco de gobernanza

Siendo conscientes de las características que definen este tipo de tecnología, es inevitable pensar que la gobernanza de *blockchain* se sumerja en una contradicción con los propósitos

gubernamentales y de la administración pública, como son el control, la coordinación y la gestión de los servicios públicos. La descentralización frente a la centralización, está instaurándose como un nuevo paradigma, a fin de incrementar la eficiencia, la transparencia, la integridad y la trazabilidad de los datos, no dejando atrás, el riesgo y la incertidumbre que este modelo de gobernanza puede provocar en el sector público.

La tecnología *blockchain,* podría suponer un cambio en las relaciones intraprocesales (entre los distintos órganos judiciales), así como en las extraprocesales, mediante la incorporación de nuevas fuentes de prueba, como más adelante se estudiará. Si bien es cierto, que el proceso digital y la transformación tecnológica de la justicia han empezado a tener cabida en nuestro sistema normativo y judicial, la tecnología disruptiva como por ejemplo, la cadena de bloques, ostenta aún una posición débil en las Administraciones Públicas. Y ello, porque para poder implementar sistemas descentralizados e inmutables, se necesita emprender una transformación cultural, organizativa y profesional de la Administración de Justicia.

En este sentido lo puso de manifiesto (DELGADO 2020), quien exponía la importancia de «tener en cuenta que no se trata de la aplicación de soluciones tecnológicas para mejorar el funcionamiento de la justicia, sino que la transformación digital exige que la tecnología vaya acompañada de una reformulación de la forma en que se presta el servicio al ciudadano». En relación a ello, y pese a la complejidad técnica de esta tecnología, el sistema judicial y por ende, todos los operadores que lo componen, deberían de ser conocedores de su funcionamiento y de las implementaciones en la realidad del tráfico jurídico, como por ejemplo, en el ámbito contractual o negocial a raíz de los contratos inteligentes.

Junto con la transformación cultural, surge la necesidad de crear un nuevo marco de gobernanza que incluya la digitalización de la Administración de Justicia como orden de prioridad y con el fin de «acoger las nuevas directrices de eficiencia procesal, organizativa y digital que permitan regular un expediente judicial 100% electrónico sobre el que se puedan aplicar de una vez por todas estas tecnologías emergentes» (BONILLA Y DE CASTRO 2021, p.7).

De conformidad a lo anterior, conviene analizar las decisiones de gobernanza sobre tres niveles interrelacionados. En primer lugar, el nivel micro, seguido del nivel intermedio y macro. Acorde con la distinción realizada por TAN *et al*. (2022), las decisiones de gobernanza a adoptar en cada nivel, son las siguientes:

- Nivel micro: las decisiones a adoptar ahondarían sobre la arquitectura de la red (pública/privada o con permisos o sin permisos), la arquitectura de la aplicación descentralizada (DApps) que permita el acceso de los usuarios a una cadena de bloques y sobre la interoperabilidad.
- Nivel meso o intermedio: hace referencia a las relaciones entre la comunidad *blockchain,* esto es, entre «mineros, verificadores, desarrolladores principales, poseedores de *tokens,* productores de contenido y usuarios de la red»[4]. En este nivel se decidirá sobre el sistema de incentivos a implementar, los mecanismos de toma de decisiones (gobernanza en cadena o fuera de la cadena) y sobre los mecanismos de consenso.
- Nivel macro: este nivel se centra en las reglas y normas que se derivan de los principios y valores constitucionales, culturales, históricos y legales de un sector o institución, siendo determinantes en la elección de los modelos de organización y control a adoptar.

Por otro lado, también resulta imprescindible atender a la interoperabilidad y a la sincronización de las bases de datos judiciales. Se lograría una mayor agilidad procesal si el orden judicial que esté conociendo de un asunto pudiera consultar de manera inmediata los datos de un procedimiento de otra naturaleza o de un justiciable. Por ello, se debería de apostar por la implantación de tecnología como el *blockchain* que permita reducir los tiempos de consulta y de información, favoreciendo así la resolución más eficiente de un asunto.

Está claro que la Administración Pública tiene que ofrecer medidas oportunas a los ciudadanos garantizando su seguridad y no vulnerando sus derechos y libertades. Debido a la escasez de pruebas empíricas que validen la tecnología *blockchain* en el ámbito de los servicios públicos y principalmente, en materia de identidad digital, el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, recoge en su artículo 3, la inadmisibilidad de los sistemas de identificación basados en tecnología de registro distribuido. Una evidencia más de que se

[4] Texto de traducción propia. Fuente: https://doi.org/10.1016/j.giq.2021.101625

necesita un marco regulatorio que ampare los riesgos referentes al tráfico de datos en una cadena de bloques. Como ya se ha puesto de manifiesto, en el mercado europeo se está desarrollando una Identidad auto-soberana, con el fin de que el titular de los mismos decida sobre el uso de sus datos personales.

Además, un problema también necesario de resolver es el relativo a los medios a disposición de la Administración de Justicia. Este tipo de redes a nivel de operatividad necesitan un sistema informático fuerte y con capacidades potenciales. Es común, encontrar a funcionarios de la justicia sin poder trabajar por una *caída de sistema* o por la imposibilidad de utilizar los medios tecnológicos en un juicio por inoperatividad, lentitud o colapso de sistema empleado.

Al fin y al cabo, como con el resto de tecnologías que se han ido implementando en el sistema judicial, la aplicación del *blockchain* ha de conducir a redefinir el proceso para lograr un encaje óptimo y garantista entre la normativa procesal y las nuevas formas de enjuiciar, gestionar y almacenar la información.

3.2.3. La protección de datos personales en el seno de una red *blockchain*

Trataremos de hacer una breve referencia y no por ello menos importante, sobre la especial protección que merecen los datos personales de los menores *(vid.* artículo 38 LOPDGDD). Se viene advirtiendo el incremento de menores en las plataformas sobre transacciones de criptomonedas y de los riesgos inherentes a ello, por lo que se deben de instaurar mecanismos capaces de garantizar que los niños no accedan a plataformas donde sus derechos se puedan mermar. En la presente investigación, todo su contenido nace sobre la premisa de que los usuarios participantes de esta tecnología *blockchain* son mayores de edad, conscientes y conocedores de las vicisitudes de su funcionamiento, o siendo menores, gozan de todas las garantías en torno al consentimiento del titular de la patria potestad.

Las características inherentes a la tecnología *blockchain*, principalmente, el carácter inmutable de los datos y transacciones registradas, han supuesto un fuerte impacto en el tratamiento de datos personales y los derechos reconocidos a toda persona física como titular de la información registrada en internet. Al amparo del art. 4 del RGPD, y bajo una conceptualización un tanto genérica, los datos «personales son cualquier información relativa a una persona física viva identificada o identificable», quedando bajo su ámbito de

protección toda aquella información recopilada que pueda inducir a identificar a una persona. Es más, y por su importancia en la materia que nos ocupa, los datos personales que hayan sido anonimizados, cifrados o presentados con un seudónimo, pero que puedan utilizarse para volver a identificar a una persona, siguen siendo datos personales y se inscriben en el ámbito de aplicación del RGPD. En esta línea y como regla general, los datos anónimos, es decir, aquellos que no guardan ninguna relación con una persona física identificada o identificable (Considerando 26 del RGPD) no están bajo el ámbito de aplicación de reglamento citado; sin embargo, los datos seudónimos, sí quedarán sujetos a las previsiones europeas y nacionales en materia de protección de datos.

No siendo objeto de estudio aquellas transacciones que no contienen datos personales, centraremos nuestra atención en aquellas redes *blockchain* que almacenen y traten datos personales, en aras de encontrar las herramientas para identificar, a los responsables de tratamiento, entre otros roles y aquellas garantías de confidencialidad y disponibilidad de los datos (AEPD 2020). Inmersos en cualquier procedimiento judicial, es evidente que los datos que cedemos para nuestra identificación procesal son inexcusablemente personales.

En consonancia a las directrices marcadas por la Agencia Española de Protección de Datos (AEPD 2020) se recomienda, previamente a implantar un proyecto *blockchain*, analizar y dar respuesta a las cuestiones a continuación expuestas.

En primer lugar, en relación a las transferencias internacionales de datos almacenados en una red *blockchain.* Se tendría que dar cumplimiento a lo previsto en el capítulo V del RGPD, a los efectos de garantizar que las transferencias de datos entre cualquier país del Espacio Económico Europeo (en adelante, EEE) y un tercer país u organización internacional, cumplan las garantías previstas en el reglamento comunitario así como las medidas de adecuación aprobadas por la Comisión Europea. Por la propia naturaleza de esta tecnología, los datos almacenados en cada bloque de la red, están distribuidos en cualquier país del mundo (más evidente si cabe, si nos encontramos en una red pública), por lo que sería necesario atender estrictamente a los riesgos consustanciales a esta tecnología, «a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado (*vid*. artículo 44 del RGPD)».

En este sentido, existe un listado de países terceros (no siendo parte del EEE) calificados con un nivel de protección adecuados por la Comisión Europea, no requiriéndose ninguna

autorización para operar con un operador ubicado en dichos territorios. No obstante, tal y como sucede con las transferencias internacionales a EE.UU. (en relación a la resolución del Tribunal de Justicia de la Unión Europea, que declaró inválida la Decisión (UE) 2016/1250 de la Comisión conocida como el Escudo de Privacidad), el artículo 49 del RGPD prevé un conjunto de excepciones o condiciones aplicables en los supuestos de no existir una decisión de adecuación para un país receptor de datos personales.

En segundo lugar, acerca de a la responsabilidad del tratamiento de los datos, cabe decir que en una red pública y descentralizada, no es una tarea sencilla determinar el responsable del tratamiento de datos (así como el encargado o corresponsables del tratamiento), debido a que, por definición no existe un organismo central que controle o verifique las transacciones y la participación de cada usuario. Expertos en esta materia, consideran a los nodos como responsables del tratamiento, puesto que persiguen los fines propios de esta tecnología, como es el almacenamiento de copias en cada bloque. Por el contrario, los mineros o nodos validadores y los desarrolladores de esta tecnología, a priori, no se consideran responsables de los datos por desarrollar, a grandes rasgos, funciones de soporte técnico y no aquellas encaminadas a determinar los fines y medios de tratamiento (*vid.* artículo 47 de RGPD*).*

Si se pretende por otro lado, determinar el responsable de tratamiento en una red privada o permisionada, se podría mitigar este riesgo debido a su propia naturaleza. Los participantes en este tipo de redes están identificados y el carácter de los nodos está preestablecido por los organismos o entidades que administran esa red. Según la clasificación aportada por ESPUGA (2021, p. 9), en la cadena de bloques privada se distinguen tres tipos de nodos: por un lado, los nodos validadores (que al igual que en las redes públicas se encargan de ejecutar el algoritmo de consenso), por otro, los nodos autorizadores como aquellos encargados de otorgar los permisos a los usuarios con acceso a la red y finalmente, los nodos usuarios responsables de las transacciones que se registran en la red y por ende, considerados como responsables del tratamiento de los datos.

En tercer lugar, el efecto inmutable de los datos personales registrados en una red *blockchain*, en principio, provoca un conflicto directo con el derecho de supresión (recogido en el artículo 17 del RGPD y popularmente conocido como derecho al olvido), regulado en los artículos 93 y 94 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantías de los derechos digitales, y de rectificación (*vid*. artículo 16 del RGPD).

En las redes privadas, el ejercicio del derecho de supresión se podría logar estableciendo «protocolos que contemplen la reescritura del bloque en casos concretos» (ESPUGA 2021 p. 10).

La inmutabilidad de los datos propia del *blockchain* y su colisión con estos dos principios, precisa de la «búsqueda de soluciones para la eliminación o modificación de información» (AEPD 2020, p. 45). Entre las soluciones que han nacido fruto de la investigación, predomina la implementación de las funciones «hash», es decir, un código alfanumérico que permite la seudonimización de los datos personales con base en una función criptográfica, de manera que únicamente el titular de esos datos pueda tener conocimiento sobre ellos (MASHOUF 2022, p. 12). Además, recordemos que la réplica de estos códigos cifrados en cada uno de los bloques favorece detectar de manera rápida cualquier alteración en los datos registrados, ya que el código *hash* que se genere con la modificación, será distinto al generado en el registro de entrada originario.

De esta manera, en una primera percepción del funcionamiento de este código cifrado se podría afirmar que, en la cadena de bloques se insertará el código *hash*, quedando fuera de la misma los datos personales (esto es, almacenamiento *off chain* de los datos) (MASHOUF 2022, p. 13). Sin embargo, esto no se puede extender a todas las redes o circunstancias, puesto que también podría contener o ser considerado como un dato personal. Así lo puso de manifiesto ESPUGA (2021) «cualquiera que conozca los datos de entrada puede ejecutar una función hash para verificar el hash que la misma revela tras la introducción de los datos y, por lo tanto, vincular dicho hash a una persona física e identificarla». Por ello, actualmente las funciones *hash* han sido consideradas como técnicas de seudonimización (permiten la reidentificación) y no de anonimización.

Para mitigar este riesgo y asegurar la protección de los datos, es necesario que la información que figura por separado, es decir, *off chain,* esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable (artículo 4.5 del RGPD). Por ello, para evitar la reidentificación del valor del *hash* se vienen empleando algoritmos de cifrados, como es el caso de la criptografía asimétrica empleada por la tecnología *blockchain.* De esta forma, se podrá cifrar el mensaje antes o después de generar el *hash*, pudiendo ser conocido mediante el empleo de las claves. También, resulta necesario implementar mecanismos en aras de que

«los datos personales sean mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales» (artículo 5.1.e) del RGPD).

Tras conocer los retos asumibles en cuanto a la protección de datos personales, trasladémonos al plano jurisdiccional y analicemos, *grosso modo*, cómo los datos personales se protegen en el seno de un procedimiento judicial.

Sin entrar en un análisis pormenorizado sobre la evolución histórica, el principio de publicidad procesal amparado en el artículo 120 de la Constitución Española, se concibe como una garantía de transparencia y control de la actividad jurisdiccional. No obstante, este principio choca con el régimen de protección de los datos personales a disposición de la Administración de Justicia y que ha sido objeto de regulación por la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información en la Administración de Justicia, que implementa el Expediente Judicial Electrónico y la Ley Orgánica 7/2015, de reforma de la LOPJ, introduciendo un capítulo sobre la «protección de datos de carácter personal en el ámbito de la Administración de Justicia».

Está claro que para enmarcar esta normativa sobre un sistema de gestión y organización *blockchain*, se tendría que implementar una red privada y permisionada, en el que cada bloque constituyera un procedimiento judicial, en el que las partes estuvieran identificadas y sobre los que regirían los principios y garantías procesales. Y es evidente, que el Consejo General del Poder, se configuraría como organismo que otorgaría los permisos y contralaría la entrada y salida de usuarios. En este supuesto, tendría cabida la normativa previamente referenciada y precisando destacar el artículo 236 ter de la LOPJ: «no será necesario el consentimiento del interesado para que se proceda al tratamiento de los datos personales en el ejercicio de la actividad jurisdiccional, ya sean éstos facilitados por las partes o recabados a solicitud de los órganos competentes, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba».

Por lo tanto, en el ámbito de la actividad judicial, los riesgos en cuanto al cumplimiento del RGPD, se podrían mitigar puesto que la función jurisdiccional se considera de carácter público, primando a estos efectos sobre la tutela de los datos de carácter personal (GONZÁLEZ 2021, p. 496).

3.2.4. ¿Qué tipo de red *blockchain* sería de aplicación en la justicia?

La posibilidad de que la tecnología *blockchain* permita implementar cadenas de bloques públicas, privadas o híbridas, implica hacer frente a idiosincrasias, arquitecturas y funcionamientos técnicos diferentes. Todo ello, en función del ámbito o sector de aplicación y los servicios que se promuevan a través de su gestión y organización. Resulta evidente que los principios y garantías que se pueden exigir de un servicio público no sean equiparables a los prestados por una organización privada con fines particulares y económicos. En base a ello, analizaremos qué tipo de red habría de implementarse en el marco de una Administración de Justicia con competencias territoriales dispares y con un amplio volumen de operadores jurídicos.

Si todos los usuarios (tanto ciudadanos que son parte en un proceso judicial como funcionarios al servicio de la administración de justicia) de la *blockchain judicial* tienen acceso y permiso para visualizar el estado de todo el expediente judicial (imaginemos que cada bloque de la cadena lo forma un expediente), éste se podría consultar de manera inmediata por cualquiera de estos usuarios. Lógicamente, esta posibilidad de consulta o acceso a un expediente se podría restringir a través de una cadena *blockchain* privada, híbrida o federada; y también a través de los acuerdos de servicios que han sido aplicadas a otras redes públicas, con el fin de restringir y controlar la disponibilidad de los datos (MASHOUF 2022).

La elección sobre el tipo de red a elegir en el servicio público de Justicia, requiere un exhaustivo y detallado esfuerzo de investigación, estudio y análisis sobre su diseño y su arquitectura. Una red privada podría mitigar los riesgos sobre la privacidad de los datos personales; sin embargo se dejarían atrás los beneficios y utilidades que la descentralización podría aportar a este servicio. Por ello, se podría diseñar una red híbrida, restringiendo el acceso a la información al igual que en las privadas pero almacenando los registros *hash* en una red pública que contribuya a incrementar los niveles de seguridad. Las redes federadas también podrían tener cabida en el sistema de justicia, no recayendo todos los permisos de acceso sobre una única autoridad judicial; sino que sean los distintos órganos que forman la planta judicial española (Tribunal Supremo, Audiencia Nacional, Tribunales Superiores de

Justicia, Audiencias Provinciales y Juzgados) quienes otorguen los permisos de acceso a la información almacenada en la *red judicial*[5].

La participación en la red exige un sofisticado sistema de permisos que garantice que las operaciones incorporadas a red han sido validadas por la autoridad competente para ello y conforme a la legislación vigente. Desde que se inicia un procedimiento judicial hasta que finaliza el número de funcionarios que emiten resoluciones, almacenan datos o notifican no son escasos, por lo que se propone asimismo, una *red judicial* permisionada.

Traemos las palabras manifestadas por RÍOS, magistrada del Juzgado de lo Mercantil nº 1 de Barcelona y pionera en el desarrollo de la tecnología *blockchain,* a los efectos de otorgar una mayor confidencialidad a los datos o información aportada: «La idea es utilizar *blockchain* como una cadena permisionada (no podría ser pública), para articular una base de datos en la que determinada información confidencial o secreta relativa a esos procedimientos, quede recogida de forma inmutable y verificable y cuyo acceso esté restringido a los sujetos autorizados por la autoridad judicial. De esta forma, una vez que una información quede registrada y sellada en un bloque, solo el juez pueda autorizar el acceso a la misma, siguiendo un concepto de anillos de confianza o *confidentiallity rings* o autorizaciones personales limitadas a los miembros del personal judicial, los abogados y procuradores de las partes y, en determinados casos a asesores externos».

Tabla 1. Los elementos de una *red judicial*

Bloques	Expedientes o procedimientos judiciales.
Nodos usuarios	Operadores jurídicos en un sentido amplio: Jueces, Fiscales, Letrados de la Administración de Justicia, Abogados, Procuradores, entre otros, aquel ciudadano que sea parte en un procedimiento judicial o cualquier otro usuario que conforme a las reglas procesales se le requiera para su participación en un pleito.
Nodos autorizadores	Los permisos se otorgarán por la autoridad judicial y éstos serán individuales y específicos para cada funcionario judicial según la

[5] Término referente a una red *blockchain* aplicada a la Administración de Justicia.

	función que se le encomiende realizar.
Nodos validadores/Mecanismo de consenso	Prueba de Autoridad. El Juez que ejerza sus funciones en una cadena de bloques autorizará la incorporación al bloque de nuevos documentos o resoluciones a efectos de garantizar una mayor transparencia y trazabilidad. Estas pruebas de consenso se tendrán que basar y regir por un marco normativo que ampare esta técnica de validación y autorización de documentos judiciales.
Almacenamiento de la información	El *hash* de cierre de cada bloque se incorporaría a una red pública para el uso equiparable a cualquier otra base de datos accesible a cualquier usuario (por ejemplo, el Cendoj). El almacenamiento de las resoluciones judiciales deberá cumplir con las previsiones legales y de protección de datos recogidas en nuestro ordenamiento jurídico.
Identificación	Todos los usuarios serán identificados para su participación en la red judicial, a través de su identidad digital auto-gestionada o mediante el uso de las herramientas tecnológicas vigentes (Cl@ve Justicia o Certificado Electrónico).
Sistema de claves	Todos los usuarios deberían tener acceso a una clave pública, que le permitiría acceder al permiso de lectura; sin embargo, la clave privada únicamente debería estar habilitada para aquellos usuarios con permisos de transcripción.

Fuente: Elaboración propia

4. Tecnología con capacidad de producir efectos probatorios

Tras un acercamiento a los estándares tecnológicos que regulan la cadena de bloques, nos sumergiremos en el valor probatorio sobre los datos almacenados en bloques criptográficamente protegidos e inmutables en el tiempo. A tal fin y como resulta evidente, la información registrada en la cadena de bloques deberá cumplir con el principio de legalidad y estar sometida a las normas sustantivas que imperan en nuestro ordenamiento jurídico (RÍOS 2021). Desde el punto de vista procesal, se analizarán las formas de introducir la prueba en el proceso judicial y las garantías que deberá aportar para que el juzgador la califique como un medio de prueba válido. En este sentido, los *smart legal contract* y su interpretación por la doctrina, han constituido uno de los ejes centrales sobre los que han girado los nuevos mecanismos de gobernanza pensados para otorgar eficacia probatoria a este tipo de relaciones contractuales.

4.1. ¿Fuente o medio de prueba?

Previamente y como aclaración, se ha de puntualizar que esta investigación tomará como soporte y fundamento, los conceptos y principios generales del procedimiento civil, de carácter supletorio al resto de órdenes jurídicos (*vid*. artículo 4 Ley de Enjuiciamiento Civil). No obstante, cuando así proceda, se realizarán remisiones expresas a la normativa aplicable a otros procedimientos (como por ejemplo, a la Ley de Enjuiciamiento Criminal, entre otras).

En el sistema procesal español, se realiza una clásica distinción entre fuente y medio de prueba. Por un lado, la fuente es un concepto extrajurídico y ajeno al proceso, constituyendo el soporte sobre el que se registra y almacena información; y por el contrario, el medio de prueba es un concepto procesal, recogido en el artículo 299 de la Ley de Enjuiciamiento Civil (en adelante, LEC) y sobre el que versan aquellos instrumentos o soportes aptos para introducir una fuente de prueba en el juicio. De conformidad al precepto citado, se enumeran como medios de prueba el interrogatorio de las partes, los documentos públicos y privados, el dictamen de peritos, el reconocimiento judicial y el interrogatorio de partes, además de los medios de reproducción de la palabra, el sonido y la imagen.

En este mismo sentido, se pronunció la *Sala de lo Social del Tribunal Supremo, en la sentencia n.º 706/2020, de 23 de julio:* «Medios de prueba son los instrumentos de intermediación requeridos por el proceso para la constancia material de los datos existentes

en la realidad exterior; mientras que la fuente de prueba se refiere a la fuente de información del mundo exterior que está en capacidad de ofrecer el medio de prueba. Las fuentes de prueba que se incorporan al proceso a través de los medios de prueba son ilimitadas (art. 299.3 de la Ley de Enjuiciamiento Civil)».

Si trasladamos estos dos conceptos al ámbito de la cadena de bloques, resulta necesario determinar «en qué medida el libro-registro que constituye la misma puede ser fuente de prueba, y por qué vía los datos registrados pueden ser introducidos en el proceso como medio de prueba» (RÍOS 2021). Atendiendo al concepto de soporte de prueba electrónica, es evidente que el libro-registro tiene naturaleza electrónica por estar todos los nodos conectados entre sí y a través de la descarga de un software en cada ordenador. Ahora bien, una copia de un *hash*, así como de los bloques afectados por una transacción se podría incorporar a un proceso siempre y cuando tenga lugar mediante los medios de prueba legalmente previstos en nuestro sistema jurídico.

En un entorno *blockchain*, procede aportar como prueba documental privada, la impresión del *hash*, es decir, «la clave alfanumérica asociado a un determinado contenido junto a la traducción en un lenguaje que sea comprensible y legible por cualquier persona» (RÍOS 2021). Constituyendo la prueba documental un soporte apto para incorporar al proceso las fuentes de prueba electrónica, nos remitiremos al artículo 3 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, a los efectos de conocer la eficacia probatoria de los documentos electrónicos privados. Al amparo de este precepto, «la prueba de los documentos electrónicos privados en los que se hubiese utilizado un servicio de confianza no cualificado se regirá por lo dispuesto en el apartado 3 del artículo 326 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. Si el servicio fuese cualificado, se estará a lo previsto en el apartado 4 del mismo precepto».

En este sentido y siempre y cuando la prueba aportada haya sido impugnada por alguna de las partes en cuanto a su autenticidad, integridad, precisión de fecha y hora u otras características, se procederá a solicitar, por la parte que la negare, una prueba pericial que coteje y verifique la información aportada o, si lo estimare necesario, podrá proponer cualquier otro medio de prueba. Ese supuesto sería de aplicación cuando el documento haya sido emitido por un servicio de confianza no cualificado conforme al Reglamento 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones

electrónicas en el mercado interior. Por el contrario, en el supuesto de que el prestador de servicio de confianza cumpla los requisitos establecidos en el Reglamento precitado y esté incluido en el listado creado a tales efectos, se presumirá que el documento reúne la característica cuestionada, garantizando la autenticidad del documento desde su emisión.

Es más, en el ámbito de la contratación electrónica, la eficacia probatoria de los documentos electrónicos se refleja expresamente en el artículo 23.3 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, según el cual «los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurran el consentimiento y los demás requisitos necesarios para su validez», es decir, producen los mismos efectos jurídicos que los contratos celebrados en la forma escrita tradicional.

Por tanto, en tal punto, se puede afirmar que el registro en *blockchain, ab initio,* es un documento privado que constituye eficacia probatoria plena (RÍOS 2021). Sin embargo, resulta imprescindible tomar en consideración dos aspectos: por un lado, la identidad y capacidad de las partes contratantes; y por otro, la hipotética pero imprescindible necesidad de tener que aportar un dictamen de un perito experto en *blockchain.*

En relación con la primera cuestión, uno de los objetivos del Reglamento eIDAS es establecer sistemas de seguridad que garanticen la veracidad y la autenticidad de una identidad determinada. Ello, a través de prestadores de servicios cualificados y no cualificados de confianza responsables de los perjuicios que se puedan ocasionar a una persona física o jurídica y bajo la supervisión de una autoridad central (en España, son establecidos y supervisados por el Ministerio de Asuntos Económicos y Transformación Digital).

Bajo el marco regulatorio actual, existe una convergencia entre el servicio ofrecido por los Prestadores de Servicios de Confianza y las pruebas que se puedan constituir bajo una tecnología *blockchain*. A pesar de que esta tecnología disruptiva, goza de una presunción de integridad, autenticidad y transparencia de la información que invalidaría cualquier otro sistema que a posterior pretendiera validar cualquier transacción en ella almacenada; ésta se ha concebido, como un instrumento y no como una alternativa a la fe pública judicial que se viene encomendando al Letrado de la Administración de Justicia.

El concepto tradicional de «fe pública judicial» en consonancia con el principio de legalidad y seguridad jurídica, ha sido objeto de un amplio análisis y desarrollo por la doctrina, recuperando muy sutilmente su concepto por su relación con la función documental en el seno de un procedimiento. En este sentido, «se ha considerado que la autenticidad es la relación existente entre el autor de un documento y su contenido, de tal manera que un documento puede reputarse como auténtico cuando su contenido queda acreditado que se ha realizado por quien aparece como su declarado autor» (PEREA 2020, p.7). A pesar de no existir una consolidada jurisprudencia sobre la autenticidad que podría reportar la tecnología *blockchain* traemos a colación la Sentencia de la Audiencia Provincial de Álava, nº 1032/2021, de 21 de diciembre de 2021 (Rec. 1395/2021), en virtud de la cual, se hace referencia a la utilización de la tecnología *blockchain* como tecnología que permite realizar una mínima auditoría de autenticidad sobre el documento privado aportado por el apelante e impugnado por la parte apelada, equiparando esta tecnología a los otros sistemas que permiten imputar la autoría a quien figura como emisor de un documento (estos son, el Código Seguro de Verificación o CSV o mediante una firma electrónica soportada por una entidad verificada o de confianza).

En relación a la segunda problemática y a pesar de que, al amparo del artículo 326.2 LEC, se podría aportar un documento electrónico privado sin el respaldo de un dictamen pericial, la práctica procesal es distinta. En consonancia a la arraigada doctrina de los tribunales españoles en cuanto a la eficacia probatoria plena de los dictámenes emitidos por expertos en la materia objeto de controversia, «podría parecer imprescindible que el documento privado aportado al proceso venga acompañado por un dictamen pericial elaborado por un técnico experto en *blockchain* que certifique la autenticidad de los datos insertos en la cadena de bloques» (RÍOS 2021).

Siendo conscientes de que la información almacenada en la cadena de bloques adopta la forma de un *hash*, nos ratificamos en la idea de que continúa siendo imprescindible aportar un dictamen pericial de un experto en *blockchain* en tanto en cuanto y salvo excepciones particulares, el juzgador no será conocedor de los aspectos técnicos y funcionales de esta tecnología. En definitiva, como requisitos *sine qua non* para que los datos registrados en la cadena de bloques se puedan incorporar al proceso como medio de prueba, se necesita

tanto la copia del *hash* como su desencriptación y simultáneamente su traducción al lenguaje natural por un perito experto.

Ante un desconocimiento puramente computacional o informático sobre la que se emerge esta tecnología, la tarea de descifrar una función criptográfica *hash* nos podría parecer simple y rápida. Sin embargo, la función *hash* utilizada en *blockchain* es el tipo SHA256 lo que supone que está formada por 64 dígitos hexadecimales de un tamaño fijo de 256 bits (32 Bytes), y de acuerdo a lo manifestado por FUENTES (2022, p. 179), «solo se podría acceder a la información utilizando lo que se denomina explícitamente un ataque de fuerza bruta, que no supone otra cosa que utilizar el sistema prueba-error a fin de obtener por pura repetición los datos encriptados». A esta primera dificultad, se une la necesidad de conocer la clave privada para poder desencriptar un *hash* y tras ello, poder acceder al *smart contract* a los efectos de ser un medio prueba ante un conflicto jurídico.

En contraposición a lo anteriormente manifestado, se podría incorporar al proceso como documento público, aquella información extraída de la cadena de bloques, como podría ser por ejemplo, el *hash* sobre una operación de compraventa**.** De acuerdo al artículo 1.216 del Código Civil (en adelante, CC), se consideran documentos públicos, «los autorizados por un Notario o empleado público competente, con las solemnidades requeridas por la ley», ostentando eficacia *erga omnes* o frente a terceros desde la fecha de su otorgamiento (*vid.* 1.218 del CC*).*

A mayor abundamiento, los documentos públicos admitidos en nuestro ordenamiento se recogen en el artículo 317 LEC, predicándose un listado de documentos *numerus clausus*. Como característica común a todos ellos, consta la intervención de una autoridad pública, ya sea judicial, notarial o registral, que en el ámbito de gestión de sus competencias, son certificadores de la autenticidad de los documentos. Consecuencia de los anterior, el documento electrónico expedido por una cadena de bloques, por sí mismo, no podría tiene carácter público por no poder encuadrarse en la legislación procesal.

A este respecto, sería necesaria una reforma legislativa que equiparase las certificaciones extraídas de la cadena de bloques con los documentos de naturaleza pública. Para ello, «resulta esencial dilucidar si por sus características tecnológicas, la cadena de bloques puede constituir prueba legal y plena sobre el hecho objeto de registro, la fecha correspondiente al sellado de tiempo y la identidad de los sujetos participantes» (PEREA 2020).

A pesar de algunos reclamos por parte de la doctrina de incluir los documentos contenidos en una *blockchain* (RÍOS 2020), no se puede aseverar en todos los casos, el acto, su contenido, la fecha y los sujetos intervienes; constituyendo este último aspecto, el principal obstáculo puesto que en las redes públicas podría ser imposible de conocer la identidad de los participantes.

Otra posibilidad podría recaer en el supuesto de que la parte interesada en aportar un hecho registrado en la cadena de bloques, solicite notarialmente la protocolarización y que en virtud del mismo se certifique la identidad del interesado, el hecho que se ha aportado al notario y la fecha de la presentación de la copia del *hash*.

Como avances en la Administración de Justicia se destaca el Protocolo de protección del secreto empresarial en los juzgados Mercantiles de Barcelona, como proyecto piloto del Consejo General del Poder Judicial (CGPJ). En virtud de este protocolo, se propone crear un *Data Room Virtual* cuando el número de documentos o información aportada al proceso sea muy voluminoso mediante el empleo de tecnología *blockchain* y limitando el acceso a las personas autorizadas por la autoridad judicial. No obstante, pese a la creación de esta propuesta pionera, el mismo texto hace referencia a la escasez de recursos en la Administración de Justicia, manifestando que: «dada la inexistencia de medios materiales en la actualidad en la administración de justicia, la creación del *Data Room* se realizará por una de las partes, que deberá adoptar las debidas precauciones de seguridad, sin perjuicio de que los gastos generados puedan ser incluidos en la condena en costas del proceso».

Por otro lado, la implantación de una red *blockchain* en el ámbito empresarial podría otorgar una mayor capacidad probatoria ante un futuro procedimiento sobre impugnación de acuerdos sociales. RIOS (2020) destacó la utilidad que para la empresa supondría poder acreditar el momento y el contenido tanto de una convocatoria de consejo de administración o de junta general, como del posible acuerdo adoptado. Este avance tecnológico ya ha sido implementado en el Estado de Delaware (EE.UU), modificándose la Ley de Sociedades e incorporando con ella, un sistema de registro distribuido como *blockchain* que posibilita la constitución, supervisión y realización de trámites y operaciones societarias. Este progreso ha otorgado una mayor seguridad transparencia y seguridad jurídica en el sector societario pero también en el mercado de valores y financiero.

La tecnología de la cadena de bloques también puede suponer una oportunidad para los procesos de identificación de las partes en un juicio virtual. A pesar de los esfuerzo técnicos y económicos que supondría el uso de una identidad digital auto-gestionada en el ámbito judicial, se conseguiría una mayor agilidad procesal en contraposición a los largos periodos de tiempo que transcurren desde que se solicita la citación de un testigo o un perito por ejemplo, hasta que es emplazado por el órgano judicial.

4.2. Especial referencia a la eficacia probatoria de los *smart contracts*

La innovación en las redes *blockchain* también ha permitido que esta tecnología de registro distribuido pueda ejecutar de forma autónoma e independiente el acuerdo entre dos partes representado digitalmente, es decir, un *smart contract*. La descentralización e inmutabilidad han culminado en una mayor seguridad frente a la tecnología preexistente, favoreciendo la minimización de errores y la intervención de terceros que otorguen validez (VALPUESTA *et al.* 2022, p. 184). Como esta obra no es de índole tecnológica, este apartado se centrará en cuestiones eminentemente jurídicas con el fin de encuadrar los contratos inteligentes en la normativa vigente en materia contractual.

A pesar de la traducción como contrato inteligente, surge la necesidad de amparar esta cuestión: ¿es en realidad un contrato, *stricto sensu?* Conscientes de las posturas contrapuestas que sobre esta cuestión, en la presente investigación se ha adoptado aquella que ampara a los *smart contracts (o smart legal contracts* desde una perspectiva jurídica) como una nueva modalidad contractual dentro de la categoría comúnmente conocida como contratos electrónicos pero con la particularidad de emplear una tecnología avanzada que afecta tanto a la formación del contrato como a la ejecución del mismo (MADRID 2020). En este sentido, la perfección de un *smart legal contract* se regirá por la normativa aplicable a la contratación electrónica, es decir, por la Ley 34/2002, de 11 de julio, de servicios de la sociedad y más en concreto por el articulado previsto en su Título IV, que en virtud del mismo, se regulan las obligaciones previas de contratación, la puesta a disposición de información clara, comprensible e inequívoca y el cumplimiento de la obligación del oferente de confirmar la recepción de la aceptación al destinatario de la oferta. Ante un conflicto contractual, el juzgador tendrá que valorar si todas las circunstancias que otorgan eficacia jurídica al *smart legal contract* se han cumplido para lo que será determinante que las partes puedan acreditar a través del proceso de generación del *smart legal contract* que estas

condiciones se han cumplido. Y una vez más, ante una red descentralizada y pública, los problemas de identidad y de localización de las partes contratantes se esbozan como los principales obstáculos a valorar por el juez.

De forma genérica, podríamos decir que tendrán naturaleza contractual, siempre y cuando, cumplan los requisitos previstos en nuestro ordenamiento jurídico, concretamente los dispuestos en el CC. A pesar de no existir una definición completamente delimitada sobre qué es un contrato, sí coexisten disposiciones (artículos 1.089 y 1.091, en relación a los arts. 1.254 y 1.261 CC) de las que se puede delimitar el concepto de contrato como aquel que se perfecciona, tras el acuerdo de voluntades o el consentimiento manifestado y cumpliendo los requisitos esenciales para su validez (*véase* art. 1.278 CC), sin perjuicio de la forma que éste adopte. De conformidad al art. 1.278 CC, en nuestro ordenamiento jurídico, rige el principio de libertad de forma, constituyendo, por tanto, los *smart contract* una posibilidad de exteriorizar la voluntad de las partes.

Por tanto, el consentimiento, a priori, se podría perfeccionar a través de un *smart contract*, tras un procedimiento puramente tecnológico que culminaría, de forma muy generalizada, en un código que será únicamente inteligible por la plataforma que se encargue de ejecutar el contrato (como es el caso de la Máquina Virtual Ethereum, EMV por sus siglas en inglés).

Partiendo de lo anterior, en virtud de un *smart legal contract,* se podrán formalizar distintos negocios jurídicos equiparables a los contratos tradiciones pero con la diferencia de la tecnología aplicada para su formalización y ejecución. Sustentemos esta afirmación con el Informe elaborado por la *Law Comission* de Inglaterra y Gales al Gobierno, según el cual, equipara los contratos tradicionales a los *smart legal contracts* (LAW COMISSION 2021), distinguiendo a su vez, las formas que puede adoptar un contrato legal inteligente y que venimos a recoger en el presente:

- En primer lugar, el contrato legal inteligente, al que denominan como *externo,* en tanto en cuanto el contrato se ha formalizado en un lenguaje natural pero su ejecución se ha encomendado a un código autoejecutable. Este tipo de contrato es el más empleado en la práctica por los escasos problemas jurídicos que podría provocar en su formación e interpretación.

- En segundo lugar, el contrato legal inteligente *híbrido,* por el que únicamente algunas obligaciones específicas del contrato en lenguaje natural se refleja en un código informático.
- En tercer lugar, aquellos en los que sus términos han sido definidos y ejecutados por un código en lenguaje de programación (por ejemplo, Solidity en la plataforma de Ethereum). Estos contratos son los que mayores problemas jurídicos plantean, sobre todo en cuanto a su interpretación por los tribunales.

Mientras que en las dos primeras tipologías manifestadas se aplicarían las reglas de interpretación propias de cualquier otro contrato tradicional, en la última tipología, será determinante conocer las normas de derecho aplicables, el lugar de cumplimiento del contrato, así como los tribunales competentes para resolver un hipotético litigio. Estas cuestiones, en el seno de una red pública en la que se pueden realizar contratos sobre la compraventa de criptomonedas por ejemplo, cobran una especial dificultad y problemática jurídica por el desconocimiento de las partes contratantes.

En este supuesto, en principio, las normas relativas a la ley aplicable sobre los contratos internacionales (como aquellas recogidas en el Reglamento conocido como *Roma I*), no se podrían aplicar. Ante esta incertidumbre, es recomendable que el algoritmo sobre el que se registra el *smart legal contract* recoja, una cláusula expresa sobre la ley y jurisdicción aplicable ante un conflicto; ello, a pesar de que sea *casi imposible* de prever por el inexorable cumplimiento de un contrato legal inteligente cuando se produzca el hecho programado.

De *facto,* el propio contrato inteligente es signo de la confianza depositada entre usuarios, puesto que su carácter determinista, elimina el riesgo de incumplimiento. Por tanto, esta confianza otorgada a la tecnología de la cadena de bloques para satisfacer el cumplimiento de un contrato, es signo de que las partes conocen y comprenden el objeto del mismo. Es evidente, que actualmente, no existe un mecanismo garantista que nos otorgue las herramientas jurídicas necesarias para, en primer lugar, poder identificar a los usuarios contratantes y por otro lado, si en el momento en el que contrataron realmente su consentimiento fue viciado.

No obstante, ante la voluntad de una de las partes de incoar un proceso judicial, como mínimo, el demandante se tendrá que identificar, conociéndose en este momento la identidad de una de las partes. En este momento, será ésta parte quien tenga que probar la naturaleza del conflicto contractual, atendiendo a los criterios sobre la carga probatoria, prevista en el artículo 217 LEC, además, del esfuerzo que de oficio tendrá que realizar el juzgador por no poder aplicar las reglas generales sobre jurisdicción y competencia.

Los contratos inteligentes presumen de una estructura determinista, es decir, bajo órdenes que sigan una estructura *if/then/else.* Ante el acontecimiento en el mundo real de la circunstancia prevista en el contrato (una vez, haya sido verificada por los oráculos), éste se ejecutará bajo unas premisas predeterminadas y en presencia de un incumplimiento, se resolverá con la ejecución de otras órdenes también previamente predefinidas (SÁNCHEZ 2020, p. 289).

En virtud de lo anterior, ¿qué ocurre con las cláusulas que actualmente se incorporan en los contratos y que a futuro, son merecedoras de posibles interpretaciones ante una controversia? De una forma rotunda, no caben en los *smart contracts,* conceptos como fuerza mayor, buena fe, negligencia o el deber de actuar como buen padre de familia previsto en el Código Civil, por ser criterios subjetivos que permiten amplias interpretaciones, tal y como se puede constatar por la dilatada jurisprudencia al efecto. Por tanto, *no todo vale* en las órdenes que las partes incorporan en un contrato inteligente, sino que tendrán que ser perfectamente verificables y objetivas. Tal característica, nos capacita para poder afirmar que los contratos inteligentes no han llegado para sustituir íntegramente a todos los contratos consumados en el mundo real (ni por ende, a los jueces o abogados que lo interpretan), sino que su aplicabilidad resulta ser limitada y en todo caso, alternativa al sistema contractual actual.

5. Retos y oportunidades de la tecnología *blockchain*

No nos cabe ninguna duda de que la Administración de Justicia está orientada a lograr procesos ágiles, dinámicos y eficientes. Cada vez más, encontramos herramientas tecnológicas que permite a cualquier persona física o jurídica recibir notificaciones de la Administración de Justicia, como es el supuesto, del *Servicio de Actos de Comunicación* adscrito al Ministerio de Justicia, al que se accede a través de Cl@veJusticia, como sistema de identificación y firma electrónica no criptográfica a efectos de identificación y firma de los interesados.

La aplicación paulatina de la tecnología *blockchain* en el sector público está favoreciendo un mayor conocimiento entre los ciudadanos y las autoridades públicas, tanto de sus beneficios como de sus costes y riesgos. En este sentido, abordaremos los retos aún pendientes de conseguir y las oportunidades que brinda esta tecnología en la Administración de Justicia. Y, como ambición intrínseca de esta obra, se espera que en unos años exista una normativa cohesionada y unificada que regule esta tecnología en detrimento al contenido actual tan disperso. Este proceso de regulación, aplicación y uso de una red *blockchain* es un proceso complejo, que conllevará estudiar sus oportunidades pero también las barreras tecnológicas, socioeconómicas, legales y culturales que emergen en el sistema de democratización vigente.

La estructura, el funcionamiento y la gobernanza de la Administración de Justicia se tendrán que enfrentar a un conjunto de retos con la finalidad de crear un sistema jurídico seguro y garante de derechos.

RETO 1. Crear un marco jurídico que otorgue seguridad jurídica y confíe en implementar, entre otros, sistemas de comunicación, de notificación o de apoderamientos basados en tecnología *blockchain.* Esta institución es consciente de los cambios tecnológicos que se están produciendo y bajo el marco de la línea estratégica adscrita al Ministerio de Justicia sobre *innovación y mejora del servicio público de justicia*, se están creando grupos de trabajo para lograr una «Justicia 2030: Accesible, Eficiente y Sostenible».

RETO 2. Implementar planes formativos que rompan con la barrera del desconocimiento de esta tecnología, dirigida a los operadores jurídicos, principalmente a los funcionarios al servicio de la Administración de Justicia.

RETO 3. El problema sobre la aceptación social en torno al *blockchain,* provocada por su vinculación errónea y directamente con fines especulativos y de inversión. En relación con este reto, se vincula la necesidad de reestructurar el equipo de personal y de superar la concepción de que los avances tecnológicos han llegado para sustituir a los humanos. Conviene dejar patente que, las personas a pesar de instaurar un sistema de cadena de bloques que faciliten una gestión más rápida, automatizada y eficiente de los procedimientos, no implica un reemplazo indiscriminado de personal.

RETO 5. Costes socioeconómicos: el consumo de energía de los mecanismos de consenso, sobre todo aquellos en base a la prueba de trabajo, es muy elevado (*supra* pág. 11); por ello, adoptar otros mecanismos de consenso en menoscabo al elevado consumo de energía, se constituye como un reto primordial a afrontar por el sistema judicial.

RETO 6. La necesidad de coexistir con la brecha digital**.** Es importante prestar una especial cautela a los colectivos que no tienen acceso o es muy limitado a la tecnología. Implementar en justicia una red *blockchain* acarrea múltiples beneficios, sobre todo de seguridad y agilidad procesal, pero no podemos dejar a un lado el problema de accesibilidad que determinados colectivos vulnerables tienen a su alcance. Los cambios tecnológicos rápidos (en los que se incluye el *blockchain)* debe ser un reto a tener en cuenta en aras de reducir la brecha digital existente y en cumplimiento a los Objetivos de Desarrollo Sostenible (Asamblea General de la ONU).

En contraposición a lo anterior, se destacan las siguientes oportunidades:

OPORTUNIDAD 1. Transparencia sobre las distintas fases procesales. Mediante el uso del *blockchain* en el sistema judicial, las partes a través de sus claves criptográficas pueden conocer el estado actual de su procedimiento judicial. Asimismo, los funcionarios de justicia pueden confiar en la trazabilidad (en relación con la integridad) manifiesta por la cadena de bloques ante un posible conflicto; citando a modo de ejemplo, aquel sobre la presentación o no extemporánea de un escrito de trámite. Además, esta transparencia favorece que la información registrada y a su vez consultada por los usuarios, haya sido actualizada de forma instantánea, no requiriéndose largos tiempos de espera para que la información se actualice, tras ser verificada y notificada por la autoridad competente (por ejemplo, actualmente y en líneas generales, se presenta por Lexnet un escrito de trámite, se recibe por el Juzgado o funcionario judicial y éste procede a notificar a las partes correspondientes). En un nuevo

modelo de justicia, cada operador jurídico tendrá una clave pública (de consulta a un expediente) y privada que le otorgue los permisos específicos acorde a sus funciones, por lo que existiría una presunción de que una vez presentado un escrito, la parte contraria puede ser conocedora del mismo.

Frente a esta transparencia, ¿cómo se podría entender la notificación por esta *red judicial*? Pues bien, entendemos que la fecha de entrada y la firma con la clave privada de un operador jurídico, sería la fecha de recepción y notificación de un escrito. Previamente a esto, debería de existir un compromiso de consulta a diario por parte de los operadores jurídicos que ostente la defensa o representación de una de las partes, pues sino, este sistema no sería operativo y podría ser un medio de incumplimiento de los plazos procesales. Sin embargo, esto se podría subsanar con la aplicación de las previsiones del artículo 162 de la Ley de Enjuiciamiento Civil, acompañado de un sistema de alertas que sea capaz de notificar cualquier cambio en un expediente judicializado.

Por otro lado, la transparencia y la réplica de la información en cada nodo del sistema judicial, garantiza a su vez la integridad de la información mitigando posibles riesgos de pérdidas de datos o de caídas del sistema de justicia (DELGADO 2020, p. 572). Esto último, es un reto que aún sigue ocurriendo, a pesar de los avances tecnológicos que se han desarrollado en los últimos años, Lexnet y los distintos sistemas de gestión procesal de los Juzgados, sufren paralizaciones, imposibilitando el trabajo de los funcionarios y por ende, ralentizando aún más la Justicia.

Desde una perspectiva del orden jurisdiccional penal, la tecnología *blockchain* puede convertirse en un buen uso para la gestión y control de las órdenes judiciales. La transparencia en relación a la trazabilidad de todos los pasos de un proceso, optimizaría los distintos elementos que confluyen en las órdenes judiciales, como pueden ser «la validación de una orden antes de ejecutarla, la necesidad de «empaquetar» una orden con información adicional, y otros elementos como el acceso a la fianza y sus requisitos para la liberación previa al juicio» (BONILLA Y DE CASTRO 2021, p. 10).

OPORTUNIDAD 2. Seguridad. La arquitectura fruto de la tecnología *blockchain* se caracteriza por los sistemas de seguridad sólidos y difíciles de manipular por usuarios externos a la red, pudiendo ser un elemento clave para garantizar una mayor seguridad y protección de los datos en el momento procesal de identificación electrónica o de acceso a

los tribunales para la asistencia en una audiencia telemática. A pesar de que el sistema actual de notificaciones Lexnet, está diseñado con una arquitectura basada en un correo electrónico securizado y mediante la utilización de la firma electrónica reconocida, se deben de superar los sistemas de identificación no criptográficos para lograr una mayor seguridad en los datos compartidos en la red. Alinear el desarrollo de la tecnología *blockchain* en el ámbito judicial y la creación de una identidad digital auto-gestionada, podría suponer un mayor grado de seguridad, confianza y certeza en cuanto a la identificación de los usuarios.

OPORTUNIDAD 3. Eficiencia. A pesar de que aún queda un largo recorrido por desarrollar y conocer esta tecnología, es incuestionable que su aplicación en el sistema procesal conlleva un avance exponencial en la tramitación de expedientes digitales, a los efectos de una mayor agilidad, eficiencia y operatividad. Entre las utilidades prácticas que reportaría esta tecnología, viene a exponer el siguiente caso de uso, trasladable a otros de índole similar: la aplicación del *blockchain* sobre los procesos de ejecución. En este sentido, dictada una sentencia condenatoria que obliga a una de las partes a satisfacer el pago de una cuantía determinada y habiendo transcurrido el plazo para pagar voluntariamente (art. 548 de la LEC), automáticamente el sistema judicial podría ejecutar el contrato inteligente previamente definido. En este sentido, la reforma de la legislación procesal podría ir encaminada a automatizar las medidas de averiguación e investigación del patrimonial, así como a retener de manera automática las cantidades adeudadas a la otra parte una vez tenga conocimiento de los bienes y derechos del ejecutado; ello, sin necesidad de que el ejecutante tenga que presentar demanda ejecutiva, solicitar las medidas de aseguramiento de su patrimonio correspondientes y solicitar que se traben determinados bienes para satisfacer la deuda.

OPORTUNIDAD 4. Interoperabilidad. Este concepto, referido a la «capacidad de compartir información, operar y realizar transacciones fácilmente entre varios sistemas» (CAGIGAS *et al.* 2021*)*. Esta cuestión debe cumplir con los estándares exigidos en el *Esquema Nacional de Interoperabilidad y Seguridad* y además, coexistir con las diferentes competencias que concurren entre las distintas administraciones del sistema judicial español (Consejo General del Poder Judicial, Ministerio de Justicia y de las Comunidades Autónomas, así como la Fiscalía General del Estado).

Conseguir la interoperabilidad entre los distintos organismos, así como con las demás entidades públicas y privadas, tal y como afirmaba ATA (2020) «permitiría utilizar la cadena de bloques por ejemplo, para realizar los apoderamientos y gestionar su registro de forma tal que un solo poder pudiera ser utilizado en el seno de cualquier procedimiento y ante cualquier Administración Pública, siempre que estas sean interoperables, evitando al ciudadano el estar concediendo poderes y autorizaciones a su legal representante para cada gestión ante las distintas Administraciones o en procedimientos judiciales».

A colación con lo anteriormente expuesto y de manera sintética, se exponen las mejoras que a lo largo de este apartado se han puesto de manifiesto.

Tabla 2. Potenciales mejoras de la justicia a través de la tecnología de *blockchain.*

Disminución del riesgo de pérdida o extravío de los datos e información del sistema público de justicia
Mejora de la interconexión y de la interoperabilidad dentro del sistema de justicia y hacia el exterior
Mejora en la gestión de las identidades para el acceso electrónico al sistema judicial o para la participación en audiencias telemáticas
Facilitación del funcionamiento del registro de apoderamientos
Respecto de la prueba, la cadena de bloques representa una forma de acreditar la autenticidad e integridad de un documento

Fuente: Justicia Digital, 2022.

6. Conclusiones

La mayoría de las fuentes contrastadas y revisadas que han sido objeto de la presente investigación, giran sobre un eje central común: la tecnología *blockchain* ha irrumpido en la sociedad, en los procesos y en las relaciones jurídicas con el valor de aportar seguridad, transparencia, eficiencia y nuevas estructuras organizativas ágiles y menos democratizadas. Sin embargo, la base de una nueva transformación digital flaquea por la ausencia de un sistema jurídico que ampare los nuevos riesgos inherentes a esta tecnología, los efectos jurídicos dentro del proceso y los parámetros técnicos para que toda red *blockchain* se considere conforme a Derecho.

Y es por esta razón, por la que los Jueces y Tribunales, junto a los demás operadores jurídicos están comenzando a delimitar la eficacia probatoria de un contrato autoejecutable o de una transacción presentada en un libro-mayor extraído de una red *blockchain.* Pero la tecnología *blockchain* pretende ir mucho más lejos de ser únicamente un nuevo soporte para una prueba digital. Nada obsta para que la Administración de Justicia se sirva de esta tecnología para ofrecer un servicio más eficiente, seguro y de calidad, es decir, para que una red *blockchain* se incorpore a su infraestructura tecnológica. Con el fin de ayudar a construir los cimientos de esta tecnología en el ámbito judicial, se vienen a exponer las siguientes conclusiones:

1. La mayoría de las redes *blockchain* se han diseñado a partir de unas necesidades subsistentes en un sector económico, en una organización o en una entidad pública. Sin embargo, una *red blockchain* aplicada al sistema judicial, tendrá un cometido adicional por su función encomendada por la Constitución Española y como sistema garante del derecho a la tutela judicial efectiva. Por ello, no podemos *hacer ojos ciegos* a los sesgos digitales aún existentes en nuestra sociedad y al factor humano como eslabón fundamental en la cadena de valor. En este sentido, se recomienda que la estructura y el marco de gobernanza diseñado para la Administración de Justicia ampare también, un período de transformación cultural y digital.

2. Las redes *blockchain* nacieron para brindar un libro-registro sobre las transacciones desarrolladas en redes públicas y sin intermediarios. No obstante, las oportunidades

que ofrece esta tecnología no giran únicamente sobre la descentralización o sobre las formas de acceso a la información, sino que a través de su sistema de encriptación o por el diseño de algoritmos sofisticados, son capaces de garantizar una mayor seguridad sobre la información registrada, otorgándole por ende, una mayor integridad y autenticidad a los hechos registrados. La evolución de esta tecnología incorpora la posibilidad de implementación en el sistema judicial, creando una red distribuida, híbrida o federada y permisionada. La copia de todas las resoluciones o cualquier otra transacción circunscrita en el seno de un proceso o procedimiento judicial, no quedaría únicamente ubicada en una aplicación informática sino que se distribuiría en cada nodo que forme la cadena de bloques, favoreciendo así las consultas y acceso instantáneo a las resoluciones judiciales dictadas por los diferentes órganos tanto nacionales como internacionales, favoreciendo la interoperabilidad entre los mismos.

3. Los usuarios encargados de validar cada transacción incorporada a la cadena de bloques, serán los validadores, es decir, aquellos funcionarios judiciales autorizados a ejercer determinadas funciones judiciales (de registro, de notificación, de impulso, de ordenación de proceso, entre otras). El mecanismo de consenso basado en la prueba de autoridad quedará delimitada y restringida según el cargo y funciones encomendadas.

4. Es evidente que los riesgos de la tecnología *blockchain*, al igual que ocurre con los demás desarrollos tecnológicos, no se pueden eliminar pero sí mitigar. La protección de los datos personales y el derecho a la intimidad, pueden colisionar con una red híbrida en tanto en cuanto, las resoluciones judiciales podrían estar disponibles para cualquier ciudadano. A pesar de ello, esta tecnología utiliza un sistema de código cifrado *hash,* que considerado hasta día de hoy, como una técnica de seudonimización, debería de evolucionar para que sea plenamente aceptado por la autoridad de protección de datos, como un código anónimo. Puntualizar, que en el marco de las relaciones internas entre los órganos judiciales, el contenido de una resolución judicial se podría consultar a través del uso de su clave privada; por el contrario, el usuario ajeno a un procedimiento judicial, podría consultarla

(garantizándose previamente que los datos personales estén anonimizados) mediante la clave pública.

5. La inmutabilidad (no pudiendo ser eliminada una transacción sin dejar rastro) y la colisión con la protección de los datos personales y los derecho de rectificación y supresión, se puede mitigar a través del consenso de prueba de autoridad (o mediante la entidad verificada determinada a tales efectos) estableciendo mecanismos transparentes y estrictamente delimitados para cumplir con los objetivos interpuestos por la normativa de protección de datos. Esta inmutabilidad referida al ámbito de la Administración de Justicia será distinta a cuando nos encontremos ante un *smart legal contract* y se desee la modificabilidad de algunas de las cláusulas. En este caso, habrá que recabar el consenso de todos los participantes, por lo que el modo de operar será diferente según el tipo de red donde esté almacenado el contrato inteligente.

6. En relación con lo anterior, según la normativa procesal vigente, un libro-registro obtenido de una *blockchain* puede ser un medio de prueba, a pesar de que la fuerza probatoria la determinará el juez según las reglas de la *sana crítica*, al igual que ocurre con el resto de pruebas digitales. La prueba digital sobre el *hash* derivado de una transacción jurídica-privada, podrá ser aportada como documento privado a un procedimiento, siempre y cuando las partes contratantes estén identificadas y se aporte un informe pericial que verifique el contenido de la transacción, así como la traducción del código a lenguaje natural.

7. La tecnología *blockchain* motivaría a alcanzar una mayor eficiencia en la tramitación de los asuntos judiciales, mediante la implementación de contratos autoejecutables que permitan una ejecución automática de tareas rutinarias, objetivas y delimitadas; consiguiendo que la información almacenada en un órgano judicial o en otra entidad pública o privada se pueda hacer valer frente otro órgano sin necesidad de reiterar el trámite necesario, por ejemplo, para acreditar la representación procesal; y finalmente, garantizando la seguridad en la tramitación de expediente electrónico mediante el sistema de encriptación asimétrica.

7. Futuras líneas de investigación

- Analizar la estructura de seguridad en entornos donde predomina la compartición y almacenamiento de datos especialmente vulnerables.
- Resolver los problemas de escalabilidad de las transacciones a fin de garantizar que la interoperabilidad entre la Administración de Justicia y las distintas entidades públicas y privadas, nacionales e internacionales, sea plenamente predicable.
- Abordar las barreras técnicas aún pendientes de resolver con la intención de crear un marco normativo con afán de continuidad en el tiempo.

Referencias bibliográficas

Bibliografía básica

AEPD. «Tecnologías y Protección de Datos en las AA.PP» [en línea]. 2020 [consulta: diciembre 2022]. Disponible en: https://www.aepd.es/es/documento/guia-tecnologias-admin-digital.pdf

ALLENDE LÓPEZ, M. «Identidad Digital Auto-Gestionada. El futuro de la identidad digital: auto-gestión, billeteras digitales y blockchain» [en línea]. 2º Ed. 2020 [consulta: diciembre 2022]. Disponible en: https://publications.iadb.org/es/identidad-digital-auto-gestionada-el-futuro-de-la-identidad-digital-auto-gestion-billeteras

ANGUIANO, J.M. «Smart Contracts: Introducción al contractware». Diario La Ley, núm 25, Sección Ciberderecho, *Wolters Kluwer*, 2019 [consulta: octubre de 2022].

ATA, F. Y GONZÁLEZ PULIDO, I. *FODERTICS 8.0: estudios sobre tecnologías disruptivas y justicia*. Granada: Editorial Comares., 2020

BARRIO ANDRÉS, M. *Criptoactivos. Retos y desafíos normativos*. 1º Ed.: Wolters Kluwer España, S.A, febrero 2021.

BAUTISTA PÉREZ, F. «Tecnología blockchain y criptomonedas: luces y sombras», LA LEY mercantil, Nº 88, *Wolters Kluwer*, 2022 [consulta: octubre de 2022].

«Blockchain Strategy». European Comission [consulta: diciembre 2022]. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy

BONILLA GAVILANES, J.M. Y DE CASTRO GARCÍA, P.M. «Cómo la innovación y la tecnología disruptiva pueden ayudar a mejorar la Administración de Justicia». Práctica de Tribunales, Nº 149, Sección Estudios, Marzo-Abril 2021, *Wolters Kluwer*, 2021 [consulta: diciembre de 2022].

CABRERA CUEVAS, M.J. [et al.]. «Justicia Digital. Guía para el diálogo sobre el diseño y uso eficiente, de calidad y ético de herramientas tecnológicas en la justicia civil». *Cotec*. [en línea]. 2022, pp. 1-109 [consulta: noviembre 2022] ISBN: 978-84-92933-56-3. Disponible en:

https://cotec.es/proyecto/guia-para-la-justicia-digital/182601b7-86e5-af12-eca0-00de51e7a833

CAGIGAS, D. [et al.]. «Blockchain for Public Services: A Systematic Literature Review». *IEEE Access.* [en línea]. 2021, vol. 9, pp. 13904 - 13921 [consulta: noviembre 2022]. ISSN 2169-3536. Disponible en:

https://ieeexplore.ieee.org/abstract/document/9326290

CASTELLÓ PASTOR, J.C. *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales.* 1º Ed. Navarra: Aranzadi, 2021.

DE LA MATA MUÑOZ, A., «Fundamentos de Blockchain». *Blockchain Intelligence* [en línea]. 2020, [consulta: octubre de 2022]. Disponible en: https://blockchainintelligence.es/recursos/

DELGADO MARTÍN, J. *Judicial-Tech, el proceso digital y la transformación tecnológica de la justicia. Obtención, tratamiento y protección de datos en la justicia*. 1º Ed. Madrid: Wolters Kluwer, 2020.

«EBSI Verifiable Credentials». EBSI European Blockchain [consulta: diciembre 2022]. Disponible en:

https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/EBSI+Verifiable+Credentials

ESPUGA TORNÉ, G. «Compatibilidad y encaje legal de la tecnología blockchain con la normativa sobre protección de datos personales» LA LEY mercantil, Nº 84, Sección Derecho digital*, Wolters Kluwer*, 2021 [consulta: diciembre de 2022].

FELUI REY, J. «Smart Contract: Concepto, ecosistema y principales cuestiones de Derecho privado». LA LEY mercantil, Nº 47, Sección Contratación mercantil, comercio electrónico y TICs, *Wolters Kluwer*, 2018 [consulta: octubre de 2022].

FUENTES SORIANO, O. *Tecnología y proceso. Problemas procesales en un mundo digital*. 1ª ed. Editorial Aranzadi, 2022

GARCÍA-VALDECASAS RODRÍGUEZ DE RIVERA, P. *Blockchain y automatización de procedimientos en la Administración Pública*. 1º Ed. Madrid: Wolters Kluwer, Marzo 2022.

GONZÁLEZ GRANDA, P. Y ARIZA COLMENAREJO, Mª.J. *Justicia y proceso: una revisión procesal contemporánea bajo el prisma constitucional.* Madrid: Dykinson, 2021.

MERCHÁN ARRIBAS, M. Y MARTÍN BAUTISTA, A.L. «The European Blockchain Service Infrastructure (EBSI) y el desarrollo de blockchain en el marco institucional europeo. Casos de uso» [en línea]. 2020, [consulta: diciembre de 2022]. Disponible en: https://blockchainintelligence.es/recursos/

NAKAMOTO, SATOSHI. Peer-to-peer Electronic Cash Systems. 2008. Disponible en: https://bitcoin.org/bitcoin.pdf

NESPRAL D., FERNANDEZ HERGUETA. R y BELTRÁN M. (coord.) *Blockchain. El modelo descentralizado hacia la economía digital.* Ra-Ma Editorial, 2021.

OBSERVATORY AND FORUM. UE. «Smart Contract». [en línea]. 2022 [consulta: diciembre 2022]. Disponible en: https://www.eublockchainforum.eu/reports

PEREA GONZÁLEZ, Á. «Blockchain y proceso civil: más allá de la jurisdicción y la fe pública judicial», Actualidad Civil, Nº 6, Sección Derecho Digital, *Wolters Kluwer*, 2020 [consulta: diciembre de 2022].

Protocolo de Protección del Secreto Empresarial en los Juzgados Mercantiles, Tribunal Mercantil de Barcelona. 2019 [consulta: diciembre 2022]. Disponible en: https://www.icab.es/export/sites/icab/.galleries/documents-noticies/2019/protocolo-de-proteccion-del-secreto-empresarial-en-los-juzgados-mercantiles.pdf

«¿Qué son los datos personales?». Comisión Europea [consulta: diciembre 2022]. Disponible en: https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_es

RÍOS LÓPEZ, Y. «Blockchain, Smart Contracts y Administración de Justicia». *Blockchain Intelligence* [en línea]. 2021, [consulta: noviembre de 2022]. Disponible en: https://blockchainintelligence.es/recursos/

RIOS, Y. «Webinar. Blockchain y Administración de Justicia». *Blockchain Intelligence*. 2020. [consulta: diciembre 2022]. Disponible en: https://blockchainintelligence.es/sesion-abierta-blockchainen-la-administracion-de-justicia/

SÁNCHEZ RUIZ DE VALDIVIA, *I. Blockchain: impacto en los sistemas financiero, notarial, registral y judicial.* 1º ed, Editorial Aranzadi, 2020.

SIRUS MASHOUF, M. «Blockchain: contratación y jurisdicción*». Revista Aranzadi de Derecho y Nuevas Tecnologías*. 2022, núm. 60.

«Success stories». EBSI European Blockchain [consulta: diciembre 2022]. Disponible en: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Verifiable+Credentials+Success+Stories

«The EU Project 'eSSIF-Lab'». eSSIF-Lab [consulta: diciembre 2022]. Disponible en: https://essif-lab.github.io/framework/docs/essifLab-project

VALPUESTA GASTAMINZA, E. Y HERNANDEZ PEÑA.J.C. *Blockchain: aspectos jurídicos de su utilización.* 1º Ed. Madrid: Wolters Kluwer, Mayo 2022.

«What is EBSI?». EBSI European Blockchain [consulta: diciembre 2022]. Disponible en: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi

Bibliografía complementaria

«EBSI Architecture, explained». CEF Digital Connecting Europe. 6 de octubre de 2021, [consulta: diciembre 2022]. Disponible en:

file:///C:/Users/Usuario/Downloads/(210610)(EBSI_Architecture_Explained)(v1.02)%20(1).pdf

ESTELLER, R. «La UE limitará el consumo de energía de las criptomonedas en caso de crisis». El Economista. 24 de octubre de 2022, [consulta: diciembre 2022]. Disponible en: https://www.eleconomista.es/energia/noticias/12003991/10/22/La-UE-limitara-el-consumo-de-energia-de-las-criptomonedas-en-caso-de-crisis.html

«Estrategia Europea de Blockchain-Folleto», European Commission. 14 de enero de 2021. Disponible en: https://digital-strategy.ec.europa.eu/en/library/european-blockchain-strategy-brochure#accept

«Identidad digital europea: el Consejo avanza hacia la cartera europea digital de la UE, un cambio de paradigma para la identidad digital en Europa». Consejo de la Unión Europea. 6 de diciembre de 2022, 11:15. Disponible en:

https://www.consilium.europa.eu/es/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/

NEUMUELLER, A. «A deep dive into Bitcoin's environmental impact». *Cambridge Judge Business School.* 2022. Disponible en: https://www.jbs.cam.ac.uk/insight/2022/a-deep-dive-into-bitcoins-environmental-impact/

«Mining the environment – is climate risk priced into crypto-assets?». European Central Bank. 2022. Disponible en:

https://www.ecb.europa.eu/pub/financial-stability/macroprudential-bulletin/html/ecb.mpbu202207_3~d9614ea8e6.en.html#toc5

«Punto Neutro Judicial», Poder Judicial España [consulta: diciembre 2022]. Disponible en:

https://www.poderjudicial.es/cgpj/es/Temas/e-Justicia/Servicios-informaticos/Punto-Neutro-Judicial/#:~:text=El%20Punto%20Neutro%20Judicial%20es,con%20objeto%20de%20facilitar%20y

«Smart Legal Contracts. Advice to Government», Law Comission. 2021. Disponible en: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf

TAN E., MAHULA, S., CROMPVOETS, «J. Blockchain governance in the public sector: A conceptual framework for public management». *Elsevier* [en línea]. 2021, vol. 39 [consulta: noviembre 2022]. DOI 101625. Disponible en: https://doi.org/10.1016/j.giq.2021.101625

NASIR MUMTAZ BHUTTA, M. [et al.]. «A Survey on Blockchain Technology: Evolution, Architecture and Security». *IEEE Access*. [en línea]. 2021, vol. 9, pp. 61048 - 61073 [consulta: noviembre 2022]. ISSN 2169-3536. Disponible en:

https://ieeexplore.ieee.org/document/9402747

Legislación citada

Carta de los Derechos Fundamentales de La Unión Europea. *Diario Oficinal de la Unión Europea*, (2016/C 202/02), de 7 de junio de 2016. Disponible en: https://eur-lex.europa.eu/eli/treaty/char_2016/oj

Constitución Española. *Boletín Oficial del Estado*, núm. 311, de 29 de diciembre de 1978, páginas 29313 a 29424. Disponible en: https://www.boe.es/buscar/pdf/1978/BOE-A-1978-31229-consolidado.pdf

Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. *Boletín Oficial del Estado*, núm. 7, de 8 de enero de 2000, páginas 575 a 728. Disponible en: https://www.boe.es/buscar/pdf/2000/BOE-A-2000-323-consolidado.pdf

Ley 18/2011, de de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia. *Boletín Oficial del Estado*, núm. 160, de 6 de julio de 2011, páginas 71320 a 71348. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2011-11605

Ley 3/2020, de 18 de septiembre, de medidas procesales y organizativas para hacer frente al COVID-19 en el ámbito de la Administración de Justicia. *Boletín Oficial del Estado*, núm. 250, de 19 de septiembre de 2020, páginas 79102 a 79126. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2020-10923

Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, *Boletín Oficial del Estado,* núm. 298, de 12 de noviembre de 2020, páginas 98821 a 98841. Disponible en: https://www.boe.es/eli/es/l/2020/11/11/6/con

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, *Boletín Oficial del Estado,* núm. 166, de 12 de julio de 2002, páginas 25388 a 25403. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, núm. 294, de 06 de diciembre de 2018, páginas 119788 a 119857. Disponible en: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

Ley Orgánica 7/2015, de 21 de julio, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. *Boletín Oficial del Estado*, núm. 174, de 22 de julio de 2015, páginas 61593 a 61660. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-8167

Proyecto de Ley de medidas de eficiencia procesal del servicio público de Justicia. *Boletín Oficial de las Cortes Generales*, núm. 97-1, de 22 de abril de 2022, páginas 131. Disponible en: https://www.congreso.es/public_oficiales/L14/CONG/BOCG/A/BOCG-14-A-97-1.PDF

Proyecto de Ley Orgánica de eficiencia organizativa del servicio público de Justicia, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, para la implantación

de los Tribunales de Instancia y las Oficinas de Justicia en los municipios. *Boletín Oficial de las Cortes Generales,* núm. 98-1, de 22 de abril de 2022, páginas 56. Disponible en: https://www.congreso.es/public_oficiales/L14/CONG/BOCG/A/BOCG-14-A-98-1.PDF

Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET. *Boletín Oficial del Estado*, núm. 287, de 1 de diciembre de 2015, páginas 113314 a 113331. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-12999

Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. *Gaceta de Madrid*, núm. 206, de 25 de julio de 1889, páginas 249 a 259. Disponible en:

https://www.boe.es/buscar/pdf/1889/BOE-A-1889-4763-consolidado.pdf

Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. *Boletín Oficial del Estado,* núm. 266, de 5 de noviembre de 2019, páginas 121755 a 121774. Disponible en:

https://www.boe.es/buscar/act.php?id=BOE-A-2019-15790

Reglamento

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Diario Oficial de las Comunidades Europeas, 4 de mayo de 2016, núm. 119. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

Reglamento (UE) 2022/858 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado y por el que se modifican los Reglamentos (UE) nº 600/2014 y (UE) nº 909/2014 y la Directiva 2014/65/UE. Diario Oficial de las Comunidades Europeas, 2 de junio de 2022, número 151. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022R0858

Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. Diario Oficial de las Comunidades Europeas, 28 de agosto de 2014, número 257. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32014R0910

Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO por el que se modifica el Reglamento (UE) n. º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea. Diario Oficial de las Comunidades Europeas, 3 de junio de 2021, número 281. Disponible en:

https://eur-lex.europa.eu/resource.html?uri=cellar:5d88943a-c458-11eb-a925-01aa75ed71a1.0018.02/DOC_1&format=PDF

Declaración

Declaración Europea sobre los Derechos y Principios Digitales. Proclamada por el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea, de 15 diciembre 2022. Disponible en: https://digital-strategy.ec.europa.eu/es/library/european-declaration-digital-rights-and-principles

Comunicación

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. La digitalización de la justicia en la UE un abanico de oportunidades (COM/2020/710 final). *Diario Oficial de la Unión Europea,* 2 de diciembre de 2020.

Disponible en: *https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0710*

Dictamen

Dictamen del Comité Económico y Social Europeo sobre «La tecnología de cadena de bloques y de registros distribuidos: una infraestructura ideal para la economía social». *Diario Oficial de la Unión Europea,* núm. 353, 18 de octubre de 2019, Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52019IE0522&from=ES

Jurisprudencia referenciada

Sentencia del Tribunal Constitucional 125/2022, de 10 de octubre de 2022. Recurso de amparo 8133-2021. ECLI:ES:TC:2022:125.

Sentencia del Tribunal Supremo 706/2020, de 23 de julio de 2020. Recurso de casación. ECLI: ES:TS:2020:2925. Fundamento de Derecho Nº 4.

Sentencia de la Audiencia Provincial de Álava 1032/2021, de 21 de diciembre 2021, Recurso de apelación 1395/2021. ECLI:ES:APVI:2021:1302. Fundamento Jurídico Nº 2.

Listado de abreviaturas[6]

Art/Arts.	Artículo/Artículos
AEPD	Agencia Española de Protección de Datos
CC	Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil
CE	Constitución Española
CE	Comisión Europea
CESCE	Comité Económico y Social Europeo
CGPJ	Consejo General del Poder Judicial
CTEAJE	Comité Técnico Estatal de la Administración Judicial Electrónica
DEH	Dirección Electrónica Habilitada
DID	Decentralized Identifier (Identidad Descentralizada)
DLT	Distributed Ledger Technology (Tecnología de Registro Distribuido)
EBP	European Blockchain Partnership (Asociación Europea de *Blockchain)*
EBSI	Infraestructura Europea de Servicios de *Blockchain*
EEB	Estrategia Europea de *Blockchain*
EEE	Espacio Económico Europeo
eIDAS	Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

[6]Los términos anglosajones han sido de traducidos al español a criterio propio.

eSSIF-Lab	European Self-Sovereign Identity Framework Laboratory (Identidad Europea Auto-gestionada)
INATBA	International Association for Trusted Blockchain Applications (Asociación Internacional para Aplicaciones *blockchain* de confianza)
LEC	Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
LOPJ	Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial
ONU	Organización de las Naciones Unidas
PLMEPSPJ	Proyecto de Ley de medidas de eficiencia procesal del servicio público de Justicia
PLOEOSPJ	Proyecto de Ley Orgánica de eficiencia organizativa del servicio público de Justicia
PoA	Proof of Authority (Prueba de Autoridad)
PoS	Proof of Stake (Prueba de Participación)
PoW	Proof of Work (Prueba de Trabajo)
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
SSI	Self-Sovereign Identity (Identidad Auto-soberana o Auto-gestionada)
UE	Unión Europea