universidad de león

FACULTAD DE DERECHO
UNIVERSIDAD DE LEÓN
CURSO 2019/2020

DERECHOS FUNDAMENTALES Y TECNOLOGÍA BLOCKCHAIN (FUNDAMENTAL RIGHTS AND BLOCKCHAIN TECHNOLOGY)

MÁSTER EN DERECHO DE LA CIBERSEGURIDAD Y ENTORNO DIGITAL

AUTOR: EDUARDO DE CELIS GUTIÉRREZ

TUTOR: DR. D MIGUEL ÁNGEL ALEGRE MARTÍNEZ

SEGUNDO TUTOR (ASPECTOS TÉCNICOS): D. PEDRO PÉREZ GRANDE

ÍNDICE

RESUMEN

Con la aparición de la tecnología Blockchain y sus bases criptográficas en materia de ciberseguridad, ha surgido conflicto en la tutela de los Derechos Fundamentales de los individuos que utilizan esta tecnología.

Los tradicionales Derechos Fundamentales van a verse limitados, modificados o menoscabados respecto a las Garantías previstas por el Ordenamiento Jurídico creando unos nuevos digitales y propios de cada plataforma Blockchain.

En este punto, parece que el nuevo marco regulatorio de Protección de Datos Europeo ha llegado tarde a la hora de acoger una tecnología que ofrece nuevas soluciones en materia de privacidad, transparencia y seguridad desde el punto de vista científico, y que adaptándose a las necesidades concretas de los usuarios sin necesidad de recurrir a una Autoridad Central. Centralización versus Descentralización.

Este nuevo paradigma nos lleva a preguntarnos si la protección de los Derechos Fundamentales por parte de la tecnología Blockchain tiene cabida dentro del Derecho convencional o si este ecosistema criptográfico alternativo únicamente protege sus propios Derechos a través del Código, su Lex Criptographica.

PALABRAS CLAVE: Blockchain, Derechos Fundamentales, Intimidad, Privacidad, Datos Personales, Protección de Datos, Registros Descentralizados, Criptoderecho, Ley Informática, Tecnología Disruptiva, Derechos ARCO-POL, Ciberseguridad.

ABSTRACT

The cryptographic-based Blockchain Technology and its cybersecurity measures have implied a confrontation with the Fundamental Right defense by private users.

The traditional protection of the Fundamental Rights can be limited, modified, or altered by this new crypto technology by the creation of new Digital Fundamental Rights within a Blockchain platform.

At this point, the new GDPR Regulation in the European Union arrives late to embrace a disrupted technology that offers new measures in terms of privacy, transparency, and security from a scientific point of view, besides an adaptative regulation without a Central Authority.

This new paradigm is questioning whether Blockchain Technology protects analogic Fundamental Rights outside its ecosystem or just create a new set of Digital Rights ruled by the Code, its Lex Cryptographica.

KEYWORDS: Blockchain, Fundamental Rights, Intimacy, Privacy, Personal Data, Data Protection, Distributed Registers, Crypto Law, Lex Informatica, Disrupted Technology, Data Protection Rights, Cybersecurity.

ABREVIATURAS

API	Interfaz de programación de aplicaciones
ARCO	Derechos De Acceso Rectificación Cancelación y Oposición
C.E	Constitución Española
DLT(s)	Tecnologías de Registro Distrbuido
RGPD/GDPR	Reglamento (UE) 2016/679, General de de Protección de Datos
DAPPs	Aplicaciones Descentralizadas basadas en Blockchain
LEC	Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil
LOPJ	Ley Orgánica 6/1985, de 6 de Junio, del Poder Judicial
LECRIM	Ley de Enjuiciamiento Criminal
LOPDGDD	Ley Orgánica de Protección de Datos Personales y Garantías de Derechos Digitales
OCDE	Organización para la Cooperación y el Desarrollo Económicos
Pág	Página
PoA	Proof of Asset (Prueba de activo)
PoS	Proof of Stake (Prueba de participación)
PoW	Proof of Work (prueba de trabajo)
P2P	Peer to Peer
P4P	Proactive network Provider Participation for P2P (Participación activa del proveedor de red en P2P)
TCP/IP	Transfer Control Protocol/ Internet Protocol
TEDH	Tribunal Europeo de Derechos Humanos
TJUE	Tribunal de Justicia de la Unión Europea
TOR	The Onion Router (protocolo de Deep Web)
STJUE	Sentencia Tribunal de Justicia de la Unión Europea

SOPA	Stop Online Piracy Act
ISPs	Proveedores de Servicios de Internet

OBJETO

La creciente preocupación por el auge de la tecnología Blockchain ha sido advertida por la mayoría de los países occidentales que han visto crecer a su sobra una plataforma en la que el Código, el consenso entre las partes y el carácter distribuido ha alcanzado un gran impacto en el Estado de Derecho.

El objetivo principal de este estudio va a ser el análisis de los aspectos técnicos de la cadena de bloques que van a poder reforzar el desarrollo de los derechos fundamentales de los ciudadanos sin que eso suponga un menoscabo de los mismos.

En la actualidad, y tras la aprobación del Reglamento General de Protección de Datos en 2016 por parte del Parlamento Europeo, nos encontramos ante una regulación centralizada y protectora del individuo en la que se traslada la responsabilidad de tratamiento de los datos de carácter personal en diversos agentes que manejan el activo más valioso de la actualidad: la Información.

El estudio de los fundamentos de la tecnología Blockchain va a llevarnos por los principios técnicos que posibilitan el respeto de los Derechos fundamentales pero que como veremos, va a suponer en muchas ocasiones, un riesgo excesivo para los usuarios que no tengan suficientes conocimientos tecnológicos para una correcta utilización de esta tecnología.

Las buenas prácticas por parte de los usuarios va a ser otra de las materias que se van a analizar en este trabajo, puesto que la Tecnología Blockchain ofrece múltiples posibilidades y configuraciones pero que deben contar con una serie de cautelas para que la seguridad sea efectiva.

Uno de los ejes centrales en el estudio va a ser el papel del Código como una verdadera regulación, la llamada Ley Informática, o como veremos, la Ley Criptográfica, que actúa como una verdadera fuerza vinculante en las transacciones entre usuarios al configurarse desde su diseño como un entorno seguro en el que las partes saben que, si se cumplen una serie de condiciones preprogramadas, la transacción se llevará a cabo con plenas garantías.

No va a ser objeto de estudio de este trabajo aquellas iniciativas en las que se pretende llamar Blockchain a proyectos que no respetan sus principios esenciales, es decir, las mal llamadas “Blockchains editables” en las que un tercero puede modificar el contenido de un bloque que ha sido verificado e integrado por parte de los nodos.

Es esencial apreciar el carácter utópico e innovador de una tecnología que pretende revolucionar el marco legal actual desde un ecosistema basado en las matemáticas, en la criptografía en la que se desconfía de los intermediarios y se otorga un carácter prevalente al individuo.

Finalmente vamos a centrarnos en el futuro de la cadena de Bloques dentro de la Regulación actual y los proyectos que pretenden acercar esta tecnología a las Instituciones.

DESCRIPCIÓN DE LA METODOLOGÍA

Dentro de las múltiples materias cursadas a lo largo del Máster Universitario en Derecho de la Ciberseguridad hubo una que despertó mi inquietud porque aunaba características técnicas e implicaciones desde el punto de vista del Derecho de la Ciberseguridad que prácticamente abordaba la totalidad de campos. Hablamos de Blockchain.

A lo largo de la elaboración de este trabajo me he encontrado con diversos problemas extraños al propio funcionamiento de la Universidad debido al Estado de Alarma por la Emergencia Sanitaria de la Pandemia Covid-19 que cortó las clases presenciales por un lado y por otra y más importante en mi caso, la asignatura de Prácticas Externas donde iba a participar en el día a día del Departamento de Blockchain de un Hub tecnológico en Madrid.

Tuve claro desde un primer momento que mi trabajo no se iba a centrar en la fiscalidad de las criptomonedas ni en los efectos jurídicos dentro del ámbito privado de los contratos inteligentes o Smart Contracts. Obviamente, forman una pequeña parte de mi exposición, sobre todo en el caso de los últimos por albergar muchos elementos que van a poner en peligro los Derechos Fundamentales de las Personas.

Mi trabajo lo he estructurado básicamente en dos partes muy diferenciadas. La primera la he dedicado a una contextualización técnica que, sin pretender ser exhaustiva ha tocado todos los puntos necesarios para acercarnos a la parte más desconocida para un jurista.

Quiero resaltar que para la realización de este trabajo me he apoyado no solo en mi Tutor principal, el Dr. Alegre Martínez a la hora de estructurar el contenido del trabajo sino también en mi otro tutor y gurú de la tecnología Blockchain, el ingeniero Pedro Pérez Grande.

Quiero destacar el peso dentro de este trabajo de las fuentes expuestas e información contenida en el manual dirigido por Pablo García Mexía "Criptoderecho. La Regulación de Blockchain", una auténtica Biblia en castellano muy actuaizada, que me ha descubierto muchos autores, fuentes y corrientes en el estudio legal de la Blockchain. Se puede decir, que este manual es una pequeña navaja suiza en tanto me ha abierto los ojos en ciertos aspectos jurídicos que al principio de mi estudio sobre Blockchain no conocía.

Igualmente, los distintos "papers" y trabajos de investigación llevados a cabo por parte del Observatorio y Foro de Blockchain de la Unión Europea, de la más reciente actualidad me han animado a leer e investigar sobre la materia. Es inspirador ver cómo esta tecnología está llamando a las puertas del Parlamento Europeo y que la Comisión está constantemente formando grupos de trabajo que permitan un acercamiento entre la Regulación y protección de los ciudadanos europeos a la par que se mantiene en contacto con los investigadores.

Del mismo modo, y debido a la constante evolución y a la bisoñez de la tecnología Blockchain he utilizado muchos recursos de revistas jurídicas online tanto españolas como extranjeras (fundamentalmente estadounidenses y británicas) en las que he descubierto que grandes profesores de importantes universidades se habían planteado

desde hace pocos meses los graves conflictos que plantea la Tecnología Blockchain y el Derecho Criptográfico respecto al ejercicio y tutela de los Derechos Fundamentales. Y finalmente y debido a la constante evolución de esta materia he utilizado y consultado muchos recursos alojados en Internet como webs especializadas en Blockchain, videos de Youtube, asistencia a Webinars en la materia, ….

La segunda parte del trabajo se ha centrado por tanto en las implicaciones jurídicas de la tecnología Blockchain ha supuesto en el ejercicio de los derechos fundamentales. En este punto he decidido centrarme en el Derecho Fundamental de la Intimidad y de la Privacidad puesto que la piedra angular desde la que parte la tecnología Blockchain y desde otro punto la actual normativa europea en materia de protección de los datos de carácter personal.

El hecho de no haber podido aprender en el ejercicio de la Asignatura de prácticas más sobre esta tecnología y haber podido trabajar más codo con codo con ingenieros informáticos conocedores de la materia ha supuesto un giro al estudio más puramente jurídico de la materia.

Una de mis fuentes para la obtención de recursos y fuentes ha sido la Biblioteca Online de la Universidad, así como las plataformas puestas de manera libre por parte de disposición de universidades extranjeras, de las que he podido extraer un gran material para la elaboración de mi contenido.

He querido centrar mi estudio en las plataformas Blockchain en sentido estricto sin querer analizar los modelos híbridos que algunos entusiastas se están empeñando en denominar cadenas de bloques, cuando no cumplen los requisitos de inmutabilidad y transparencia necesarios para cumplir con los estándares de esta tecnología.

Sin lugar a duda, el despegue de esta tecnología abrirá el camino a múltiples estudios que desarrollen sus implicaciones en los derechos y libertades de los individuos en su relación con la Criptografía y la Protección de la Privacidad.

PARTE CENTRAL DEL TRABAJO

1. INTRODUCCIÓN

El nacimiento de los nuevos Derechos Fundamentales digitales derivados del derecho fundamental analógico de la intimidad personal y familiar del art. 18.1 CE, en relación con el derecho fundamental autónomo de protección de datos y la especial protección al uso de la informática del art. 18.4 CE, tras la entrada en vigor del Reglamento (UE) 2016/679 de Protección de Datos, y la transposición *sui generis* española en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de Derechos Digitales en su título X, supone un reto para los juristas a la hora de integrar y aproximar dentro del ordenamiento jurídico las bondades de una nueva tecnología surgida a mediados de la década de los 2000 por el misterioso Satoshi Nakamoto: la tecnología *Blockchain* o *Cadena de Bloques* que se define como un registro descentralizado de datos en el que no existe una autoridad verificadora de la información y autoría de la misma.

La clave de este trabajo será, por tanto, buscar los elementos que acercan a esta tecnología criptográfica, matemática y disruptiva al respeto de los distintos derechos fundamentales amparados tanto por la Constitución Española como en el marco europeo.

El eje central de este estudio jurídico va a ser el concepto del DATO PERSONAL, puesto que en la utilización de la tecnología Blockchain van a introducirse en las cadenas de bloque ficheros que podrían ser considerados como datos personales, y que, por ende, deberían respetar los principios fundamentales establecidos por el Reglamento General de Protección de Datos.

La Tecnología Blockchain y el Reglamento General de Protección de Datos parten de polos separados en el tiempo en cuanto a su nacimiento, pero condenados a encontrarse en la búsqueda del mismo objetivo: el respeto al anonimato de los usuarios, o en caso del RGPD a la protección de la intimidad personal.

El desarrollo de la tecnología Blockchain tiene un gran impacto en los diferentes campos jurídico-económicos actuales, como son las criptomonedas, los contratos inteligentes o *Smart Contracts*, su aplicabilidad en el mundo de la fe pública registral y notarial, así como en el seno de la Administración de Justicia, por cuanto se trata de una tecnología fiable, basada en la verificación de distintos nodos o partes y con un grado de seguridad muy alto a la hora de proteger su contenido.

Estas bondades provenientes de la tecnología distribuida van a chocar de una manera muy directa con los pilares de los derechos fundamentales digitales integrados en el Derecho de Protección de Datos, llamados derechos ARCO-POL, sobre todo en lo referente a los derechos de cancelación, oposición, portabilidad y al derecho al olvido.

2. CONTEXTUALIZACIÓN. ASPECTOS TÉCNICOS

2.1. TECNOLOGÍA BLOCKCHAIN: "BLOCK-CHANGE"

El anhelo humano del CAMBIO, de la vanguardia tecnológica, así como su utilización para reordenar las relaciones humanas, ha sido una constante desde que el ser humano se organiza en sociedad tal y como recoge el adagio latino "*ubi ius, ibi societas*".

En este sentido la tecnología Blockchain va a introducir un nuevo escenario, tanto en la esfera privada como en la pública, a la hora de relacionarnos con los poderes públicos.

La OCDE y la Unión Europea de una manera contundente han admitido que la Tecnología Blockchain y las Tecnologías de Registro Distribuido (DLTs) constituyen hoy la tecnología digital de mayor potencial disruptivo para la Humanidad.[1]

La primera definición legal de Blockchain tuvo que esperar a 2018, cuando la Asamblea Legislativa del Estado de California en su Ley 2658 definió esta tecnología como "un registro o base de datos matemáticamente seguro, ordenado de forma cronológico y descentralizado".[2]

¿Qué es una Cadena de Bloques?

El concepto de "bloque" hace referencia a estructuras de datos que son generados por los ordenadores que forman parte de una red entre iguales. Estas estructuras de datos son registros que contienen transacciones, que generan un nuevo bloque una vez que se termine, formando una cadena. Cada bloque contiene elementos propios de su cadena de bloques.

Se trata de un REGISTRO DISTRIBUIDO, es decir, un Libro Mayor de contabilidad. Los datos contenidos en la Blockchain van a registrarse, replicarse y sincronizarse en todos los nodos/ordenadores de la red.

Blockchain es mucho más que una Fintech por lo que no podemos reducir la implementación de esta tecnología al ámbito de las criptomonedas como Bitcoin , pese al decisivo impulso que ha supuesto para el conocimiento, estudio y desarrollo de la tecnología.

Blockchain y el resto de DLTs parten de una preocupación principal, que es la PRIVACIDAD de los usuarios que utilizan dicho sistema, tal y como se recoge en el Manifiesto *Cypherpunk* de Eric Hughes que analizaremos a lo largo del presente trabajo.

[1] MAZZONE, C. (2018) "Presentation of the EU Blockchain Observatory and Forum". Blockchain Innovation in Europe. Simposio celebrado en Viena el 22 de mayo de 2018, https://www.eublockchainforum.eu/reports

[2] "Blockchain means a mathematically secured, chronological, and decentralized ledger or database". Cfr. California Assembly Bill 2658, https://legiscan.com/CA/text/AB2658/id/1821719

¿Cuál es el cambio que propone Blockchain?

Dentro del mundo Legaltech, la preocupación por el alcance e intromisiones de las tecnologías en la vida personal de los ciudadanos, de los poderes públicos, ha reforzado el planteamiento de esta tecnología a través del CÓDIGO, es decir, de las matemáticas, en aras a controlar la información que queda a disposición de los terceros interlocutores.

Cada individuo, gracias a la tecnología Blockchain, puede responder a tres preguntas importantes sin menoscabar su privacidad. Éstas son:

- La Autenticidad de la información
- La posesión de permisos para poder actuar.
- La existencia de un registro cronológico en el que consta el momento exacto de cada transacción.

El cambio propuesto por Blockchain goza por tanto de un componente imperativamente tecnológico y automático con una característica fundamental que la distingue de otras esferas regulatorias: la irreversibilidad de sus transacciones.

Igualmente, esta tecnología de naturaleza distribuida busca la eliminación de los intermediarios en cualquier tipo de transacción entre particulares, reforzando el concepto de "*peer to peer*", o igualdad entre pares.

2.2. INFLUENCIA DE OTRAS TECNOLOGÍAS DISTRIBUIDAS EN LA ACTUAL BLOCKCHAIN

En la edad de oro de los datos, o Cuarta Revolución Industrial, existe una superabundancia de información. En esta etapa cobra importancia el papel de los SISTEMAS/TECNOLOGÍAS DISTRIBUIDOS, que son definidos como componentes autónomos, o sistemas de software, que están ubicados en una red y que pueden comunicarse entre sí mediante mensajes.[3]

Para que el misterioso fundador de Blockchain, bajo el pseudónimo de Satoshi Nakamoto crease Blockchain, el papel de tecnologías desarrolladas décadas atrás como las Redes Peer-to-Peer y la Criptografía y sobre todo, de Internet tuvieron un papel decisivo en el mismo.

La tecnología *peer-to-peer*, tal y como la conocemos en la actualidad, tuvo su nacimiento a finales de los años 90, concretamente en el año 1999 con programas de intercambio de archivos musicales como NAPSTER.[4]

[3] MAUPIN, J.A (2017), "Blockchains and the G20: Building an Inclusive Transparent and Accountable Digital Economy". Center for International Governance Innovation Policy Brief bº 101, Center for International Governance Innovation.

[4] GLIBIN, Rebecca, "The P2P Wars: How Code Beat Law," in IEEE Internet Computing, vol. 16, no. 3, pp. 92-94, May-June 2012, doi: 10.1109/MIC.2012.57.

Estas tecnologías son *Redes de Igual a Igual*, en las que una red de ordenadores a nivel mundial usa una arquitectura distribuida en la que comparten cargas de trabajo en la red. Cada par/nodo/ordenador conectado a dicha DTL tiene los mismos derechos y obligaciones que los demás.

Por lo tanto, podemos decir que parte del carácter disruptivo y vanguardista de Blockchain proviene de la ruptura centralista de las Redes P2P respecto a la generalidad de sistemas de redes que mediante la relación cliente-servidor la mayoría de transacciones digitales.

Este carácter rutpturista de la tecnología Peer to Peer establece una arquitectura informática basada en la descentralización de los datos, de tal forma que no existe ningún servidor que aloje todos los datos. Existen dos modalidades de redes P2P:

A.- MODELO NAPSTER (P2P DE PRIMERA GENERACIÓN):

Los servidores centrales no albergan contenido alguno, pero si que existe un sistema de indexación y búsqueda de archivos alojados en la red al que debían recurrir todos los usuarios para intercambiar los contenidos. Este era el modelo del "viejo Napster".[5]

B.- MODELO KAZAA-FASTRACK (P2P DE SEGUNDA GENERACIÓN):

No existe centralización de ningún elemento, de tal forma que las funciones de búsqueda y de indexación de la información se encuentra también en todos los nodos de la red. Dentro de estas redes de segunda generación existen los denominados "supernodos" que son ordenadores de mayor potencia, velocidad y capacidad. [6]

Los elementos de una red P2P que se van a replicar en una Blockchain.

Las redes de pares están formadas por un conjunto de ordenadores, denominados nodos, con los mismos privilegios. En este sentido, toda red peer to peer va a estar compuesta por la siguiente estructura:

- NÚCLEO: compuesto por Internet con los protocolos TCP/IP.
- NODOS: se encuentran en el siguiente nivel. Aquí se sitúa la Blockchain, por ejemplo.
  Los nodos de la Blockchain se van a comunicar utilizando internet a través del protocolo común de determinada cadena de bloques en la que cada uno va a validar y almacenar una copia completa de toda la información. Es importante que

[5] TYSON, J. "How the old Napster worked". Artículo alojado en https://computer.howstuffworks.com/napster.htm

[6] WATSON, S. "How Does Kazaa Work". Artículo publicado en la web How Stuff Work".https://computer.howstuffworks.com/kazaa3.htm#:~:text=Kazaa%20uses%20peer%2Dto%2Dpeer,directly%20online%20to%20share%20content.

a este nivel todos los nodos cumplan las mismas reglas y se mantengan actualizados.

- DAPPs: Acrónimo de "Decentralized Applications" o aplicaciones descentralizadas, son un tipo de aplicaciones cuyo funcionamiento no depende de puntos de control o servidores centrales sino que funcionan en base a una red descentralizada como una Blockchain.[7]

Las Guerras Legales P2P:

Fundamentalmente, la colisión entre el uso de una tecnología informática vanguardista como las redes P2P iba a chocar, debido al volumen de tráfico a nivel mundial de información compartida en estas plataformas, iba a venir por las empresas titulares de derechos de Propiedad Intelectual como las multinacionales discográficas y audiovisuales como Promusicae, Warner Music, Universal Music, Emi Music y Sony BMG que demandaron en España a programadores de famosas redes P2P por presuntos perjuicios de más de 13.000 millones de euros.

El planteamiento de los litigios frente a esta tecnología se inició a través de dos vías: una frente a los desarrolladores y otra frente a los usuarios.

Tanto en una como en otra situación, desde 2008 se fueron sucediendo los fallos absolutorios a los desarrolladores como el famoso Pablo Soto, creador de numerosos programas de intercambio basados en tecnología distribuida como ManolitoP2P, Blubster y Piolet, por la presunta comisión de delitos contra la propiedad intelectual.

De acuerdo con la SAP Madrid de 13 de abril de 2014 "**carecen de cualquier posibilidad de control** sobre el empleo concreto que dan los usuarios a la herramienta informática puesto que éstos no precisan de intermediación técnica alguna por parte de aquellos para operar".

Respecto a los usuarios, tanto las legislaciones nacionales como las distintas directivas europeas en materia de Protección de la Propiedad Intelectual han amparado el concepto de copia privada, es decir, el mero intercambio sin compensación económica está amparado por el derecho.

Por lo tanto podemos señalar a NAPSTER como uno los principales programas que protagonizaron la denominada "Guerra de los P2P", tal y como fue definida por la profesora Rebecca Giblin, de la Universidad de Monash, en su artículo "The P2P Wars", en el que analizó las disputas legales entre los creadores de contenido y los softwares basados en tecnología distribuida (DLTs) a finales de la década de los años noventa, así como el triunfo de la tecnología sobre el derecho convencional.

Los creadores de contenido invirtieron sus esfuerzos sobre todo en persuadir a las empresas proveedoras de servicios (ISPs) para que asumiesen un papel más decisivo en cuanto al control sobre las infracciones cometidas por sus usuarios. La fuerza de los Lobbies de la industria cultural también ha actuado desde mediados de la década de los 2000 hasta hoy día a la hora de forzar a los parlamentos nacionales e internacionales, como el Parlamento Europeo, para la aprobación de leyes en contra de la piratería online,

[7] Bit2Me Academy. https://academy.bit2me.com/que-son-las-dapps/

como la famosa SOPA (Stop Online Piracy Act, de 26 de Octubre de 2011)[8], aprobada por el Congreso de los Estados Unidos de América.

El impacto de la tecnología P2P en las regulaciones mundiales ha sido enorme debido a que esta tecnología disruptiva supone un desafío de evolución a un rito tan elevado que los Parlamentos siempre van por detrás. Este impacto lo podemos apreciar en:

1) El carácter distribuido de estas redes hace muy difícil identificar a los usuarios
2) Los programas P2P crean una red con una potencia muy superior a la de cualquier equipo individual porque utilizan recursos de múltiples nodos que trabajan a la vez, causando una ventaja física.

Redes P2P y la Privacidad

Una de las funcionalidades que han sido implementadas por la tecnología Blockchain basadas en las redes P2P han sido las relativas a la búsqueda del anonimato de los usuarios. Esto nos lleva a hablar de Retroshare y las redes entre pares anónimas.

Estos sistemas de comunicación e intercambio de archivos se caracterizan por utilizar un sistema de enrutado de comunicaciones a través de redes superpuestas con la finalidad de ocultar la localización del usuario de los nodos.

Freenet es una de las plataformas creadas con la finalidad de evitar la censura en Internet en aras a la protección del Derecho a la Libertad de Expresión. Freenet utiliza "un sistema de almacenamiento de datos descentralizado para mantener y entregar información, y cuenta con una suite de software libre para publicar y comunicarse en la web sin correr el riesgo de ser censurado."[9]

Otro protocolo que usa el P2P para implementar las comunicaciones anónimas es **Invisible Internet Project o I2P**. Utiliza una variante del onion routing de TOR llamado "garlic routing" para dificultar el análisis de tráfico y aumentar la velocidad de transferencia de datos. I2P permite navegar por Internet de forma anónima, comunicaciones seguras, blogging anónimo y transferencia de archivos cifrada.

Redes P4P[10]

[8]Stop Online Piracy Act, del Congreso de los Estados Unidos de América, aprobada el 26 de Octubre de 2011.

[9]"Cómo funciona Freenet". Artículo escrito por la comunidad hacktivista "The Hacking News". https://latesthackingnews.com/2017/05/29/19914/

[10] https://www.malavida.com/es/analisis/redes-p2p-evolucion-de-un-protocolo-mas-alla-de-las-descargas-006483

Las **Proactive network Provider Participation for P2P** se definen como modelos híbridos de las actuales redes P2P que pretender optimizar las conexiones entre los nodos, es decir, mejorar la velocidad y calidad en las funciones de intercambio de archivos y velocidad de la red.

Respecto a estas redes, como sucede con todas las tecnologías disruptivas, se van a generar pros y contras:

- PÉRDIDA DE NEUTRALIDAD DE LA RED: Por una parte, la utilización de un sistema a través del que circula gran cantidad de información a una velocidad muy alta va a suponer un mayor control de los datos por parte de los Proveedores de Servicio (ISPs)
- INCREMENTO DE VELOCIDAD EN LOS INTERCAMBIOS: esta nueva tecnología va a suponer un paso adelante en las tecnologías distribuidas y va a atraer a grandes empresas tecnológicas.

2.3. CRIPTOGRAFÍA Y FIRMA DIGITAL. SEGURIDAD EN LA BLOCKCHAIN.

La base de la tecnología Blockchain se encuentra en seguridad ofrecida por técnicas criptográficas en las que se ofrezcan técnicas de cifrado para ocultar la información integrada en la cadena de bloques y que no sea fácil de resolver[11]. Lo habitual será establecer un mínimo de tiempo para resolver un problema matemático en aras a probar la fortaleza del sistema. Si se descubriese la forma de "minar" ese resultado en menos tiempo, la seguridad se rompería.

La Criptografía va a permitir de prescindir de los intermediarios, tanto desde el punto de vista legal como técnico al crear un sistema fiable de intercambio de información a través de la cadena de bloques sin necesidad de que un tercero certifique u otorgue confianza, como por ejemplo una administración o entidad verificadora.

Por lo tanto, la Criptografía va a crear una seguridad alternativa a la ofrecida por un intermediario, que va a descansar en e consenso de todos los nodos de una cadena de bloques que otorga fiabilidad y confianza en las transacciones[12]

En Blockchain se utiliza la firma con clave asimétrica, en la que se usan claves públicas y privadas:

1) La clave pública es la dirección de un usuario en la propia cadena de bloques, y que se muestra al resto
2) La clave privada es la contraseña, y que solo es conocida por el usuario. Le permite la protección de sus activos digitales.

[11] MERKLE, R.C "Protocols for public key cryptosystems". Proc. 1980 Symposium on Security and Privacy. IEEE Computer Society, pp. 122-133.
[12] NORTON ROSE FULBRIGHT (2016), Unlocking the Blockchain. A Globlal legal and regulatory guide, https: //www.nortonrosefulbright.com/knowledge/publications/141573/unlocking-the-blockchain-a-global-legal-and-regulatory-guide-chapter-1/.

Respecto al mecanismo de Hash, aunque posteriormente lo desarrollaremos en mayor profundidad podemos apuntar que es una función matemática creada de manera aleatoria por un conjunto de datos alfanuméricos que se añaden a un archivo y su resolución garantiza la INTEGRIDAD de los datos.
Cualquier alteración del contenido de un archivo "hasheado" o del propio "hash" supondría una vulneración de su contenido, sería detectado por la Blockchain y no validado.

El Proceso de Consenso como elemento fundamental en la validación de un nuevo bloque en la cadena:

Al tratarse de un sistema distribuido, todos los nodos deben contar con la misma información y contar con los mismos permisos para el correcto funcionamiento de una Blockchain.
Los nodos necesitan un sistema en el cual se garantice el consenso para poder aprobar una transacción. Comúnmente se utilizan dos sistemas:

1) El Proof of Work(PoW) o Minería, en la que las decisiones sobre los cambios se toman en función del trabajo realizado. Es el sistema de consenso utilizado en Bitcoin y consume muchos recursos.
   La función del minero consistirá en validar y sellar el problema matemático planteado. El primero que resuelva el problema logrará la recompensa y avisará al resto de nodos para que comprueben y validen. Una vez realizado ese paso, dicho bloque se añade a la cadena y no podrá ser modificado.
2) Proof of Stake (PoS), o prueba de participación. En este caso los nodos son validadores de bloques. Realizan esta actividad de una manera aleatoria pero dando una mayor probabilidad a quienes cumplan con los requisitos exigidos. Las criptomonedas que utilizan este sistema, como Peercoin, NXT o Bitshares son mas sostenibles.

2.4. SMART CONTRACTS. LA PREPROGRAMACIÓN DE UN CONTRATO

El protocolo basado en tecnología Blockchain denominado de una manera coloquial para el conjunto de usuarios "Smart Contract" se considera a día de hoy un concepto vivo y en constante evolución desde que Nick Szabo[13] describió por primera vez en 1994 qué funciones iba a integrar esta aplicación técnica.

La complejidad de un Smart Contract se encuentra en la configuración del mismo puesto que una vez que describe todos los condicionantes, cláusulas, plazos y demás opciones, estos son conocidos por las partes y se genera confianza.

El incremento en el uso de contratos inteligentes ha venido por su versatilidad a la hora de crear contratos con condiciones pago, garantías, pactos de confidencialidad de una manera clara precisa y sobre todo independiente de terceros, salvo como veremos la figura de los oráculos.

El concepto de Smart Contract por lo tanto es anterior al desarrollo de la tecnología Blockchain actual, pero nació limitado por la tecnología sobre la que operaba, la

[13] SZABO, Nick. "Smart Contracts" (1994)

denominada EDI[14]. No fue hasta 2009, y gracias al desarrollo de la tecnología Blockchain cuando se pudieron desarrollar todas las funcionalidades que mejoraron este protocolo.

Identificación de las partes en un Smart Contract. Utilización de la criptografía:

Un Smart contract está compuesto por una serie de líenas de código en el que participan dos partes que se identifican con la clave pública de su monedero ("wallet") y que utilizarán su clave privada para firmar el Smart contract, con el que se manifesta el consentimiento.

Ejemplo de Smart Contract[15]:

```
/* Allow another contract to spend some tokens in your behalf */
function approve(address _spender, uint256 _value)
    returns (bool success) {
    allowance[msg.sender][_spender] = _value;
    return true;
}

/* Approve and then comunicate the approved contract in a single tx */
function approveAndCall(address _spender, uint256 _value, bytes _extraData)
    returns (bool success) {
    tokenRecipient spender = tokenRecipient(_spender);
    if (approve(_spender, _value)) {
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }
}

/* A contract attempts to get the coins */
function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
    if (balanceOf[_from] < _value) throw;                 // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw;  // Check for overflows
    if (_value > allowance[_from][msg.sender]) throw;   // Check allowance
    balanceOf[_from] -= _value;                           // Subtract from the sender
    balanceOf[_to] += _value;                             // Add the same to the recipient
    allowance[_from][msg.sender] -= _value;
    Transfer(_from, _to, _value);
    return true;
}

/* This unnamed function is called whenever someone tries to send ether to it */
function () {
    throw;     // Prevents accidental sending of ether
}
```

Aproximarse a una definición de un Smart Contract o Contrato Inteligente nos lleva a analizar en primer lugar la imprecisión del calificativo "inteligente", dado que lo más preciso, tal y como indica el Profesor García Mexía, sería hablar de CRIPTOCONTRATO.[16]

Existe un consenso por parte de la doctrina en definir esta figura como un acuerdo o contrato digitalizado autoejecutable y auto aplicable, que verifica las condiciones del mismo o que directamente lo ejecuta. Los criptocontratos son FÓRMULAS que

[14] Electronic Data Interchange.
[15] Fuente: https://blockgeeks.com/guides/smart-contracts/
[16] GARCÍA MEXÍA, P., "Del ciberderecho al criptoderecho. La Criptoregulación", págs. 97 y siguientes)

contienen intercambios o acuerdos con una característica en el Criptoderecho, esto es, la IRREVERSIBILIDAD y la TRAZABILIDAD de los mismos.[17]

Suponen el paradigma del CRIPTODERECHO por cuanto aúnan características de la contratación electrónica y de la criptografía.

Composición de un Smart Contract desde el punto de vista técnico: [18]

A.- BLOCKCHAIN

La utilización de la tecnología Blockchain por parte de los protocolos denominados contratos inteligentes ha sido decisiva para el despegue de estos últimos.

El Smart contract se registrará en el libro mayor de una Blockchain determinada (pública, privada, permisionada o no permisionada) y el conjunto interconectado de nodos tendrá una copia completa de todo ese libro mayor, que se irá actualizando constantemente mediante la agregación de nuevos bloques, en base a la tecnología criptográfica que ya hemos explicado anteriormente.

B.- CRIPTODIVISAS

Se definen como las representaciones digitales inscritas en una Blockchain de activos que pueden representar derechos económicos o políticos. El proceso de digitalización de un activo en un "token" se denomina tokenización.

Las criptodivisas son divisas P2P puramente digitales que se caracterizan por ser transparentes, seguras y privadas y no dependientes de ningún banco central, lo que supone que se trata de activos muy volátiles.[19]

Cada criptodivisa opera en su propia Blockchain y entre las más conocidas nos vamos a encontrar con Bitcoin y Ethereum. Cuentan con su propio registro de operaciones que es accesible a todo el mundo y por lo tanto trazable.[20]

Estándares dentro de las criptodivisas:

Cada criptodivisa cuenta con características propias que habilita a las mismas a ser utilizadas para cierto tipo de intercambios.

[17] M. STAMPATORI, "Smart contract – How To Create A Smart Contract", *The Guide for Non Technical Managers To Smart Contracts*, Kindle Edition. 2019.

[18] NAVARRO DE ANDRÉS, Santiago. "Contratos Inteligentes. En especial, su implantación práctica en negocios Blockchain". Criptoderecho. La regulación de Blockchain. Páginas 319 y siguientes.
[19] SZABO, N. (2017) "Money, Blockchains and Social Scalabiity". Unenumerated, Februeary 2017. https://www.ted.com/talks/don-.taps_how_the_blockchain_is_changing_money_and_business/up-next.
[20] Consultado en la web especializada https://academy.bit2me.com/que-es-una-criptomoneda/

En la actualidad, podemos citar como estándares de criptodivisas más utilizados el ERC-20 y el ERC-721.

C.- SMART CONTRACT

El último elemento es el propio diseño de la formula de los intercambios en base a esta tecnología criptográfica que debe de tener una serie de cautelas y medidas de accountability o seguridad desde el diseño.

Una de las características principales de los criptocontratos es su carácter auto-ejecutable si se cumplen las condiciones que se han preestablecido en las correspondientes líneas de código. En este sentido, y desde el sentido más estricto del término, los Smart contracts no quieren depender de intermediarios o de agentes externos para su validez.

Los oráculos:

Sin embargo, en la actualidad, y para evitar los riestos de alteraciones artificiales en los valores de cotización, se ha creado una figura denominada Oráculo, que se define como "las fuentes externas a la Blockchain que aportan información sobre el mundo real a los Smart contract según estos lo solicitan. Estos oráculos pueden ser tanto referencias a páginas webs o a dispositivos físicos o incluso personas (pensemos en un Juez, un Letrado de la administración de Justicia o un Funcionario de Hacienda).

Los Smart Contract van a ser el paradigma del estudio de la protección de los derechos fundamentales en relación con la tecnología Blockchain.

3. IMPLICACIONES JURÍDICAS: BLOCKCHAIN Y DERECHOS FUNDAMENTALES DIGITALES AFECTADOS

3.1. *LEX CRIPTOGRAPHICA*: CODE IS LAW

Ya hemos hablado en apartados anteriores acerca de la decisiva importancia de la base criptográfica de la Blockchain a la hora de crear un ecosistema propio y potencialmente al margen de las normas jurídicas.

Si partimos del actual Estado de Derecho y de Imperio de la Ley como expresión de la voluntad popular, la irrupción de Blockchain va a suponer, en el campo de los derechos fundamentales, que la protección otorgada por el ordenamiento jurídico no va a tener la misma efectividad sobre ciertos actos de los usuarios en el ciberespacio que pudiesen afectar a aquellos.

La tecnología ha incidido de una manera decisiva en los Derechos Fundamentales "analógicos", creando unos nuevos en la esfera digital y reconfigurando los antiguos dependiendo del estado de la tecnología.

La creación de un espacio en el que los derechos fundamentales digitales de las personas sean absolutos, es decir, oponibles *erga omnes*, implica la inexistencia de límites en su ejercicio por parte de su titular a cambio de perder cualquier tipo de medida de protección en caso de la violación de dichos derechos, precisamente por la laxitud y el carácter voluble de la tecnología.

El profesor de Harvard Thibault Schrepel[21], planteó un estado imaginario en el que las personas/usuarios de Blockchain pueden negociar dentro de ese ecosistema digital cuáles de los derechos fundamentales que han sido reconocidos por los Estados en la actualidad van a operar en sus relaciones en la Blockchain, y del mismo modo, y con carácter independiente, van a pactar unos nuevos o incluso disponer de dichos derechos en aras a obtener servicios *online*.

Estas afirmaciones planteadas por la doctrina son revolucionarias y suponen un cambio de paradigma en cuanto al ejercicio y protección de derechos incardinados con la dignidad humana, los derechos Fundamentales en aras a la promesa del desarrollo tecnológico.

La aparición de la tecnología Blockchain ha supuesto, por tanto, una revolución en la doctrina científica, en cuanto que supone introducir un nuevo ecosistema, basado en la Criptografía y en las redes distribuidas tipo P2P pero también con base en una Filosofía que denominada "CypherPunk" (término acuñado por Eric Hughes en su Manifiesto CypherPunk) en la que el Código Tecnológico es un tipo de derecho especial: el Criptoderecho, la LEX INFORMATICA.

[21] T. SCHREPEL, "Anarchy, State, and Blockchain Utopia: Rule of Law versus Lex Cryptographia in General Principles and Digitalisation. Hart Publishing,. 2020.

Y es que autores como May o Atzori previeron esa vis expansiva de la Criptografía a la hora de regular las relaciones entre usuarios de la plataforma desafiando al Estado de Derecho o Imperio de la Ley a la hora de proteger y regular las discrepancias con una base matemática.

La idea de utilizar la criptografía para proteger los Derechos Fundamentales de Libertad y Privacidad de los Ciudadanos tiene bases del Manifesto Comunista de Karl Max y que fue desarrollada por la cultura cypherpunk y criptoanarquista de finales de los años setenta.

Eric Hughes formuló el Manifesto Criptoanarquesta en mayo de 1988 y en el cual establecía los principios de esta revolución:

"La privacidad es necesaria para una sociedad abierta en la era electrónica. La privacidad no es secretismo. Una cuestión privada es algo que no queremos que todo el mundo sepa, pero una cuestión secreta es algo que no queremos que nadie sepa. La privacidad es la capacidad de revelarse selectivamente al mundo.(…) Así mismo la privacidad en una sociedad abierta requiere la criptografía. Si yo digo algo, quiero que lo oigan sólo aquellos a los que iba dirigido lo que decía. Si el contenido de mi discurso está al alcance de todo el mundo, no tengo privacidad. Encriptar es indicar que se desea la privacidad y encriptar con sistemas criptográficos « débiles » es indicar que no se tiene un gran interés en la privacidad. Además, revelar la propia identidad de forma que no hayan dudas cuando lo estándar es el anonimato requiere del sistema de firmas criptográficas.(…)[22]

Existen múltiples manifestaciones dentro del Criptoderecho. En el caso del Criptoderecho nacido de la Blockchain, el componente de la irreversibilidad de las transacciones va a ser el que dota de independencia al mismo al prescindir del componente humano y de cualquier norma para su desarrollo[23]

La Blockchain, debido a sus características técnicas, amenaza de una manera directa al Estado de Derecho, en el sentido en que el derecho aprobado en los Parlamentos Nacionales e Internacionales no va a poder aplicarse de la misma manera dentro que fuera de él. Es por ello, que el profesor Robert Nozick planteó la coexistencia de dos ecosistemas condenados a entenderse: El Estado de Derecho fuera de Blockchain y la Lex Cryptographica dentro del entorno Blockchain.[24]

[22] HUGES, E. "The Crypto Anarchist Manifesto". Mayo 1988 y "Cypherpunk´s Manifesto". 1993.
[23] M.J. CASEY y P. VIGNAM P. (2018), "In Blockchain We Trust", MIT technology Review, volume 121, nº 3, p.10-16.
[24] NOZICK, Robert (1974. "Anarchy, State and Utopia". Harvard 18ª Ed. Basic Books.

El límite marcado por la tecnología Blockchain

Es pacífica entre la doctrina científica la asunción de que un sistema de registro distribuido como Blockchain puede articular relaciones entre particulares prescindiendo de las normas jurídicas[25].

Blockchain es una tecnología que asegura la PRIVACIDAD de sus usuarios a través de la técnica de la PSEUDONIMIZACIÓN[26]; es decir, que cuando usamos una Blockchain pública o privada, los usuarios no revelan su identidad, sino que muestran su clave pública, esto es, una identidad encriptada formada por una secuencia alfanumérica.

El concepto de "prueba de conocimiento cero" como paradigma de la privacidad de Blockchain

Esta disociación entre el mundo real y el escenario Blockchain se refuerza gracias a los avances dentro de la Lex Informática como la denominada "Prueba de Conocimiento Cero" (Zeroknowledge Proof) que ha sido implementada en transacciones que utilizan la tecnología Blockchain, tanto en materia de criptomonedas como en criptocontratos en los que exista un intercambio de valores.

La Prueba de Conocimiento Cero significa que estas transacciones van a ser validadas por un tercero ajeno y que no conoce a ninguna de las partes ni tampoco conoce la naturaleza jurídica de la transacción que se esté llevando a cabo.[27]

Dentro del registro de la Blockchain aparecerá por tanto la EXISTENCIA de una transacción, pero no la IDENTIDAD, la NATURALEZA ni la CAUSA de la transacción, quedando este dato al margen del conocimiento de extraños a la cadena de bloques.

Ello va a tener un efecto significativo respecto a los efectos jurídicos fuera del entorno Blockchain en derechos como el de PROPIEDAD (art. 33 CE) en tanto en cuanto se configura un criptocontrato para la realización de una operación de transacción de un bien inmueble en el que hay un desplazamiento de la propiedad va a colisionar con el ordenamiento vigente regulado en el Código Civil (arts. 1445 y siguientes), así como en el art. 1280 del mismo, y la legislación hipotecaria, en la medida en que el propio Criptoderecho contenido en el código puede permitir que si se dan y se cumplen las circunstancias fijadas en el contrato inteligente, se ejecuten automáticamente y el acuerdo sea válido, debido a la IRREVERSABILIDAD DEL CONTRATO. Ningún tribunal podría anular la validez de un criptocontrato de acuerdo a este planteamiento.

25 UK Government Act, 2016, 41

26 NARAYANAN, Arvind y CLARK, Jeremy, (2017) Bitcoin's Academic Pedigree, 60 COMMUNICATIONS OF THE ACM 36 (2017)

27 What Are ZK-SNARKs?", Z CASH (2019), publicado en la web https://z.cash/technology/zksnarks.html.

La irreversibilidad como eje central del criptoderecho

La esencia del carácter irreversible de una transacción realizada en una Blockchain se basa en el carácter descentralizado del registro. "Nadie controla la Blockchain, pero al mismo tiempo, todos los nodos de la misma Blockchain lo están".[28]

¿Son alternativos el Estado de Derecho y la Lex Criptográfica?

Dentro del ecosistema de una Blockchain no se puede aplicar con carácter general la regulación legal aprobada en los Parlamentos nacionales, lo cual va a afectar sobremanera el ejercicio de los DERECHOS FUNDAMENTALES porque precisamente estos son protegidos por el IMPERIO DE LA LEY fuera del entorno Blockchain.

En este punto debemos acudir al párrafo segundo del Preámbulo de la Carta de los Derechos Fundamentales de la Unión Europea,[29] en el cual se establece que:

"Consciente de su patrimonio espiritual y moral, la Unión está fundada sobre los valores indivisibles y universales de la dignidad humana, la libertad, la igualdad y la solidaridad, y se basa en los principios de la democracia y el Estado de Derecho. Al instituir la ciudadanía de la Unión y crear un espacio de libertad, seguridad y justicia, sitúa a la persona en el centro de su actuación".

De una interpretación literal de este párrafo podemos determinar que los derechos fundamentales de la persona únicamente van a ser protegidos plenamente dentro del Derecho, quedando desprotegidos dentro del ecosistema de la Blockchain. Sin embargo, a continuación vamos a ver cómo muchos de estos derechos fundamentales van a poder ser protegidos por parte de la *Lex Criptographica*.

¿La Lex Criptográfica protege los derechos fundamentales analógicos?

Los nuevos desafíos planteados por la tecnología Blockchain en el ámbito legal tienen un grave impacto en el reconocimiento y defensa de los Derechos Fundamentales tradicionales por cuanto éstos no van a ser tutelados con la misma efectividad en el ecosistema creado por la informática y la criptografía.

El tradicional status quo en el que los Poderes Públicos van a detentar el poder Legislativo, el Poder Ejecutivo y el poder Judicial va a adoptar un giro copernicano en favor de la Tecnología como garante de estos derechos fundamentales

[28] T. SCHREPEL, Thibault. "Anarchy, State, and Blockchain Utopia: Rule of Law versus Lex Cryptographia" in *General Principles and Digitalisation*, Hart Publishing. 2020.

[29] Publicada en el Diario Oficial de la Unión Europea de 30 de marzo de 2010.

Ya lo indicaba uno de los pioneros en la regulación del ciberderecho como J. Reidenberg al establecer que "*para los entornos de la red y en la sociedad de la información (…) el Derecho y la regulación pública no son la única fuente normativa".*[30]

Autores como Robert Nozick y Schrepel defienden en sus tesis sobre esta dicotomía que Derecho y Criptoderecho pueden coexistir permitiendo a la tecnología crear un equivalente a la Justicia ordinaria que fije unas reglas y se asegure para que se cumplan.

¿Significaría esto que los usuarios de una Blockchain podrían proteger sus derechos fundamentales dentro de una Blockchain según la Lex Criptographica? Para dar una respuesta positiva, el profesor Schrepel establece tres consideraciones: .[31]

1.- Existe una equivalencia respecto a los Derechos Fundamentales reconocidos por el Estado de Derecho y los que se reconocen por la Lex Criptographica: Esta consideración podría ser abrazada por el Derecho Natural que admite la existencia de una serie de derechos que son anteriores a cualquier legislación. Alternativamente, se podría aplicar con carácter extensivo el Derecho Positivo, en el sentido que los Derechos Fundamentales pueden ser transpuestos a la esfera de la Blockchain.

2.- La Lex Criptographica no fija un Sistema de Fuentes tal y como realiza el Estado de Derecho

En este punto el propio J. Reidenberg considera al hablar no de Ley Criptográfica (este concepto es posterior) sino al tratar de definir el marco de la Ley Informática que el Código puede sustituir al Derecho, cuando estas normas tecnológicas estén en mejor situación para resolver un problema regulatorio.[32]

3.- El paradigma actual del criptoderecho se encuentra en la configuración actual de los Smart Contracts.

Code is Law: El Derecho como Código[33]

El código criptográfico de la Blockchain va a ser la única norma, al menos dentro de las Blockchain públicas y no permisionadas, que va a regular las relaciones entre los usuarios de un criptocontrato.

Este carácter de norma tecnológica, al margen de la normativa vigente "en el mundo físico", va a asentarse en la encriptación e irreversibilidad de las transacciones llevadas a cabo a través de esta tecnología. Precisamente porque esa irreversibilidad es quien otorga a los usuarios la confianza en el sistema y no en el Derecho tradicional.[34]

30 REINDENBERG, J.R, Lex Informatica: The Formulation of Information Policy Rules through Technology, " Texas Law Review 76.

31 SCHREPEL, Thibault. "Anarchy, State, and Blockchain Utopia: Rule of Law versus Lex Cryptographia" in *General Principles and Digitalisation*, Hart Publishing. 2020.

32 REIDENBERG, J.R, "Lex Informatica: The Formulation of Information Policy Rules through Technology, " Texas Law Review 76.

33 LESSIG, L., (2001) "Code and Other Laws of Cyberspace". Editorial Basic Books.

34 DE FILIPPI, P y WRIGHT, A. (2018) Blockchain and the law. The Rule of Code.

La anterior afirmación supone que la única forma en la que un usuario de Blockchain pudiese ejercer acciones por una vulneración de un Derecho Fundamental sería sacrificando la esencia de esta tecnología, es decir, a través de la exposición de su privacidad, mediante la revelación de su propia clave privada o la de aquel que hubiese vulnerado el derecho.

La Elección en tutela de los Derechos Fundamentales

La tutela de los Derechos Fundamentales de las personas va a ser diferente dependiendo si los usuarios la buscan a través del poder coercitivo del Estado o en el Criptoderecho.

La tutela de los Derechos Fundamentales por parte del Ordenamiento Jurídico establece una serie de límites en el ejercicio de los mismos como el correspondiente a la ponderación de dos derechos en colisión y el acceso a los Juzgados y Tribunales para hacer valer cualquier tipo de menoscabo.

Por lo tanto se genera entre los usuarios de Blockchain una crisis en relación con el Derecho aplicable al ofrecer la posibilidad de aplicar por un lado el derecho criptográfico creado en un criptocontrato, y por otra parte el Derecho tradicional "offline" en el que se garantiza la tutela de los derechos y libertades fundamentales.

La coexistencia de dos normativas dentro de la esfera de Blockchain va a implicar que el usuario tenga que tomar una decisión consistente en asumir que dentro Blockchain ciertos derechos fundamentales van a ser expuestos y se van a regular por la Ley Criptográfica, especializada y adaptada a la realidad de dicho ecosistema, o no usar dicha tecnología.

En caso de que el usuario asuma los riesgos de la utilización de Blockchain, va a tener que considerar un doble escenario:

Si la tecnología Blockchain sigue su actual crecimiento y su uso llega a ser indispensable dentro de Internet, la legitimidad de los Limites a los Derechos Fundamentales tendría que ser cuestionada de la manera que lo planteó Rober Novick no existe en la actualidad una capacidad dispositiva de los ciudadanos para decidir si se aplica el Estado de derecho o el derecho Criptografico.

3.2. DERECHO DE PRIVACIDAD Y PROTECCIÓN DE DATOS

La tecnología Blockchain permite crear a sus usuarios un registro o libro en el que se recojan transacciones de una manera rápida, segura, trazable, criptográfica y de una manera transparente de una forma descentralizada o distribuida entre una basta red de ordenadores o nodos que forman parte de una determinada plataforma y que no depende de terceros sino de los propios usuarios de dicha red. La característica principal de esta tecnología es la irreversibilidad de los datos validados obligatoriamente por la mayoría de los usuarios e introducidos de manera cronológica haciendo imposible la alteración de los mismos. Con esta tecnología se garantiza la autenticidad y la protección de la información que se introduce.

A través de Blockchain podemos controlar la seguridad de la información gracias a la criptografía, la alta tecnología en la que se utilizan protocolos avanzados de verificación y protección de las operaciones de tal forma que os miembros de la plataforma expulsarían cualquier alteración contra el sistema.

La transparencia del modelo Blockchain supone que todo cuanto se escribe en el registro de una Blockchain determinada puede ser leído por cualquiera que tenga acceso a la misma (este acceso obviamente será mayor si hablamos de una Blockchain púbica no permisionada).

Sin embargo, pese a que tal y como hemos ido analizando a lo largo de este trabajo, nos encontramos con una tecnología segura en términos de integridad de la información alojada en ella, se nos plantean graves conflictos a la hora de determinar su respeto por el derecho fundamental de Intimidad Personal.

Nuestra Constitución Española en el art. 10.2 establece que "las normas relativas a los derechos fundamentales y a las libertades públicas que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de los Derechos Humanos y los Tratados y Acuerdos Internacionales sobre las mismas materias ratificados por España."

El art. 12 de la Declaración Universal de los Derechos Humanos establece que "Nadie será objeto de interferencias arbitrarias en su vida privada, familia, su domicilio o su correspondencia ni de ataques a su honra ni a su reputación. Toda persona tiene Derecho a la Protección de la Ley contra tales interferencias o ataques".

El Derecho a la intimidad, reconocido en el art. 18.1 CE reconoce, engloba y trata de proteger la esfera más privada del ser humana compuesta por la vida privada y familiar, que en el art. 12 DUDH garantiza a través de la prohibición de conductas de carácter público o privado que tengan por objeto una intromisión en el ámbito del ser humano[35]

En conexión con los artículos anteriores, el art. 8.2 del Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales de Roma[36] establece que "no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sin en tanto en cuanto esta inferencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud, de la moral o la protección de los derechos y las libertades de los demás." Este artículo, claramente fija una serie de límites al ejercicio del derecho y que van a tener que ser tomados en consideración a la hora de establecer un análisis dentro del ámbito tecnológico.

[35] SAURA ESTAPA, J. Comentarios al texto de la Declaración Universal de los Derechos Humanos. Art. 9 En: PONS RAFOLS, X. La Declaración Universal de los Derechos Humanos: Comentario artículo por artículo. 1ª Ed. Barcelona. 1998. Icaria Editorial S.A, p.p 226-229

[36] Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950. Instrumento de Ratificación de 26 de septiembre de 1979 (BOE Nº 243, de 10 de octubre de 1979).

Uno de los vacíos legales que nos encontramos con la tecnología Blockchain es la protección de la privacidad de los usuarios.

Consecuentemente debemos dirigir nuestro estudio hacia la nueva regulación en materia de protección de datos tanto en el ámbito europeo con el Reglamento General de Protección de Datos y con la Ley Española, puesto que puede existir una colisión entre ambas.

La importancia del tipo de Blockchain en relación con la Privacidad.

En este momento, conviene dedicar un análisis a los dos tipos de Blockchain que pueden configurarse, las públicas y las privadas.

Las Blockchain Públicas no tienen restricciones para acceder a ellas, leer los datos registrados en su libro mayor, así como agregar nuevas transacciones u operaciones con los que encadenar un nuevo bloque.
Debido a la ausencia de una autoridad central que verifique la autenticidad y validez de la transacción, esta labor se encomienda a los Mineros.

Una Blockchain Privada limita, como su propio nombre indica, el acceso a la lectura y el desarrollo de operaciones dentro de la misma a usuarios determinados.

Sin embargo, dentro de las configuraciones de cada tipo de Blockchain, la capacidad otorgada a sus usuarios para poder generar nuevas cadenas de bloques depende de los PERMISOS. Así nos encontramos con:

- Blockchains sin permisos: aquellas en las que no existen restricciones para los usuarios
- Blockchain permisionadas: se definen como aquellas Blockchains, generalmente privadas, que están configuradas para una red privada y bajo invitación de sus miembros. En este caso, se plantea una quiebra del principio de descentralización al ganar peso los administradores (intermediarios o middle men).

Dependiendo qué tipo de Blockchain se utilice, el criptoderecho resultante de dicha Blockchain va a colisionar más o menos con el Derecho.

Tal y como vamos a desarrollar en los siguientes puntos, la tendencia por parte del mercado, una vez que el RGPD entró en vigor el 25 de mayo de 2018, es buscar fórmulas híbridas en las que se pueda integrar Blockchain.
Esta tecnología cuenta con muchas ventajas para los usuarios en cuanto se genera una mayor confianza en la privacidad y en las relaciones de igual a igual pero que necesita de una adecuación dentro de una Legislación externa al Criptoderecho para que la misma pueda tener efectividad fuera de la Blockchain.

Pese a las reticencias planteadas por parte de la doctrina, como establece la profesora Carmen Perete Ramírez, sobre los problemas de encaje de Blockchain con el respeto del derecho fundamental a la protección de datos del art. 18.4 CE, la vigencia y aplicabilidad de las Blockchains en el tráfico jurídico y relaciones personales y con las Administraciones Públicas es no solo posible sino adecuado desde el Derecho.

El difícil encaje de Blockchain dentro del marco establecido por el RGPD al buscar una centralización de la información en todos los servicios online como el comercio electrónico, el cloud computing o los servidores de internet choca con el carácter descentralizado de la cadena de bloques.

Comparativa de los Principios de los dos ecosistemas en relación con la Privacidad:

A.- PRINCIPIOS DE LA TECNOLOGÍA BLOCKCHAIN

Por una parte, los principios básicos en los que se basó la tecnología Blockchain desde sus inicios son la publicidad, la inmutabilidad, la descentralización, la distribución, el consenso de los usuarios, el código abierto de su software, y la seguridad criptográfica[37].

El principio de publicidad implica la utilización de la firma digital del usuario que registra el verificador del bloque, quedando a la vista del resto. Dicho alcance obviamente será mayor.

Debido a que la criptografía de Blockchain establece cifrados asimétricos, la publicidad de la clave pública podría llegar a identificar al usuario debido a la reiteración en el uso de dicha clave en una misma Blockchain.

Uno de los caracteres más controvertidos dentro de la protección de la privacidad y su adecuación al RGPD va a ser el carácter de inmutabilidad por dos cuestiones. En primer lugar, el nacimiento de las redes P2P es anterior al planteamiento de normativa de protección de datos con un carácter centralizado, por lo que hay que medir el alcance de una posible interpretación restrictiva del carácter de inmutabilidad de un bloque insertado dentro de una Blockchain.

La inmutabilidad es por tanto un sinónimo de confianza entre los usuarios de Blockchain, en el sentido de que en la propia cadena de bloques el hash de un bloque anterior se referencia en el ulterior y así sucesivamente. La variación de cualquier dato introducido en una cadena de bloques rompería la misma y sería el fin último de la cadena de Blockchain.

El carácter distribuido de la Blockchain significa una huida de la centralidad, de los intermediarios del sistema. Dentro de este ecosistema, se encontrarían no solo los abogados, legisladores sino también ingenieros de sistema o programadores que configurar y mantienen una red Blockchain.

En este punto debemos analizar el concepto de la **Identidad Descentralizada**:

La identificación dentro de una red Blockchain es suministrada por el propio usuario. Muchas veces basta con que el usuario acredite por sí mismo la identidad de sí mismo, otras veces es un tercero, que puede ser una administración o una entidad..[38]

[37] Ver artículo "¿Qué es la tecnología de la contabilidad distribuida o blockchain?" publicado por la Revista Criptonoticias, disponible en https://www.criptonoticias.com/informacion/que-es-tecnologia-contabilidad-distribida-blockchain/

[38] **SOTOMAYOR, Antonio. "**Covid-19, Identidad y el Sr. Patata - BlockTimes #2", https://youtu.be/t9ONc6Hoq4I

Cada usuario y de forma privada crea una identidad única dentro de la Blockchain. Por otro lado, nos encontramos con las entidades o administraciones que emiten un conjunto de atributos para su posterior firma electrónica A esta operación se denomina credencial verificada.

En este contexto el usuario puede revelar una serie de datos sin revelar la identidad de él mismo porque la entidad ha emitido una credencial verificada relativa a su competencia o a una información específica que puede ser de naturaleza fiscal, médica, administrativa, u otra.

Este sistema descentralizado prevé una fórmula para evitar que varias entidades que hayan emitido acreditado a un mismo usuario sobre unos datos crucen datos (por ejemplo, la información relativa a un test de seropositividad de Covid-19) de tal forma que quedase revelada la identidad del usuario. La Blockchain permite al usuario crear múltiples identidades para cada relación o conjunto de atributos.
La identidad descentralizada cambia el paradigma, puesto en vez de que las características de una identidad queden almacenadas en un mismo sitio, como una Red Social, una página web,… y que esos datos se vayan engordando y beneficiando a dicha empresa, ahora la identidad es controlada por el propio usuario, y van a ser las entidades y empresas quienes van a ayudar mediante la emisión de credenciales.

B.- PRINCIPIOS DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS:

El marco legal establecido por el RGPD parte de un enfoque radicalmente opuesto al planteado por la Blockchain en materia de protección de la privacidad de las personas. La nueva regulación vigente desde el 25 de mayo de 2018 se fundamenta en un enfoque centralizado y tecnológicamente neutro.

La regulación europea es incompleta por cuanto regula la protección del derecho autónomo de protección de datos desde el punto de vista de un modelo de explotación y de negocio basado en la red concentrado, es decir, en redes sociales, servicios de almacenamiento o hosting, motores de búsqueda, … obviando la realidad de la tecnología Blockchain que plantea desafíos en materia de tratamiento de datos.

La propia profesora Perrete Ramírez establece que “el propio reglamento ha quedado obsoleto al no contemplar las posibilidades planteadas por parte de Blockchain”. Sin embargo, y de acuerdo al profundo análisis efectuado por el Profesor Schrepel, la idiosincrasia de ambas leyes, la del Reglamento y la Lex Criptográfica que opera dentro de la tecnología Blockchain estrechan lazos y están condenadas a entenderse.

Sin pretender un análisis pormenorizado de los principios regulados en el RGPD, debemos citarlos:

1.- licitud, lealtad y transparencia en el tratamiento de los datos
2.- limitación del fin
3.- minimización de los datos

4.- exactitud de los datos
5.- integridad y confidencialidad
6.- limitación del almacenamiento

La figura del responsable del tratamiento de los datos de carácter personal que determina los fines de los datos recogidos se alza como el eje fundamental en el cumplimiento de la normativa en materia de protección de datos.

El RGPD pretende identificar en todo momento a la persona que debe garantizar el cumplimiento de dichos requisitos, centralizando todas las operaciones que se lleven a cabo mientras existan datos de carácter personal. Esta figura va a suponer una de los mayores escollos entre ambos ecosistemas para poder convivir dentro del marco de la legalidad constitucional.

La persona, como titular de derechos y deberes reconocidos por parte del ordenamiento jurídico va a tomar una posición de control sobre los datos que hayan sido objeto de tratamiento y que tengan carácter personal y privado, en lo que se denomina como un enfoque user-centric[39] con un eminente carácter patrimonial del derecho de protección de datos.[40]

Blockchain y su aproximación al RGPD:

El valor del dato personal, la información, es el nexo de unión entre ambas regulaciones nacidas desde distintos puntos de partida.

Es prudente considerar que ambas posturas no parten de polos opuestos puesto que dotan de poder al individuo a la hora de manejar su identidad pero no tanto así la información contenida en los distintos soportes.

No podemos obviar que cuando hablamos de Blockchain nos estamos refiriendo a un libro, una base de datos en la que se introducen caracteres alfanuméricos referidos a transacciones y validados por los disntintos nodos de esta singular red descentralizada. Por lo que, sin lugar a dudas, refleja que el usuario de una Blockchain es consciente de que su interacción dentro del ecosistema va a generar una serie de intercambio de datos.

El RGPD devolvió al usuario a través de un reforzamiento del Consentimiento, el poder de decidir sober qué información, durante cuánto tiempo y para qué finalidad. Sin embargo, la cadena de bloques nación desde una perspectiva subversiva y contraria al poder establecido, reforzando el poder de los pares y huyendo de autoridades centrales, crenado sistemas democráticos, transparentes y autogestionados en las que la regla no es el consentimiento sino el consenso.[41]

[39] PERETE RAMÍREZ, Carmen. "Blockchain, Privacidad y Protección de datos de Carácter Personal". Criptoderecho, la regulación del Blockchain. 2018. Ed. Wolters Kluwer. Página 177.
[40] GARCÍA MEXÍA, P. Y PERETE RAMÍNEZ, C. " Internet y el Reglamento General de Protección de Datos".
[41] FILIPPONE, R, "Blockchain and individual´s control over personal data in European data protection law". Tilburgh University, Master Law & Technology, 2017, págs.. 32 y 33.

El Dato de Carácter Personal como elemento integrador entre ambos sistemas.

Para poder determinar si dentro del ecosistema Blockchain existe respeto o no a la normativa en materia de protección de datos, debemos de diferenciar qué tipos de información se incorpora al registro distribuido[42]. En caso de que los datos introducidos careciesen de la naturaleza de dato personal, no existiría vulneración de este derecho autónomo fundamental de protección de datos.

El art. 4.1.) RGPD define dato de carácter personal como "toda información sobre una persona física identificada o identificable. Se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular, mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física , fisiológica, genética, psíquica, económica , cultural o social de dicha persona".

Ya hemos apuntado en anteriores epígrafes relativos a la Identidad Distribuida que existen mecanismos criptográficos que podrían limitar la información facilitada por parte de un usuario de Blockchain de una manera razonablemente protectora de su intimidad sin revelar ningún dato que lo identifique.

En las distintas Blockchain se introducen datos, información, a través de distintos mecanismos.

1.- CLAVES PÚBLICAS:

Desde la entrada en vigor del RGPD, se ha superado el temor de que un usuario de Blockchain sea identificado por su clave pública. Los métodos criptográficos permiten crear tantas identidades como sea necesario sin que se revele la verdadera identidad. En este caso, la utilización de claves públicas puede considerarse como respetuoso con el RGPD.

Sin embargo, como ya advirtió el Tribunal de Justicia de la Unión Europea en la STJUE relativa al C-582/14, las direcciones IP so datos personales en determinadas circunstancias, por lo que, aquel usuario de Blockchain que utilizase su clave pública sin adoptar las medidas de seguridad suficientes, podría estar compartiendo un dato de carácter personal.
En la actualidad, para evitar esta colusión con el RGPD bastaría con utilizar una VPN y en su caso acceder a través de la red TOR para ocultar los datos relativos a la IP. Con el estado de la técnica actual, podemos considerar que no se tratarían de unas medidas desproporcionadas, habida cuenta que son los propios participantes de una Blockchain quienes deciden el grado de efectividad o intensidad de sus derechos, amparándose en la Lex Informática.

2.- FUNCIÓN HASH:

Se trata de una técnica de seudonimización de la información. La función del "hasheado" o del "hash & pepper" de la información incorporada a una cadena de bloques permite

[42] PERRETE RAMIREZ, C. "Blockchain, Privacidad y Protección de datos de carácter personal". Criptoderecho. La Regulación de Blockchain. (2018)

verificar la autenticidad de la información que inicialmente se ha incorporado a la plataforma, constituyendo una seguridad probatoria de dicha información digital. Si alguien manipulase o alterase el contenido de un documento con un hash, este sería distinto y se advertiría una vulneración de la Blockchain.
Hay que recordar que el hasheado de un documento se unidireccional y no puede revertirse[43]

El Grupo de Trabajo del artículo 29 precisa que es común entre los usuarios de la Blockchain considerar que un dato seudonimizado es 100% anónimo puesto que el estado de la técnica actual podría llevar a revelar el contenido del archivo encriptado mediante la función hash ordinario, es decir, sin la incorporación de la "pimienta"(pepper) en forma de números aleatorios incorporados al hash inicial.

De todas formas, puede concluirse que la utilización de datos hasheados es una medida diligente en aras a proteger la privacidad de los datos pero no perfecta.

3.- DATOS ENCRIPTADOS:

Los datos encriptados e incorporados a una Blockchain a priori van a adolecer de la presunción de seudonimización, es decir, de falta de anonimato al poder revertirse.

Cómo fortalecer la privacidad de los datos personales en Blockchain.

En este punto cabe preguntarnos si el Derecho Fundamental de Intimidad y Privacidad del art. 18.1 CE se encuentra en peligro cuando los usuarios utilizan una Blockchain.

La primera cuestión se ha de centrar en el tipo de Blockchain utilizada, puesto que no todas tienen el mismo nivel de ciberseguridad respecto a la privacidad de los datos incorporados a la misma.

En segundo lugar, vamos a excluir aquellas Blockchain que referencian datos alojados fuera de la Blockchain puesto que el objeto de este análisis debe centrarse en el aspecto purista de una Blockchain gobernada por el Criptoderecho.

Establece el art. 25 RGPD como exigencia para el cumplimiento de los principios de protección de datos, el diseño de cualquier sistema utilizado por una empresa o entidad debe verificarse con anterioridad para garantizar el respeto a la privacidad de los datos que vayan a tratarse.

Para que una Blockchain respete el principio de Privacidad desde el Diseño va a tener que configurar una serie de protocolos a fin de que los usuarios sepan cómo proteger los datos que se introducen.

Una de las obsesiones por parte de los ingenieros de sistemas que desarrollan en la actualidad mejoras de la tecnología Blockchain es conseguir un sistema global, descentralizado, sin intermediarios y sobre todo anónimo.

[43] Grupo de Trabajo del artículo 29. Dictamen 05/2014.

Ni Bitcoin ni Ethereum, ejemplos principales de las Blockchain Públicas no permisionadas, pueden garantizar el anonimato de las transacciones, pero sin lugar a duda con las debidas cautelas se puede conseguir.

Cierto es que como registros descentralizados donde se almacenan datos, las Blockchain se consideran un objetivo muy cotizado por parte de los ciberdelincuentes.

Un sistema descentralizado en el que no exista una autoridad central tiene por objetivo crear un ecosistema de confianza entre sus usuarios. Los individuos no eligen realizar transacciones en una red Blockchain porque pretendan realizar algo ilegal, sino porque buscan defender su privacidad.

Sin embargo, la tesis que acerca al RGPD y la Blockchain se encuentra en la propia consideración y valor que se otorga al dato de carácter personal.

Una Blockchain Pública como Bitcoin no es anónima, pero, al contrario que ocurren con las organizaciones centralizadas como los Bancos centrales, no está interesado en la información contenida en su libro mayor ni comercia con dichos datos. Hay que recordar que Blockchain está desarrollado en Código Abierto y tiene un carácter altruista.

El anonimato queda desprotegido en ciertas cadenas de bloque de rebote, pero, con la adopción de una serie de buenas prácticas los usuarios podrán asegurarse una debida protección de su privacidad.

Centrando este estudio de la fuga de información de las cadenas de bloques en posiblemente la Blockchain más famosa, podemos apuntar que estas se pueden producir de las siguientes maneras:[44]

- Crear un monedero ("wallet") de Bitcoin es relativamente sencillo y no exige tener conocimiento informáticos ni de criptografía.
- Las transacciones que han sido verificadas en Bitcoin desde su creación en 2009 están disponibles para todo el mundo. Otra cosa es que descrifrar el contenido de los bloques tenga sentido o sea sencillo.
- El monedero de Bitcoin es una clave pública, un código alfanumérico que actúa como un pseudónimo para el resto de usuarios. Esta situación genera una relativa incertidumbre.
- El Big Data y los Algoritmos y potencialmente la Tecnología Cuántica va a cambiar los estándares de seguridad de todos las tecnologías vigentes de internet, tanto las centralizadas como las descentralizadas.

Concretamente los puntos de fuga de información de carácter personal en una Blockchain van a ser:

1- La dirección IP desde la que un usuario realiza a través de su wallet una transacción en Bitcoin, Ethereum u otra.
Ya hemos dicho que de acuerdo con el Grupo del Artículo 29, las Direcciones IP son datos de carácter personal.

[44] https://academy.bit2me.com/bitcoin-no-es-anonimo/

2- La utilización de monederos poco seguros: La utilización de un servicio web de monederos expone la privacidad de sus clientes los cuales en su registro, fuera de la Blockchain, introducen sus datos de carácter personal y podría producirse fácilmente una fuga de información.
3- La compraventa de criptomonedas en Exchangers poco seguros.

A pesar de todos estos inconvenientes, la regulación en materia de Protección de datos y las medidas técnicas que pueden ser implementadas por una Blockchain para su adecuación y respeto a estos derechos fundamentales es viable y factible.
La adopción de unas buenas prácticas, el conocimiento de la tecnología y un fortalecimiento de los protocolos va a ser esencial en el futuro de la tecnología Blockchain no solo en lo referente a las criptomonedas, objeto de ciberdelitos debido al contenido económico de los mismos, sino en el caso de los criptocontratos o contratos inteligentes porque estos contienen datos de carácter personal mucho más desarrollados e incluso pueden contener diversas obligaciones o reconocimientos de derechos que en caso de su exposición pueden causar un verdadero menoscabo en los titulares.

Medidas de ciberseguridad en una Blockchain:

A.- Utilización de VPN: La utilización de una red virtual privada permite conectar dos nodos de forma segura. Esto posibilita enrutar todas las comunicaciones en una red Blockchain: se podría enmascarar la IP.
Dentro de unas buenas prácticas en materia de ciberseguridad, el usuario debería utilizar una VPN de pago o configurada ad hoc, puesto que la mayoría de empresas que ofrecen estos servicios podrían traficar con los datos albergados en su red virtual.

B.- Utilización de TOR: La utilización de este software permite implementar varias capas de seguridad en la navegación.

C.- Utilización de Mezcladores: se trata de servicios que mezclan bitcoins de un usuario con los de otro antes de que lleguen a su destino. Las transacciones se fragmentan y el destinatario tiene el mismo valor pero desde varios usuarios.

La Elección en tutela de los Derechos Fundamentales

La tutela de los Derechos Fundamentales de las personas va a ser diferente dependiendo si los usuarios la buscan a través del poder coercitivo del Estado o en el Criptoderecho.

La tutela de los Derechos Fundamentales por parte del Ordenamiento Jurídico establece una serie de límites en el ejercicio de los mismos como el correspondiente a la ponderación de dos derechos en colisión y el acceso a los Juzgados y Tribunales para hacer valer cualquier tipo de menoscabo.

Por lo tanto se genera entre los usuarios de blockchain una crisis en relación con el Derecho aplicable al ofrecer la posibilidad de aplicar por un lado el derecho criptográfico creado en un criptocontrato, y por otra parte el Derecho tradicional “offline” en el que se garantiza la tutela de los derechos y libertades fundamentales.

La coexistencia de dos normativas dentro de la esfera de Blockchain va a implicar que el usuario tenga que tomar una decisión consistente en asumir que dentro Blockchain ciertos derechos fundamentales van a ser expuestos y se van a regular por la Ley Criptográfica, especializada y adaptada a la realidad de dicho ecosistema, o no usar dicha tecnología.

En caso de que el usuario asuma los riesgos de la utilización de Blockchain, va a tener que considerar un doble escenario:

Si la tecnología Blockchain sigue su actual crecimiento y su uso llega a ser indispensable dentro de Interntet, la legitimidad de los Limites a los Derechos Fundamentales tendría que ser cuestionada de la manera que lo planteó Rober Novick no existe en la actualidad una capacidad dispositiva de los ciudadanos para decidir si se aplica el Estado de derecho o el derecho Criptografico.

3.3 BLOCKCHAIN Y EL DERECHO AL OLVIDO.

Otro de los Neoderechos Digitales reconocidos en nuestro Ordenamiento Jurídico que pueden entrar en conflicto con las características de la Tecnología Blockchain es el llamo Derecho Al Olvido ("Right to be Forgotten").

La repercusión y alcance del Derecho al Olvido en la sociedad actual ha tenido un crecimiento exponencial en las últimas décadas, más aún a partir de 2010 con el auge de las redes sociales y otras tecnologías en las que el usuario inconscientemente ha enriquecido mediante la subida de datos de carácter personal como fotografías, textos, números de teléfono, datos de filiación, gustos, aficiones, …. Un almacenamiento de datos en servidores centralizados y radicados en empresas concretas.[45]

Este Derecho Fundamental tiene su desarrollo actual en el art. 18.4 CE en relación con los apartados 1 y 2 del mismo artículo referentes a la Privacidad pero también y de una manera intensa al Derecho a la Dignidad Humana previsto en el art. 10 CE, tal y como defiende el Tribunal Constitucional en la STC 292/2000, de 30 de noviembre, que ubica a este derecho dentro de la Carta Magna de una manera integrada y compleja.

Este nuevo derecho fundamental Digital por fin ha sido positivado en los artículos 16 y 17 del Reglamento 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos con un carácter innovador y posteriormente transpuesto en la normativa española en los artículos 93 y 94 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de Derechos Digitales.

La mayoría de la doctrina ha venido configurando e interpretando este derecho mayoritariamente desde el punto de vista de las Redes Sociales y de los Buscadores de Internet, pero tal y como advirtió el profesor R. Carr "asistimos en la actualidad a una vertiginosa proliferación de herramientas tecnológicas que alteran nuestra forma de concebir nuestra relaciones sociales, e incluso en ocasiones en el modo de percibir la

[45] COCHACHO LÓPEZ, A. "Reglexiones en torno a la última actualización del derecho al olvido digital. Revista de Derecho Político. Universidad Nacional de Educación a Distancia. (2019) Nº 104 enero-abril. Páginas 197 y ss.

realidad".[46] Por supuesto, dentro de estas nuevas tecnologías que afectan a los derechos fundamentales, y en concreto el derecho al olvido en Internet irrumpe con fuerza la tecnología Blockchain.

Dentro de Internet "la memoria es la regla, el olvido la excepción"[47] puesto que en él se preserva todo y se convierte en un presente continuo. La doctrina igualmente invoca la teoría del eterno retorno de Nietzsche para plantear este problema que afecta por igual a todo el mundo. Autores como Mayer Schönbenger han equiparado la perpetuidad de la información fijada en internet a un tatuaje[48]

¿Ha previsto el RGPD el derecho al olvido respecto a Blockchain?

La Agencia Española de Protección de Datos ha definido este derecho como "la manifestación de los tradicionales derechos de cancelación y oposición aplicados a los buscadores a internet. El derecho al Olvido hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumpla los requisitos de adecuación y pertinencia previstos en la normativa. En concreto el derecho a limitar la difusión universal e indiscriminada de los datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima (es decir, la que conste en Boletines Oficiales o en informaciones publicadas en medios de comunicación amparadas en el derecho fundamental del art. 20 de Libertad de Expresión o de Información)"[49]

El carácter inmutable y no editable de los bloques supone que los datos personales incorporados a Blockchain no van a poderse modificar o eliminar lo cual choca con los principios reconocidos por la nueva regulación europea.

Ya hemos visto en el apartado anterior del capítulo que el RGPD configura la protección de la privacidad del individuo desde de un punto de vista "user-center" mientras que Blockchain otorga esta protección de una manera descentralizada en la que una red de iguales y anónima protege esta identidad, basada en un sistema que a priori refuerza el acceso a los datos con el uso de la criptografía. Sin embargo, ya hemos visto que el RGPD no se detuvo en analizar las especialidades de esta tecnología distribuida.

Esta tensión relativa a la durabilidad o limitación de los datos de carácter personal almacenados en una base de datos distribuida es enorme, en tanto y cuanto Blockchain se a erguido como una tecnología resistente frente a la censura digital.[50]

Ya hemos analizado con carácter general al derecho de protección de datos que las tecnologías venideras basadas en la Cuántica, así como el crecimiento exponencial del Big Data en un sistema de gestión de la información centralizado en grandes servidores

[46] CARR, r. (22017. ¿Qué está haciendo Internet con nuestras mentes? Superficiales, Barcelona, Taurus.
[47] SIMÓN CASTELLANO, P. (2012) "El derecho al olvido en el universo 2.0". Textos universitaris de biblioteconomía i documentació, núm 28, p.1.
[48] MAYER-SCHÖNBERGER, V (2009). Delete: The Virtue of Forgetting in the Digital Age, Princeton, Princeton University Press, p 2.
[49] AEPD https://www.aepd.es/portalwebAGPD/canaldelciudadano/derecho_olvido/index-ides-idphp.php (ultima consulta el 3 de julio de 2020)
[50] FINK, Michéle. "Law and Autonomous Systems Series: Blockchain and the Right to be Forgotten". University of Oxford, 2018.

en la nube, el poder de los indexadores de los buscadores de las grandes compañías como Google, Amazon, Microsoft o Apple, van a amenazar las medidas de anonimización o pseudonimización que la tecnología Blockchain se está esforzando en desarrollar.

Papel de las Legislaciones nacionales.

Existe por lo tanto un vacío legal respecto al encaje de la tecnología Blockchain y el derecho al olvido tal y como se ha regulado por parte del Reglamento General de Protección de datos.

Algunos expertos plantean como solución que la legislación nacional de cada Estado miembro de la Unión Europea limite el alcance del derecho al olvido en los sistemas Blockchain, lo cual no está exento de dificultades tecnológicas y de contradicciones jurídicas, aparte el riesgo de nueva fragmentación en la forma de regular este derecho, que es lo que el RGPD pretende superar.

Este vacío legal no ha sido resuelto ni por parte de la doctrina ni por la Jurisprudencia, aunque parece que debido a la evolución en la utilización de protocolos P2P en el ámbito empresarial y financiero a través de las criptodivisas y proliferación de contratos inteligentes cada vez más complejos, no tardará en plantearse un intento de control del estado de derecho sobre esta tecnología para su encaje en el respeto de los derechos fundamentales.

Otros especialistas sugieren la posibilidad de desarrollar cadenas editables que permitan a uno o varios administradores reescribir o cambiar bloques de información de posición sin alterar la totalidad de la cadena, con el consiguiente peligro de falta de transparencia y de inseguridad jurídica, por cuanto estaríamos hablando de otra tecnología diferente a Blockchain por cuanto quiebra sus principios esenciales.

Posibles conflictos entre derechos fundamentales dentro de la Blockchain

La tecnología Blockchain cambia el status quo en la protección de los derechos fundamentales puesto que se va a convertir en un potenciador de algunos derechos fundamentales como el Derecho a la Libertad de Expresión del art. 20 de la Constitución Española, pero sin embargo va poner en peligro otros derechos como son los derechos contenidos en el art. 18 de la Constitución como el Derecho a la Privacidad, a la Intimidad, a la Propia Imagen, y al derecho al honor.

Blockchain solo va a poder proteger los derechos fundamentales que los usuarios en la manera en que se hubiese configurado un criptocontrato, pero no va a poder ampliar la tutela de estos en caso de infracciones que tuviesen sus efectos fuera de dicho ecosistema en el caso de que vulnerasen derechos de un tercero.

La razón de esta falta de ejecutividad o protección de la Ley Criptográfica fuera en la vida real se basa en el anonimato del presunto infractor del derecho de un tercero reforzado por el carácter descentralizado de la ley que impide poder accionar contra el usuario. La información que se ha introducido en la red no se puede modificar.

Por lo tanto se cumple el axioma según el cual "una persona puede reclamar una compensación por la vulneración de un derecho fundamental por parte de un infractor pero jamás podrá ejecutarla porque no conoce la clave privada del infractor ni puede ser compensado económicamente"[51]

En este sentido, todo derecho fundamental que sea vulnerado dentro de una Blockchain va a tener muy difícil obtener su tutela.

En el caso de que un usuario publique información de carácter personal de un tercero en una Blockchain y que dicha difusión causase un daño al violar su intimidad personal o su privacidad, va a ser imposible, una vez validado dicho bloque borrar dicha información o cancelarla, incluyo en el caso remoto de que el perjudicado descubriese la identidad del infractor.

Por estas razones ni el poder judicial de los estados a través de sus juzgados y tribunales ni un sistema de autorregulación integrado dentro de una Blockchain va a ser suficiente para obtener una solución.

La utilización de la tecnología Blockchain va a implicar un nuevo paradigma en el que los usuarios, desde el momento que acceden a esta tecnología, van a decidir si disponen o no de la tutela sobre sus derechos fundamentales en caso de que sean menoscabados por un tercero.

3.4. DERECHO A LA TUTELA JUDICIAL EFECTIVA

El artículo 79 LOPDGDD introduce el Título X con una declaración de intenciones llamada a reconocer una serie de garantías a los Derechos nacidos en la Era Digital. En este sentido, establece que "los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en internet. Los Prestadores de Servicios de la Sociedad de la Información y los Proveedores de Servicios de Internet contribuirán garantizar su aplicación."

El Derecho a la tutela Judicial efectiva, reconocido en el art. 24 de la Carta Magna española establece el acceso de los ciudadanos a obtener una protección por parte de Juzgados y Tribunales a través de un procedimiento justo, legal, sin dilaciones indebidas y con una serie de garantías procesales y de representatividad y asesoramiento por parte de especialistas que salvaguarden la integridad de este.

La tecnología Blockchain, tal y como hemos estudiado a lo largo del presente trabajo plantea una revolución en la forma de relacionarse sin necesidad de intermediarios, basándose en un sistema de confianza asegurado por la criptografía y la verificación de las transacciones.

Una de las características de la Blockchain y concretamente de los contratos inteligentes como paradigma del criptoderecho es el carácter autoejecutivo e inmutable de los mismos

51 T. SCHREPEL, Thibault. "Anarchy, State, and Blockchain Utopia: Rule of Law versus Lex Cryptographia" in *General Principles and Digitalisation*, Hart Publishing. 2020.

una vez se hayan perfeccionado. ¿Podría entrar a valorar un Juzgado o Tribunal la validez de un criptocontrato? ¿Pueden denunciar los usuarios de una Blockchain la vulneración del derecho de tutela judicial efectiva en caso de que los Juzgados se declarasen para conocer de un contrato regulado por la Ley Criptográfica?

El auge de la tecnología Blockchain y sus posibilidades de agilizar las transacciones y de resolver los conflictos a través de la inclusión de cláusulas arbitrales al margen de la Tutela Judicial Efectiva de Juzgados y Tribunales crea sin lugar a duda un problema en materia de uniformidad a la hora de resolver una misma situación de hecho.

Sin embargo, esto plantea una posibilidad no de conflicto sino de elección por parte del ciudadano que renuncia a obtener la protección jurídica de un método heterocompositivo de solución de conflictos, centralizado y revestido de Autoridad y Fuerza Constitucional por unas clausulas preconfiguradas en Código dentro de un Smart Contract.

Estos dos ecosistemas permiten a la sociedad revelarse bien complementarias en tanto y cuanto Blockchain respeta el Estado de Derecho o de forma independiente en la que las relaciones jurídicas surgidas, desarrolladas y ejecutadas dentro del ecosistema Blockchain carecerían de la coerción estatal y únicamente serían reguladas por el Código informático.[52]

Robert Nozick en su libro "Anarquía, Estado y Utopía" defendía que las personas tratan de vivir en varias comunidades, se adaptan a ellas o intentan cambiar lo que lo les gusta. Algunas comunidades van a ser abandonadas, otras sufrirán este camino de adaptación, otras se quebrarán y desaparecerán, y otras aprovecharán las nuevas oportunidades y florecerán, duplicando su poder. Las comunidades son libres de evolucionar y debería existir ninguna imposición por parte de ninguna autoridad siempre que todos sus miembros se hayan adherido voluntariamente a un Código".

Sin lugar a duda, esta visión utópica de la resolución de conflictos por parte del autor estadounidense provoca una colisión con los Estados Sociales y Democráticos de Derecho al prescindir de las autoridades judiciales.

Desde un prisma jurídico, y ante un Juzgado o Tribunal, una transacción incluida en una cadena de bloques se encuentra dentro de la legislación nacional en materia de contratos, tanto civiles como mercantiles, y que se refiere a acuerdos entre usuarios (partes) en las que la secuencia del código utilizado en la Blockchain no deja de ser un elemento más de un contrato sinalagmático y complejo. Es decir, "el código no constituye un contrato, pero sí responde a un acuerdo que le da sentido y al que sirve de expresión".[53]

La utilización de Blockchain como evidencia digital.

Otro de los elementos configuradores de la tutela judicial efectiva se encuentra el derecho fundamental procesal del "Proceso con todas las Garantías".

[52] NOZICK, Robert. "Anarchy, State, and Utopia." .Basic Books, 1974

[53] LEGREN-MOLINA, Antonio, "Los contratos Inteligentes en España. La disciplina de los Smart contracts". Revista de Derecho Civil vol. V, número 2.(abril-junio) págs. 193-241. Consultado a través de http: //nreg.es/ojs/index.php/RDC.

El grupo de trabajo en materia de ciberseguridad del Consejo General del Poder Judicial(CGPJ) lleva varios años trabajando en la integración de la Blockchain en la Administración de Justicia, no solo desde el punto de vista organizativo, en el que se ha planteado la creación de Blockchains privadas permisionadas y con utilización de figuras de confianza externa, Oráculos, que podrían recaer en Funcionarios de la Administración de Justicia como Letrados de la Administración de justicia (LAJs) o los propios Jueces y Magistrados.

Los objetivos de privacidad, confidencialidad, trazabilidad y alto grado de seguridad criptográfica atraen al ecosistema legal fuera de Blockchain de tal forma que el Derecho a la Tutela Judicial efectiva y Blockchain podrían integrarse dependiendo del tipo de cadena de bloques que se pretenda utilizar.

El mayor problema con el que se encuentran los Juzgados y Tribunales ante la información contenida en una Blockchain es la inmutabilidad, debido a que una vez verificado e incorporado a la cadena de bloques, esa transacción no puede modificarse.

Para evaluar el valor de la Blockchain como evidencia digital que pueda ser utilizada en un proceso debemos tener en cuenta las tres fases de verificación de este protocolo:

1) La Prueba de Integridad (Proof of Integrity), es decir, que el contenido se mantenga inmutable
2) La Prueba de la Existencia (Proof of Existance), el sellado del tiempo
3) La Autoría de los intervinientes.

Si un documento digital incorporado a un procedimiento judicial basado en la tecnología Blockchain cumpliese estos tres requisitos, hablaríamos de un documento público.

Sin embargo, el art. 319 LEC requiere tres elementos a fin de considerar que un documento tiene esta consideración de documento público: El hecho, acto o estado de las cosas; la fecha de emisión; y la identidad de los intervinientes.
La cadena de bloques, por otro lado, quedaría encajada en el art. 317 LEC, en la que el contenido puede venir protegido por alguna de las técnicas que se han explicado en el apartado de criptografía, es decir, un hash simple, un “hash & pepper”.

La utilización de la Identidad Distribuida en la que un usuario de Blockchain únicamente comparta ciertos aspectos de su personalidad con la entidad verificadora correspondiente, otorgaría un alto grado de seguridad a la Administración de Justicia a la hora de valorar un documento probatorio en formato Blockchain, como por ejemplo un Smart contract.

Para que un Smart Contract o la compra de una criptomoneda fuese un documento público se debería confirmar los requisitos del art. 319 LEC. La Ley de Enjuiciamiento Civil establece en un numerus clausus cuales son documentos públicos: documentos administrativos, judiciales o notariales. En la actualizad ya existen voces que reconocen a la Blockchain el carácter de documento público.[54]

[54] RÍOS, Yolanda. Magistrada del Juzgado de lo Mercantil de Barcelona. “Webinar Administración de Justicia y Blockchain” celebrado el 7 de mayo de 2020.

El Grupo de Trabajo del CGPJ ha determinado lo siguiente:

- La Blockchain no cumple estrictamente los tres elementos necesarios para establecer la naturaleza de documento público del art. 318 LEC.
    - El contenido de la prueba puede ser un hash: Las partes procesales deben aportar el hash así como la traducción a través de un informe pericial que traduzca el contenido cifrado.
    - La fecha es el sellado de tiempo: es autentica por la propia naturaleza de las Blockchains.
    - El principal problema respecto a la validez es el relativo a la identidad IDENTIDAD:

Lo ideal sería atribuir ciertas notas regladas o protocolizadas a las cadenas de bloques para que el que pudiera operar lo hiciera con cierta confianza.

Finalmente, y de acuerdo con la normativa actual y dentro del Proceso, los archivos provenientes de Blockchain solo van a poder ser admitidos como prueba dentro de las categorías de Documento Privado y como Prueba Pericial.

3.5 BLOCKCHAIN EN EL MARCO EUROPEO

La Comisión Europea es conocedora de las bondades de una tecnología transformadora de la economía y de los derechos de los ciudadanos. En este sentido en el año 2018 puso en marcha el "Observatorio y Foto de la Cadena de Bloques de la UE" (European Blockchain Observatory and Forum [55] con la finalidad de impulsar las iniciativas relevantes en esta tecnología, así como analizar los riesgos y tendencias en materia de Legaltech, Fintech basada en tecnología Blockchain.

Esta función de asesoramiento e impulso a la Blockchain en Europa ha sido apoyada por el propio Parlamento Europeo, que comenzó publicando un primer informe en febrero de 2017 titulado "Cómo puede cambiar nuestra vida la tecnología de bloques"[56] en el que se centraba el estudio en el impacto de esta tecnología en materias como Propiedad Intelectual e Industrial o incluso en el voto electrónico.

La Comisión Europea es consciente de las fricciones existentes entre la reciente legislación aprobada en 2016 con el RGPD (vigente desde 25 de mayo de 2018) y la tecnología Blockchain generando una incertidumbre jurídica que juega en contra del desarrollo de una tecnología con infinitas posibilidades a la hora de mejorar los canales institucionales y el funcionamiento de ciertos procesos en la sociedad actual .

En este sentido, la propia Comisión indica que "Primero y principalmente, Europa necesita aclarar el marco regulatorio. Es un objetivo prioritario resolver las tensiones

[55] Los objetivos fijados por este Observatorio son el impulso en la innovación y desarrollo del econsistema Blockchain dentro de la UE, y asudar a cimentar la posición europea como uno de los lideres mundiales en la transformación propuesta por esta tecnología. Ver https://www.eublockchainforum.eu/about

[56] BOUCHER, Phillip. "*Cómo puede cambiar nuestra vida la tecnología de la cadena de Bloques*". EPRS – SERVICIO DE ESTUDIOS DEL PARLAMENTO EUROPEO- Unidad de Previsión Científica (STOA). 2017.

actuales entre el RGPD y Blockchain. La legalidad, fiscalidad y contabilidad de los criptoactivos (tokens) debe ser aclarado, así como cualquier cuestión concerniente a su mercado y relación con el Euro."

La Comisión Europea es consciente que a nivel internacional Gobiernos como el Chino están elaborando un proyecto de cadenas distribuidas de bloques así como la transformación de la divisa china, el Yuan, en una moneda virtual, avalada y respaldada por el Banco Popular Chino.

Recientemente, en Abril de 2020, el Gobierno Chino ha anunciado el éxito de dos importantes iniciativas basadas en Blockchain y Tecnología Criptográfica. La primera de estas iniciativas consistió en la introducción en cuatro ciudades del país la utilización de una moneda digital estatal, el DCEP, con un resultado muy prometedor.

El segundo proyecto desarrollado con éxito por China está relacionado al establecimiento de un Servicio de Red basado en tecnología Blockchain, denominado BSN, que a fecha actual está en pleno funcionamiento.

China ha puesto su objetivo en el año 2035 para cumplir con sus objetivos de implementar esta tecnología en todos los sectores tecnológicos que tendrán no solo repercusión en el sector legal y financiero, sino también en el propio desarrollo tecnológico como sucede en el campo de las telecomunicaciones y la Inteligencia Artificial.[57]

En este sentido, se plantean varias opciones[58] para afrontar en el seno de la Unión Europea para poder un paso adelante y no quedarse atrás en la carrera regulatoria de una tecnología que ha quedado fuera de la regulación del ambicioso proyecto del Reglamento General de Protección de Datos.

A.- INTRODUCIR EXCEPCIONES DENTRO DEL RGPD PARA ADAPTARLAS A LA REALIDAD BLOCKCHAIN:

Existen voces en la comunidad tecnológica y jurídica europea que están reclamando a la Comisión y al Parlamento una flexibilidad regulatoria respecto a esta normativa consistente en introducir exenciones respecto a las exigencias impuestas por el Reglamento a los Responsables y Encargados de Tratamiento de Protección de datos, cuando se trate de entornos Blockchain.

Esta opción podría justificar una ruptura en la neutralidad tecnológica fijada por el RGPD que busca una uniformidad en la materia por razones de especial trascendencia.

[57] MAGAS, Julia " Top facts on China´s Crypto Yuan and related Blockchain Proyects. Publicación digital en COINTELEGRAPH https://cointelegraph.com/news/top-facts-on-chinas-crypto-yuan-and-related-blockchain-projects

[58] PERETE RAMÍREZ, C. *"Blockchain, Privacidad y Protección de datos de Carácter Personal"*. Criptoderecho, la regulación del Blockchain. 2018. Ed. Wolters Kluwer. Páginas 211-212.

B.- APROBACIÓN DE UNA NORMATIVA ESPECÍFICA EUROPEA EN BLOCKCHAIN.

El objetivo de esta potencial regulación debería ser una ordenación integral de esta tecnología para crear un marco jurídico confiable en en los mercados de criptodivisas cuyo volumen está creciendo en la actualidad.
Liechtenstein ha aprobado el 3 de octubre de 2019 la "Ley sobre Tokens y de Proveedores de Servicios TT" [59]en cuyo artículo 1 establece los objetivos de la misma:

Artículo 1:

1) *Esta ley establece el margo legal para todas las transacciones basadas en Tecnología de Confianza ("Trustworthy Technology") y en partigular regula:*
    a. *Las bases legales en derecho civil relativas a Tokens y derechos de representación reconocidos en los Tokens y en sus transferencias*
    b. *La Supervisión y derechos de las Obligaciones de los Proveedores de Servicios TT*
2) *El objetivo será:*
    a. *Proporcionar confianza en las comunicaciones legales digitales en el sector financiero y económico, así como la protección de los usuarios de los Sistemas TT.*
    b. *Fomentar la creación marco legal neutral con base a una tecnología neutral basada en la excelencia e innovación para organizar los servicios y sistemas TT.*

C.- MANTENER EL RGPD COMO ÚNICO MARCO REGULATORIO DE LA U.E:

Sin lugar a dudas esta es la opción más conservadora, en la que se mantendría el RGPD como una norma transversal y tecnológicamente neutra respecto al tratamiento de datos de carácter personal .
De optar por esta vía, la utilización de la tecnología Blockchain derbería adecuarse irremediablemente a los principios fijados por el Reglamento en perjuicio del desarrollo tecnológico y valor añadido que ofrece Blockchain.

En este caso, la doctrina mayoritaria, tal y como establece la Profesora Perete Ramírez, sería necesario que el Comité Europeo de Protección de Datos, vía art- 70 estableciese un marco regulatorio para los ciudadanos y empresas europeas en el desarrollo de la tecnología Blokchain, en aras al mantenimiento de la seguridad jurídica.[60]

La preocupación por tanto, en el seno de los expertos europeos en materia legal y tecnológica se encuentra en que Europa quede atrás en el desarrollo de la tecnología al haber aprobado una regulación que restringe y condiciona el desarrollo de cualquier

[59] Law of 03 October 2019 on Tokens and TT Service Providers (Token and TT Service Provider Act; TVTG). Liechtenstein Legal Gazette. En vigor desde el 1 de enero de 2020.

[60] PERETE RAMÍREZ, C. *"Blockchain, Privacidad y Protección de datos de Carácter Personal"*. Criptoderecho, la regulación del Blockchain. 2018. Ed. Wolters Kluwer. Página 212.

tecnología basada en la descentralización de la información y en la criptografía y que aboga, por el contrario, por una Normativa neutra en defensa del usuario centralizado, tal y como hemos visto en este capitulo, dejando la tutela de los Derechos Fundamentales únicamente en manos de las autoridades centralizadas sin permitir ningún tipo de concesión al desarrollo de Blockchain.

CONCLUSIONES

El estudio realizado sobre el impacto de la tecnología Blockchain sobre los Derechos Fundamentales de los ciudadanos ha buscado arrojar algo de luz así como tender puentes entre dos regulaciones condenadas a entenderse.

He abordado el problema regulatorio porque para entender esta tecnología distribuida, disruptiva y basada en la búsqueda utópica de la Privacidad y el no sometimiento a ningún tipo de autoridad central surge un constante desafío al Estado de Derecho y a la Regulación de las relaciones humanas tal y como las conocemos en la actualidad.

Internet ha supuesto una nueva revolución industrial en la que el factor humano va a ser decisivo no desde el punto de vista mecánico y lineal que teníamos en el siglo XIX con el nacimiento de la producción en cadena, sino una posición innovadora, inspiradora y creativa que nos permita interactuar con la tecnología de una manera más eficiente. Esto sin duda nos va a suponer un cambio en el paradigma.

Cuando comencé a estudiar y a buscar información sobre la tecnología Blockchain como jurista me aparté de la búsqueda de las bonanzas financieras, de activos volátiles, de mercados secundarios propios de las Fintech para acercarme a las implicaciones más profundas de esta tecnología en las personas.

Un defensor de Blockchain defiende el anonimato, defiende la comunidad y la autoregulación basada en un factor muy olvidado en la sociedad actual: la confianza.

Sin embargo, tal y como hemos analizado a lo largo de estos dos largos capítulos, el Estado de Derecho y el Criptoderecho pugnan dentro de sus propios ecosistemas por tener el control de las relaciones que surgen entre usuarios de la tecnología Blockchain.

Esta situación regulatoria pretende pasasr el testigo al usuario para que sea él quien elija cual de los dos sistemas es más ventajoso para él, como si un usuario medio tuviese el conocimiento suficiente para saber si su libre disposición de sus derechos es así.

La situación regulatoria actual no permite a los individuos ejercer de sus derechos de una manera paralela a la prevista en el Ordenamiento Jurídico dentro de una Blockchain en el desarrollo de transacciones económicas u otro tipo de negocio jurídico.

Coincido con la mayor parte de la doctrina que he mencionado en este trabajo en lo relativo a que la regulación en materia de protección de datos de carácter personal por el RGPD europeo ha supuesto un paso adelante pero que es incompleta y no permite una adaptación a las nuevas tecnologías que se apartan de una noción centralizada.

Lo primero que tenemos que tener claro a la hora de analizar la tecnología Blockchain y su protección a los Derechos Fundamentales de las personas es que su protección va a depender del tipo de Blockchain que se utilice:

Una Blockchain Pública y no permisionada es la plataforma menos respetuosa con una protección adecuada de los Derechos Fundamentales porque lleva a los extremos el

ejercicio de los mismo. Por una parte, utiliza el cifrado para proteger la identidad de los usuarios a través pero los datos introducidos en la Blockchain, al ser inmutables una vez se han incorporados a un bloque, quedan expuestos para siempre sin posibilidad de edición. En este caso, nunca podríamos ejercer una Ponderación de Derechos Fundamentales en caso de confrontación del Derecho de Libertad de Expresión y el Derecho de Intimidad, en el caso de que se introdujese información de un tercero.

En el momento en que empezamos a implementar el uso de plataformas Blockchain Privadas y permisionadas, en las que los usuarios acceden conociendo una serie de reglas previamente configuradas y aceptadas por los miembros, esa sobreexposición o potencial vulneración de derechos fundamentales se encuentra más controlada.

Una de las mayores críticas realizadas por parte de la Doctrina hacia la utilización de Blockchain ha sido el nulo respeto al derecho al olvido debido al carácter inmutable de los datos incorporados a la cadena de Bloques.

El Derecho al Olvido se encuentra protegido en nuestra Constitución española tanto por el derecho a la dignidad humana como por el derecho autónomo de protección de datos y fue pensado y configurado en relación con sistemas de almacenamiento de información centralizado como Indexadores de Información en Buscadores Online, Hemerotecas, y sobre todo en las Redes Sociales.

Considero que la vulneración al derecho al olvido por parte de Blockchain es mínima e irrelevante por dos motivos:

- Blockchain es un sistema distribuido en el que la información almacenada en el libro mayor es introducida por consenso de todos sus miembros y el acceso a la misma no está igual de expuesto que un navegador ni una red social.
- La tecnología Blockchain está basada en la confianza y en las buenas prácticas de sus usuarios. La información subida relativa a transacciones está cifrada y las direcciones de los monederos no revelan una identidad.

El respeto de los derechos fundamentales dentro de la tecnología Blockchain viene determinado en un primer momento por la propia seguridad del protocolo, y en este caso se cumple. Blockchain es una tecnología segura, transparente y con muchos más procesos de verificación que el resto de nuevas tecnologías no distribuidas, es decir, centralizadas que se utilizan en la actualidad y que operan en Internet.

En este punto, lo crucial es la adopción de una serie de buenas practicas por parte de los usuarios de Blockchain para una mayor garantía de los derechos fundamentales que se ponen en juego en las transacciones realizadas como son la utilización de medios criptográficos avanzados, la conexión a través de VPNs, protección de las claves privadas de los monederos, …. Y sobre todo no introducir datos personales no cifrados dentro de una cadena de bloques.

Sin lugar a duda, el mayor desafío al que se enfrentan las Autoridades Nacionales e Internacionales es la de adaptar la Tecnología Blockchain a su marco regulatorio como un instrumento en su beneficio pese a que ello suponga una renuncia en el control sobre los ciudadanos.

Tal y como he apuntado en el último aparatado del capítulo referente al marco regulatorio de la UE es que Europa quede rezagada en la carrera mundial por adaptar esta tecnología disruptiva en beneficio de los derechos de los ciudadanos.

Desde el año 2017, la Comisión Europea a través de su Observatorio y Foro dedicado a Blockchain, ha advertido las bondades que esta tecnología puede traer en la protección de derechos fundamentales de las personas como el Derecho Fundamental de Participación Política a través del polémico voto electrónico pero también en defensa de la Propiedad Intelectual, materia en la que actualmente el Parlamento ha aprobado la Directiva (UE) 2019/790 de los Derechos de Autor.

Blockchain es un entorno con infinitas posibilidades para poder ayudar a la Regulación en la protección de los derechos fundamentales a través de la creación de un marco legal seguro. Por eso es necesario que cualquier tipo de movimiento regulatorio sea flexible y adaptativo para poder respetar las especialidades de una tecnología distribuida en la que el anonimato, la transparencia y la ciberseguridad son sus razones de ser.

BIBLIOGRAFÍA

Libros y Revistas Jurídicas

BOUCHER, P. "*Cómo puede cambiar nuestra vida la tecnología de la cadena de Bloques*". EPRS – SERVICIO DE ESTUDIOS DEL PARLAMENTO EUROPEO-Unidad de Previsión Científica (STOA). 2017.

CASEY, M.J y VIGNAM, P. *"In Blockchain We Trust",* MIT technology Review, volume 121, nº 3, p.10-16. 2018

DE FILIPPI, P y WRIGHT, A. *"Blockchain and the law. The Rule of Code".* Harvard University Press. 2018

FILIPPONE, R, "Blockchain and individual´s control over personal data in European data protection law". Tilburgh University, Master Law & Technology, 2017, págs.. 32 y 33.

FINK, M.. "Law and Autonomous Systems Series: Blockchain and the Right to be Forgotten". University of Oxford. 2018.

GARCÍA MEXÍA,P. (Director). "*Del ciberderecho al criptoderecho. La Criptoregulación",*. La Ley - Wolters Kluwer. 2018

GARCÍA MEXÍA, P. Y PERETE RAMÍNEZ, C. *"Internet y el Reglamento General de Protección de Datos"*. La Ley - Wolters Kluwer. 2018.

GLIBIN, R., *"The P2P Wars: How Code Beat Law,"* . IEEE Internet Computing, vol. 16, no. 3, pp. 92-94, May-June 2012.

LEGREN-MOLINA, A., "*Los contratos Inteligentes en España. La disciplina de los Smart contracts".* Revista de Derecho Civil vol. V, número 2.(abril-junio) págs. 193-241. 2018. Consultado a través de http://nreg.es/ojs/index.php/RDC.

LESSIG, L., (2001) "*Code and Other Laws of Cyberspace"*. Editorial Basic Books.

MAUPIN, J.A, *"Blockchains and the G20: Building an Inclusive Transparent and Accountable Digital Economy".* Center for International Governance Innovation Policy Brief bº 101, Center for International Governance Innovation. 2017

MAZZONE, C. "*Presentation of the EU Blockchain Observatory and Forum".* Blockchain Innovation in Europe. Simposio celebrado en Viena el 22 de mayo de 2018,

MERKLE, R.C *"Protocols for public key cryptosystems".* Proc. 1980 Symposium on Security and Privacy. IEEE Computer Society, pp. 122-133.

NARAYANAN, A. y CLARK, J. *"Bitcoin's Academic Pedigree",* 60 COMMUNICATIONS OF THE ACM 36. 2017

NAVARRO DE ANDRÉS, S. "*Contratos Inteligentes. En especial, su implantación práctica en negocios Blockchain*". Criptoderecho. La regulación de Blockchain. Páginas 319 y siguientes. La Ley - Wolters Kluwer. 2018

NOZICK, R. "*Anarchy, State and Utopia".* Harvard 18ª Ed. Basic Books. 1974

PERETE RAMÍREZ, C. *"Blockchain, Privacidad y Protección de datos de Carácter Personal"*. Criptoderecho, la regulación del Blockchain. 2018. Ed. Wolters Kluwer. Página 177.

REINDENBERG, J.R*, "Lex Informatica: The Formulation of Information Policy Rules through Technology"*. Texas Law Review 76. 1997

SAURA ESTAPA, J. Comentarios al texto de la Declaración Universal de los Derechos Humanos. Art. 9 En: PONS RAFOLS, X. La Declaración Universal de los Derechos Humanos: Comentario artículo por artículo. 1ª Ed. Barcelona. Icaria Editorial S.A, p.p 226-229. 1997

SCHREPEL, T "*Anarchy, State, and Blockchain Utopia: Rule of Law versus Lex Cryptographia in General Principles and Digitalisation*". Hart Publishing,. 2020.

STAMPATORI, M. "Smart contract – How To Create A Smart Contract", *The Guide for Non Technical Managers To Smart Contracts*, Kindle Edition. 2019.

TYSON, J. "How the old Napster worked". Artículo alojado en https://computer.howstuffworks.com/napster.htm

SZABO, N. (2017) "Money, Blockchains and Social Scalabiity". Unenumerated, February. 2017

Fuentes web:

BIT 2 ACADEMY: https://academy.bit2me.com/

BLOCK GEEKS: https://blockgeeks.com/guides/smart-contracts/

GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 05/2014, de 10 de abril de 2014. https://edpb.europa.eu/our-work-tools/article-29-working-party_es

HUGHES, E. "Cypherpunk´s Manifesto". 1993.

LATEST HACKING NEWS: "Cómo funciona Freenet". https://latesthackingnews.com/2017/05/29/19914/

MAGAS, Julia " Top facts on China´s Crypto Yuan and related Blockchain Proyects. Publicación digital en COINTELEGRAPH https://cointelegraph.com/news/top-facts-on-chinas-crypto-yuan-and-related-blockchain-projects

MALAVIDA: https://www.malavida.com/es/analisis/redes-p2p-evolucion-de-un-protocolo-mas-alla-de-las-descargas-006483

MAY, T. "The Crypto Anarchist Manifesto". 1988

NORTON ROSE FULBRIGHT, Unlocking the Blockchain. A Global legal and regulatory guide, https://www.nortonrosefulbright.com/en/knowledge/publications/0f7d02ac/unlocking-the-blockchain-a-global-legal-and-regulatory-guide---chapter-1

OBSERVATORIO Y FORO EUROPEO DE LA CADENA DE BLOQUES EN LA U.E: https://www.eublockchainforum.eu/about

REVISTA CRIPTONOTICIAS. *"¿Qué es la tecnología de la contabilidad distribuida o blockchain?"*, disponible en https://www.criptonoticias.com/informacion/que-es-tecnologia-contabilidad-distribida-blockchain/

RÍOS, Y. "*Webinar Administración de Justicia y Blockchain"* celebrado el 7 de mayo de 2020.

SOTOMAYOR, A. "*Covid-19, Identidad y el Sr. Patata - BlockTimes #2*", https://youtu.be/t9ONc6Hoq4I

WATSON, S. "*How Does Kazaa Work". Artículo publicado en la web How Stuff Work"*.https://computer.howstuffworks.com/kazaa3.htm#:~:text=Kazaa%20uses%20peer%2Dto%2Dpeer,directly%20online%20to%20share%20content.

Z CASH: "What are ZK-SNARKs", disponible en https://z.cash/technology/zksnarks.html.

Normativa

California Assembly Bill 2658, https://legiscan.com/CA/text/AB2658/id/1821719

Carta de los Derechos Fundamentales de la Unión Europea. Publicada en el Diario Oficial de la Unión Europea de 30 de marzo de 2010.

Constitución Española. Publicado en BOE núm. 311, de 29/12/1978

Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950. Instrumento de Ratificación de 26 de septiembre de 1979 (BOE Nº 243, de 10 de octubre de 1979).

Law of 03 October 2019 on Tokens and TT Service Providers (Token and TT Service Provider Act; TVTG). Publicada en el Boletín Oficial de Liechtenstein el 3 de octubre de 2019.

Stop Online Piracy Act, del Congreso de los Estados Unidos de América, aprobada el 26 de Octubre de 2011.

UK Government Act, 2016, 41

Jurisprudencia

SAP Madrid de 13 de abril de 2014

SAP Madrid de 13 de abril de 2014

STC 58/2018, de 4 de Junio. (BOE núm. 164, de 7 de julio de 2018, páginas 68409 a 68433)

STJUE relativa al C-582/14, de 19 de octubre de 2016