IDENTIDAD DIGITAL Y RESPONSABILIDAD CIVIL DE LAS PLATAFORMAS DIGITALES: DE LAS REDES SOCIALES AL METAVERSO

DIGITAL IDENTITY AND CIVIL LIABILITY OF DIGITAL PLATFORMS: FROM SOCIAL NETWORKS TO METAVERSE

Actualidad Jurídica Iberoamericana Nº 18, febrero 2023, ISSN: 2386-4567, pp. 1008-1033

Almudena
GALLARDO
RODRÍGUEZ

ARTÍCULO RECIBIDO: 12 de octubre de 2022
ARTÍCULO APROBADO: 5 de diciembre de 2022

RESUMEN: Nos encontramos actualmente ante una evolución tecnológica que hace que las personas pasen más tiempo en línea y realicen actividades cotidianas de forma virtual constantemente. Este desarrollo está relacionado con el avance de Internet, la red de redes, que ha sido clasificada en tres etapas: Web1, Web2 y Web3. Desde la Web2, debido al auge de las redes sociales, los ciudadanos han avanzado cada vez más en la creación de una identidad digital, facilitando su información a las plataformas digitales de forma recurrente. En atención a ello, ¿Qué responsabilidad llevan aparejadas las plataformas digitales al gestionar la identidad?

Igualmente, con el metaverso se comienza a hablar de una nueva "identidad soberana", con la que los ciudadanos recuperarán el control de los datos que componen su identidad digital gracias a técnicas de blockchain. ¿Cómo cambiará la responsabilidad de las plataformas en este nuevo mundo digital? Estas preguntas serán tratadas a lo largo de esta investigación.

PALABRAS CLAVE: Identidad digital; plataformas electrónicas; responsabilidad civil; metaverso.

ABSTRACT: *We are currently facing a technological evolution that makes the population spend more time online and constantly perform daily activities virtually. This development is related to the advance of the Internet, the network of networks, which has been classified into three stages: Web1, Web2 and Web3. Since Web2, due to the rise of social networks, citizens have increasingly advanced in the creation of a digital identity, providing their information to digital platforms on a recurring basis. In view of this, what responsibility do digital platforms carry when managing identity? Likewise, the metaverse is the beginning of a new "sovereign identity", with which citizens will regain control of the data that make up their digital identity thanks to blockchain techniques. How will the responsibility of platforms change in this new digital world? These questions will be addressed throughout this research.*

KEY WORDS: *Digital identity; electronic platforms; civil liability; metaverse.*

I. INTRODUCCIÓN.

Hoy en día, es una realidad que cada vez se utilizan más las plataformas electrónicas para realizar compras, aumentando a partir de la pandemia, así como las plataformas de gestión de redes sociales (Facebook, Instagram, Twitter, LinkedIn, etc.). En el caso de las redes sociales, al acceder a una plataforma, creamos una identidad digital sobre nosotros mismos, en la cual proporcionamos información personal a la plataforma (como nombre y apellidos, dirección, número de teléfono, etc.). Además, en estas redes sociales, interactuamos con otros usuarios y compartimos información personal como fotos, noticias, opiniones, "likes", etc.

Desde la irrupción de Internet, la identidad física evoluciona a una identidad digital o identidad 2.0, a través de las acciones que realizamos en Internet. La imagen que proyectamos en la red puede ser distinta a nuestra identidad física y no es necesario que ambas se correspondan. Cada acción que realizamos en Internet deja una huella que refleja nuestros gustos, preferencias, comportamiento y forma de ser. Es decir, "ya no se trata de una identidad definida por rasgos físicos, ni por documentos que acreditan al portador unas capacidades y le habilitan para realizar ciertas actividades, sino de un concepto más amplio en el que la vida digital enriquece la vida real dando lugar a la Identidad Digital"[1].

Asimismo, la manera de gestionar la identidad en la Red también ha evolucionado, puesto que la propia Internet ha ofrecido cada vez más servicios para que los usuarios construyan su propia identidad. Así, la evolución de Internet ofrecerá nuevas formas de gestionar la identidad en función de la modalidad de

1 VVAA.: *Identidad Digital: El nuevo usuario en el mundo digital*, Coordinación editorial de Fundación Telefónica: Rosa María Sáinz Peña, Planeta, Madrid, 2013.

• Almudena Gallardo Rodríguez
Profesora Ayudante Doctora de Derecho Civil.
Universidad de Salamanca.
algaro@usal.es

www en la que nos encontramos. En este sentido, existe una evolución de Internet conocida como Web1, Web2, Web3, que desarrollaremos en el presente trabajo.

La creación de un perfil en una red social lleva a la formación de una identidad digital, lo que implica ceder información personal. A medida que interactuamos en la red, vamos definiendo aún más nuestra identidad digital día a día, por lo que los datos personales que cedemos a las plataformas digitales son cada vez mayores.

En este sentido, en el caso de que la plataforma digital haga un uso inadecuado sobre nuestros datos personales, la pregunta que surge es: ¿Qué tratamiento realizan las plataformas con nuestros datos personales? ¿deriva responsabilidad civil por parte de las mismas en cuanto a la gestión de los datos que conforman nuestra identidad digital? Una vez aclarado este punto, extrapolaremos estas cuestiones a lo que hoy en día se conoce como Metaverso, o realidad virtual inmersiva.

El presente estudio se estructura del siguiente modo: en primer lugar, haremos referencia a cómo se conforma la identidad digital en las plataformas digitales; para ello realizaremos un acercamiento conceptual y legal a lo que se entiende por identidad digital. Asimismo, veremos cómo ha evolucionado la identidad digital a través de las diferentes modalidades de Internet. En segundo lugar, trataremos la responsabilidad civil de las plataformas de gestión de redes sociales, encargadas de tratar los datos personales de los usuarios ligados al concepto de identidad digital. En este caso, analizaremos la relación contractual entre la plataforma y el usuario de la misma; la normativa a la que deben acogerse las plataformas en el tratamiento de los datos, por lo que analizaremos las cuestiones más relevantes en el Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos y Derechos Digitales Española; y abordaremos, de manera concreta, la responsabilidad civil en la que pueden incurrir las plataformas en el tratamiento de los datos personales. En tercer lugar, vislumbraremos el futuro de esta cuestión haciendo una referencia al metaverso.

II. LA IDENTIDAD DIGITAL.

1. Conceptualización.

El concepto de identidad digital se encuentra en constante desarrollo y aún no cuenta con una definición universal y aceptada en el ámbito legal. Actualmente, es la doctrina la que está perfilando este concepto, así como diversos organismos internacionales[2]. Por esta razón, compartimos a continuación aquellos conceptos sobre identidad digital que han ido ofreciendo diversos autores especializados en

2 Allende López, M.: *Identidad digital autosoberana,* 2020, Disponible en: https://www.icd.go.cr/portalicd/images/docs/uif/doc_interes/acerca_uif/IDENTIDADDIGITAL.pdf

la materia, con el fin de perfilar una conceptualización de este fenómeno. Respecto a las definiciones propuestas por la doctrina resaltamos las siguientes[3]:

Por un lado, García Mexía señala que "es una cuestión muy compleja para la que no hay consenso doctrinal. La identidad digital puede definirse como la proyección del `yo´ personal en un entorno digital con su inherente e inalienable dignidad".

Por su parte, Bueno de Mata indica que "la identidad digital es, por un lado, lo que el resto de los individuos dicen que somos en la Red, y por otro, los datos personales que nosotros mismos compartimos sobre nuestra propia persona".

En cambio, Brito Izquierdo dispone que es "cualquier aproximación al concepto de identidad digital del individuo se debe poner en relación, a su vez, con los conceptos de `identidad digital´ y de `individuo´ cuya definición, a priori, tampoco resulta sencilla de construir", y define el concepto de identidad digital atendiendo al "estándar internacional ISO/IEC 24760-1: 2019: `Seguridad y privacidad de TI: un marco para la gestión de identidad´, se podría definir como un conjunto de atributos relacionados con una entidad, la cual, no tiene por qué ser necesariamente humana, lo que introduce una dimensión interesante más allá del individuo o de la persona física, en el sentido esbozado por la Declaración Universal de los Derechos Humanos. En tal sentido, si este conjunto de atributos o datos digitales se asocia a un individuo o a un ser humano, en particular, permitiendo su identificación y autenticación confiable en línea (capacidad de autenticarse ante los demás y a actuar en base a la confianza establecida mediante medios electrónicos)".

Asimismo, Puyol Montero define la identidad digital como "el conjunto de la información sobre un individuo o una organización expuesta en Internet (datos personales, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha persona en el plano digital". Y añade que "esta identidad está integrada por los diferentes atributos que compartimos en las diversas plataformas, de modo y manera que diferentes identidades digitales, hoy por hoy, se corresponden con una misma persona. Por eso se puede afirmar que los usuarios pueden proyectar más de una identidad digital a través de múltiples comunidades" [4].

En consecuencia, a día de hoy no contamos con único concepto de identidad digital en ninguna normativa, sino que dicho concepto lo ha ido ofreciendo la

3 Cfr. VVAA., "Diálogos para el futuro judicial XVII. Identidad digital y proceso judicial", coord. Álvaro Perea González (Letrado de la Administración de Justicia). *Diario La Ley*, Nº 9777, Sección Plan de Choque de la Justicia, Encuesta, 25 de enero de 2021, Wolters Kluwer.

4 Puyol Montero, J.: *La tecnología «Blockchain» y la identidad digit*al, en: https://confilegal.com/20190325-125312/ [Fecha de consulta: 5 de septiembre de 2022].

doctrina especializada y diversos organismos. Por tanto, la identidad digital se construye a través de la información que cada persona comparte sobre él en Internet. Además, dicha identidad digital se configura por nuestro comportamiento y forma de actuar en las redes sociales. En este sentido, es importante tener en cuenta que puede ser alterada a lo largo del tiempo, y que nuestra identidad digital puede estar disociada con nuestra identidad física, no debiendo tener la misma personalidad ni rasgos de identidad en terreno físico que en el terreno virtual.

2. Reconocimiento Legal.

Es importante indicar que a nivel legislativo la identidad digital empieza a contar con un cierto respaldo que posteriormente se deberá materializar en las diferentes normativas internacionales.

Debemos partir del reconocimiento de la identidad como un derecho humano. Tal y como indica Allende López: "paradójicamente, la Declaración Universal de Derechos Humanos (DUDH) no menciona la palabra identidad ni una sola vez, ni tampoco reconoce explícitamente el derecho a ser identificado". Sin embargo, como señala el autor, el documento de la DUDH sí reconoce "el derecho de todo ser humano al reconocimiento de su personalidad jurídica en cualquier lugar" (art.6); el "derecho a una nacionalidad" (art. 15); y el "derecho a la propiedad privada" (art. 17), por lo que "para garantizar los anteriores derechos, las personas han de ser identificables. De ahí que entendamos que el derecho a tener una identidad y a ser identificable se reconoce en la DUDH de forma implícita"[5].

A nivel de regulación, es de obligada referencia tratar el reconocimiento legal a nivel europeo por medio del Reglamento eIDAS, así como a nivel nacional en España, en la Carta de Derechos Digitales, al reconocer por primera vez el "Derecho a la identidad en el entorno digital"[6]. A pesar de ello, no podemos hablar de un reconocimiento legal expreso a nivel globalizado de la identidad digital, por lo que después de estas dos referencias, indicaremos los derechos globales[7] si reconocidos y aparejados a la identidad digital.

En este sentido, la *Agenda de Naciones Unidas para el año 2030 y los Objetivos de Desarrollo Sostenible* incorporan dentro de su ODS 16.9 la obligación a los países de proporcionar antes de 2030 una identidad legal para todos[8]. Es importante, puesto

5 Allende López, M.: *Identidad digital autosoberana,* 2020, Disponible en: https://www.icd.go.cr/portalicd/images/docs/uif/doc_interes/acerca_uif/IDENTIDADDIGITAL.pdf

6 https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

7 Bueno De Mata, F.: "El derecho de acceso universal a internet: reconocimiento legal y perspectiva procesal", *Nuevos retos en materia de derechos digitales en un contexto de pandemia: perspectiva multidisciplinar*, Aranzadi, Navarra, 2022, pp. 69 y ss.

8 Disponible en: https://www.fundacioncarolina.es/wp-content/uploads/2019/06/ONU-Agenda-2030.pdf [Fecha de consulta: 10 de septiembre de 2022].

que la identidad legal no es un término que tenga un significado legal globalizado ni es un concepto tradicionalmente reconocido por la ley en muchos países. Por todo ello podemos decir que la ONU indica que existe un derecho individual a la identidad según el derecho internacional y ello hará que el derecho civil de los diferentes estados deberá reconocer la identidad digital como un derecho en los años venideros.

De igual modo, hay que mencionar dos Reglamentos:

1. El *Reglamento (UE) Nº 910/2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior*, conocido como el Reglamento eIDAS (conocido por sus siglas en inglés eIDAS, electronic IDentification, Authentication and trust Services)[9], se aprobó el 23 de julio de 2014 (entró en vigor en 2016), aunque el Reglamento se centra más en formas de identificación digital que en la identidad digital en sí misma, al regular todo lo relativo a la firma electrónica como método de identificación a nivel europeo.

2. La Comisión Europea en julio de 2021 ha presentado una propuesta que modifica el Reglamento eIDAS, denominado *Reglamento eIDAS2* con el fin de regular la identificación digital transfronteriza dentro de la Unión Europea[10]. En este sentido, Ursula Von Der Leyer, presidenta de la Comisión Europea, en su discurso sobre el estado de la Unión, el 16 de septiembre de 2020, expuso: "Cada vez que una aplicación o un sitio web nos pide que creemos una nueva identidad digital o que nos conectemos fácilmente a través de una gran plataforma, en realidad no tenemos ni idea de lo que sucede con nuestros datos. Por este motivo, la Comisión propondrá una identidad electrónica europea segura"[11]. Para conseguir dicha identidad digital, el Reglamento eIDAS2 propone emitir una "cartera de identidad digital europea". Esta cartera de identidad "permitirá a los ciudadanos identificarse digitalmente, almacenar y gestionar datos personales y documentos oficiales en formato electrónico", por lo que en dicha cartera se podrá llevar, por ejemplo, el DNI, el carnet de conducir, tarjetas bancarias, titulaciones universitarias, etc. y será válido de igual forma en todos los Estados Miembros de la UE[12].

La novedad más importante es que el ciudadano tendrá el pleno control sobre la cartera de identidad digital, esto es, será responsable sobre el uso de

9 https://www.boe.es/doue/2014/257/L00073-00114.pdf [Fecha de consulta: 10 de septiembre de 2022].

10 https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021PC0281&from=EN
Vid. Llanera González, P.: *Identidad digital. Actualizado a la Orden ETD/465/2021, de 6 de mayo (sobre métodos de identificación remota) y a la propuesta de Reglamento eIDAS2*, Bosch, Barcelona, 2021.

11 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_es [Fecha de consulta: 10 de septiembre de 2022].

12 https://ec.europa.eu/commission/presscorner/detail/es/QANDA_21_2664

sus datos personales (art. 6.bis.7 eIDAS2)[13]. Por tanto, nuestros datos ya no dependerán de las plataformas de redes sociales, por lo que afectará en términos de responsabilidad civil en el tratamiento de los datos, y la misma abre la puerta a lo conocido como "identidad digital auto-soberana" basada en tecnología descentralizada blockchain[14]. En otras palabras, la administración de la identidad no estará a cargo de las plataformas, sino que serán los usuarios los que tendrán la responsabilidad final sobre su manejo.

En España, aunque contamos con una Ley Orgánica de Protección de Datos y Derechos Digitales desde 2018[15], no es hasta julio de 2021, gracias a la denominada Carta de Derechos Digitales[16], donde se encuentra un reconocimiento a la regulación de la identidad digital. Si bien, la Carta de Derechos Digitales no es una ley, sino una declaración, esto quiere decir que no es ni vinculante ni obligatoria, por lo que nos encontramos ante una especie de *soft law* que sirve para interpretar o dar orientaciones en la aplicación de determinados derechos. En este sentido, dentro del bloque de "Derechos de la libertad", se reconoce expresamente el "Derecho a la identidad en el entorno digital", el cual viene conformado por cuatro epígrafes, y en su punto uno indica que: "El derecho a la propia identidad es exigible en el entorno digital. Esta identidad vendrá determinada por el nombre y por los demás elementos que la configuran de acuerdo con el ordenamiento jurídico nacional, europeo e internacional".

A pesar de que la identidad digital aún no se ha reconocido legalmente a nivel global en textos internacionales, los derechos relacionados con la identidad física si se aplican también a la identidad digital, ya que son considerados como bienes jurídicos inherentes a la dignidad humana. Estos derechos incluyen la protección de la intimidad, la imagen y la reputación personal, y están protegidos por la Declaración Universal de Derechos Humanos y el Convenio Europeo de Derechos Humanos, en sus arts. 12 y 8 respectivamente[17].

13 Cfr. El art. 6.bis.7 eIDAS2 dispone: "El usuario mantendrá pleno control sobre la cartera de identidad digital europea. El emisor de la cartera de identidad digital europea no recopilará información sobre el uso de la cartera que no sea necesaria para la prestación de los servicios de esta, ni combinará datos de identificación personal u otros datos personales almacenados o relacionados con el uso de la cartera de identidad digital europea con datos personales obtenidos a través de otros servicios ofrecidos por dicho emisor o a través de servicios de terceros que no sean necesarios para la prestación de los servicios de la cartera, a menos que el usuario lo haya solicitado expresamente. Los datos personales relacionados con la provisión de carteras de identidad digital europea se conservarán en soporte físico y lógico por separado de cualesquier otros datos mantenidos"

14 *Vid.* Alamillo Domingo, I.: "La identidad descentralizada como garantía de la privacidad en la vida digital", *La Ley privacidad* , Nº 5, Sección El foro de la privacidad, Tercer trimestre de 2020, Wolters Kluwer LA LEY 9425/2020.

15 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales. https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

16 https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

17 https://blog.signaturit.com/es/mas-alla-de-la-reputacion-online-que-se-entiende-por-identidad-digital-y-que-derechos-estan-asociados-a-ella [Fecha de consulta: 16 de septiembre de 2022]

3. La evolución de la identidad digital en Internet: de la web 2 a la Web 3

La forma de gestionar la identidad digital en la Red ha evolucionado, puesto que la propia Internet ha ofrecido cada vez más servicios para que los usuarios construyan su propia identidad. Así, la evolución de Internet ofrecerá nuevas formas de gestionar la identidad en función de la modalidad de WWW en la que nos encontramos. En este sentido, existe una evolución de Internet conocida como Web1, Web2, Web3. Brevemente, cada una de las webs consisten en lo siguiente[18]:

La Web1 permitía a los usuarios leer páginas web y hacer comentarios en foros y blogs, su identidad digital era limitada a los sitios que visitaban. La Web2, actualmente en uso, permite interactuar y alimentar los servicios con información, permitiendo la creación de perfiles y páginas por parte de cada usuario. La identidad digital es una construcción personal, donde cada persona decide qué información incluir en su perfil, pero esta información está sujeta al tratamiento de datos por parte de los proveedores de servicios como Facebook o Instagram.

Por último, dentro de la Web. 3.0 se encuentra el metaverso, que consiste "en una combinación entre el mundo físico y el mundo digital, es decir, un lugar virtual donde, a través del uso de diferentes tecnologías (gafas de realidad virtual, gafas de realidad aumentada, guantes y otras prendas o dispositivos hápticos, etc.), los usuarios podrán sumergirse e interactuar con otras personas y objetos como si lo hicieran en el mundo real"[19]. La Web3 es una web de lectura, escritura y confianza que está en desarrollo y se considera el futuro de internet. Se diferencia de la actual Web2 por ser un "Internet descentralizado", en el que los datos se distribuyen a través de las redes sin que ninguna entidad sea propietaria de la información, gracias a la tecnología blockchain.

En la web 3.0 la identidad digital es conocida como auto-soberana, pues su almacenamiento no se encuentra dentro de ningún proveedor de servicios, sino que depende de una tecnología descentralizada basada en blockchain. En definitiva, hablamos de infraestructuras descentralizadas para que los usuarios creen y gestionen sus activos digitales, teniendo como un ejemplo lo que actualmente se conoce como metaverso, o la configuración de la cartera digital vinculada al reglamento EiDas2 anteriormente citado. En este caso, la identidad digital creada es interoperable, se crea por parte del usuario y puede ser usada por igual ante cualquier proveedor de servicios.

18 Bueno de Mata, F.: "Del metaverso a la metajurisdicción: desafíos legales y métodos para la resolución de conflictos generados en realidades virtuales inmersivas", *Derecho de privacidad y derecho digital*, ISSN 2444-5762, Vol.7, Núm. 27, 2022, pp. 21 y ss.

19 https://www.mdzol.com/estilo/2022/2/10/web-30-metaverso-guia-para-comprender-el-futuro-de-internet-220630.html [Fecha de consulta: 15 de septiembre de 2022].

Para entender qué es la "Identidad Digital auto-soberana" tenemos que partir de los tipos de identidad digital. Es decir, en la gestión de la identidad digital se distinguen dos modelos: un modelo centralizado (centralizado, federado y distribuido) y un modelo descentralizado[20].

En la doctrina, el experto en la materia en identidad digital, ALLEN, en su artículo *the path to self-Sorevering Identity*, 2016, considera que los modelos de identidad digital han evolucionado desde la llegada de internet, y distingue cuatro fases[21]:

"-Fase 1. Identidad centralizada. Control administrativo por una sola autoridad o jerarquía.

-Fase 2. Identidad federada. Control administrativo por parte de varias autoridades federadas.

-Fase 3. Identidad centrada en el usuario. Control individual o administrativo a través de múltiples autoridades sin requerir una federación.

-Fase 4. Identidad auto-soberana (identidad descentralizada). Control individual a través de cualquier número de autoridades".

Concretamente, la identidad auto-soberana es la que se encajaría con el uso de blockchain[22]. En este sentido, diversos agentes, tanto públicos como privados, están trabajando para conseguir una identidad descentralizada con la utilización del blockchain. Un ejemplo de ello lo tenemos en España. La Asociación Española de Normalización, UNE, el 20 de diciembre de 2020 publicó la Norma UNE 71307-1 bajo el título "Tecnologías Habilitadoras Digitales. Modelo de Gestión de Identidades Descentralizadas sobre blockchain y otras Tecnologías de Registros Distribuidos. Parte 1: Marco de referencia". La Norma UNE 71307-1 define "un marco de referencia genérico para la emisión, administración y uso descentralizados de aquellos atributos que faciliten la caracterización (identificación) de individuos u organizaciones, permitiendo a estos últimos crear y controlar su propia identidad digital de forma autogestionada, sin la necesidad de recurrir a autoridades centralizadas". Tal y como indica la nota de prensa emitida por la UNE, esta norma constituye un hito al ser "el primer estándar mundial sobre identidad digital descentralizada en Blockchain"[23].

20 PÉREZ BES, F.: "Identidad y blockchain", en *Criptoderecho. La regulación de blockchain*, edición Nº 1, LA LEY, 2018. LA LEY 13760/2018.

21 ALLENDE LÓPEZ, M.: *Identidad digital autosoberana,* 2020, Disponible en: https://www.icd.go.cr/portalicd/images/docs/uif/doc_interes/acerca_uif/IDENTIDADDIGITAL.pdf

22 MERCHÁN MURILLO, A.: "Identidad digital Blockchain e Inteligencia Artificial: aspectos jurídicos de presente y futuro a debate", *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, ISSN-e 2444-8478, Vol. 7, Nº. 1, 2021, pp. 191 y ss.

23 https://www.une.org/salainformaciondocumentos/NP%20Norma%20UNE%20Blockchain%20dic-20.pdf [Fecha de consulta: 15 de septiembre de 2022].

Asimismo, hay que destacar que la identidad auto-soberana se rige por una serie de principios propios[24], los cuales pueden resumirse en la idea de que la identidad digital en la Web 3.0 debe ser independiente a la existencia real del usuario, controlada por el usuario mismo y no por proveedores de servicios, accesible por el usuario con una contraseña, transparente y con código abierto, persistente y con derecho al olvido, portátil y disponible en cualquier sistema, basada en el consentimiento del usuario, con divulgación mínima de datos personales, y con protección de derechos del usuario.

En este sentido, la tecnología blockchain sirve para solventar algunos problemas que plantea la identidad digital, identificados por WINDLEY[25], como son la falta de proximidad, escalabilidad, flexibilidad, privacidad y consentimiento. Así, según Alamillo Domingo "los sistemas de gestión de identidad digital basados en tecnologías de registro distribuido (DLT) pueden desempeñar un papel importante en la implementación de un derecho personal a la identidad, con una fuerte visión de autodeterminación y autonomía personal, al menos cuando nos referimos a personas físicas. Estas tecnologías de registro distribuido, y en particular la tecnología de cadenas de bloques o Blockchain, normalmente basada en criptografía de clave pública, permiten la creación de un registro inmutable que se gestiona de una manera absolutamente descentralizada, permitiendo nuevas aplicaciones hasta ahora impensables, con un potencial transformador más allá de cualquier duda"[26].

El autor señala que en un sistema en el que cualquier información puede ser escrita en un nodo de red y se copiará en todos los demás, ninguno puede eliminarla. Para esto, se utilizan tecnologías de registro distribuido como blockchain para crear una identidad auto-soberana (SSI) controlada y administrada por la persona individualmente sin la intervención de terceros.

III. LA RESPONSABILIDAD CIVIL DE LAS PLATAFORMAS DIGITALES EN EL TRATAMIENTO DE DATOS QUE CONFORMAN LA IDENTIDAD DIGITAL.

A continuación, vamos a analizar a quién se le atribuiría la responsabilidad civil en el tratamiento de los datos que conforman la identidad digital, para lo que diferenciaremos los supuestos en relación con los dos escenarios apuntados: la

24 Allen, C.: "Self-Sovereign Identity Principles", disponible en: https://github.com/ChristopherA/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md; https://masterethereum.com/identidad-auto-soberana-master-blockchain-online/

25 Windley, P.: "Fixing the Five Problems of Internet Identity", https://blog.sovrin.org/fixing-the-five-problems-of-internet-identity-b55ea072c3ea

26 Alamillo Domingo, I.: "La identidad descentralizada como garantía de la privacidad en la vida digital", *cit.*, LA LEY 9425/2020.

web2 y la web3. En este apartado nos vamos a centrar en la Web 2. Dentro de la Web 2.0 se enmarcan de manera concreta las redes sociales.

1. Relación contractual entre el usuario y las plataformas de redes sociales.

Al registrarse como usuario en una red social proporcionamos toda una serie de datos personales (email, número de teléfono, dirección etc.), y una vez creado el perfil lo nutrimos con contenido (como fotos, comentarios, gustos, aficiones, etc.), que conforma nuestra Identidad Digital. Además, el registro implica que el usuario del servicio tiene que aceptar unos "Términos y Condiciones". Asimismo, las plataformas, siempre que se recaben datos personales, tendrán que contar con una "Política de privacidad", que tendrá que aceptar el usuario.

Por tanto, al aceptar mediante el conocido "*click agreement*" en el que a golpe de *click* aceptamos "términos y condiciones" y las "políticas de privacidad", se está generando con ese simple *click* una relación contractual entre el usuario y la plataforma. Se trata de un contrato atípico, denominado contrato de adhesión, "contratos típicos de las redes sociales donde el usuario sólo puede aceptar o rechazar todas las condiciones en su conjunto"[27].

El contrato de adhesión es un contrato bilateral, pues ambas partes deben cumplir sus obligaciones, y se caracteriza por que las cláusulas del contrato son impuestas por una de las partes, es decir, "no son ambas partes las que redactan el clausulado, sino que éste es predispuesto e impuesto por una de ellas a la otra, que no puede más que aceptarlo o rechazarlo"[28]. Faus Puyol lo define como aquel contrato "que contiene cláusulas, estipulaciones o condiciones de carácter general redactadas de forma previa por una empresa para aplicar a todos los contratos que la misma celebre, y cuya aplicación no puede evitar el consumidor o usuario si desea obtener el bien o servicio de que se trate"[29]. Esto es, las cláusulas del contrato son redactadas por la plataforma de forma unilateral sin existir negociación posible por parte del usuario, por lo que si el usuario quiere hacer uso del servicio tiene que aceptar las condiciones establecidas en el contrato. En los "Términos y Condiciones" y en la "Política de Privacidad" se establece lo siguiente:

-Los "Términos y Condiciones" son redactados por el proveedor del servicio, y consisten en las cláusulas que establecen los derechos y obligaciones de las partes.

27 Platero Alcón, A., "La responsabilidad de las redes sociales: el caso de Ashley Madison", *Boletín Mexicano de Derecho Comparado*, nueva serie, año XLIX, núm. 150, septiembre-diciembre de 2017, pp. 1259-1288, https://revistas.juridicas.unam.mx/index.php/derecho-comparado/issue/archive.

28 "Contrato de adhesión", Guía Jurídica, La Ley. https://guiasjuridicas.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbF1jTAAAUMjAzNLtbLUouLM_DxblwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoAiq9eTTUAAAA=WKE [Fecha de consulta: 16 de septiembre de 2022].

29 Concepto ofrecido por Faus Pujol, M.: *Práctico obligaciones y contratos*, Vlex.com, diciembre 2022.

Aunque cada plataforma incluirá sus propias condiciones de uso, hay determinados cláusulas que obligatoriamente deben incluirse, como[30]: identificación del titular, derechos del usuario, duración, rescisión, legislación aplicable, método para la resolución de conflictos, y las responsabilidades que asumirán ambas partes.

- La "Política de privacidad" se refiere a cómo las plataformas gestionan nuestros datos e información personal y garantizan la privacidad de los usuarios. Dicha política debe cumplir con el Reglamento General de Protección de Datos (RGPD)[31], y la Ley Orgánica de Protección de Datos Personales y Garantías de Derecho Digitales (LOPDGDD)[32]. Así, con la entrada en vigor del Reglamento todas las empresas han tenido que adaptar sus "Políticas de Privacidad" a la normativa, incluidas las empresas que tienen una actividad en la Unión Europea (UE), por ejemplo, empresas como Facebook o LinkedIn[33].

Atendiendo a lo anterior, ¿cómo debe realizarse el tratamiento de datos personales en las plataformas de redes sociales?; y ¿qué responsabilidad asume la plataforma respecto a dicho tratamiento? Estas preguntas van a ser abordadas a continuación.

2. Normativa aplicable por parte de las plataformas en el tratamiento de los datos personales.

Como hemos indicado, en lo referente al tratamiento de datos las plataformas digitales de la Web 2 tienen que incluir las "políticas de privacidad", las cuales tiene que cumplir con el Reglamento General de Protección de Datos (RGPD)[34], y la Ley Orgánica de Protección de Datos Personales y Garantías de Derecho Digitales (LOPDGDD) española[35]. A continuación, vamos a destacar los aspectos

30 Pueden consultarse ejemplo de condiciones de uso de Facebook o LinkedIn: https://es-es.facebook.com/legal/terms; https://es.linkedin.com/legal/user-agreement#dispute

31 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32016R0679

32 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales. https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

33 Pueden consultarse ejemplos de políticas de privacidad de Facebook: https://es-es.facebook.com/privacy/policy/; o de LinkedIn: https://es.linkedin.com/legal/privacy-policy

34 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32016R0679

35 Ley Orgánica de Protección de Datos Personales y Garantías de Derecho Digitales https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673
La Agencia Española de Protección de datos, en septiembre de 2018, publicó un decálogo para la adaptación al RGPD de las políticas de privacidad en internet. https://www.aepd.es/sites/default/files/2019-12/informe-politicas-de-privacidad-adaptacion-RGPD.pdf

más relevantes de cada normativa a tener en cuenta para un uso adecuado sobre el tratamiento de los datos personales de los usuarios.

A) Reglamento General de Protección de Datos.

La normativa sobre protección de datos en la UE está compuesta por el Reglamento General de Protección de Datos (RGPD) y la Directiva 2016/680, que regulan la protección de datos personales en general y para las autoridades policiales y de justicia, respectivamente[36]. El RGPD entró en vigor en 2016 y se empezó a aplicar a todos los Estados Miembros de la UE en mayo de 2018[37].

La protección del tratamiento de datos personales de las personas físicas es un derecho fundamental. Así viene recogido en el art. 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el art. 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE), que determina que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan" (considerando 1 RGPD).

El RGPD tiene un triple objetivo: "Garantizar el derecho fundamental a la protección de datos personales; proteger los derechos y libertades fundamentales de las personas físicas; la libre circulación de los datos personales en la UE"[38].

El RGPD, respecto a su ámbito de aplicación, el mismo abarca tanto a responsables y encargados de tratamientos de datos establecidos en la UE como a aquellos fuera de la UE que ofrezcan bienes o servicios a ciudadanos europeos o realicen un seguimiento de su comportamiento. Para cumplir con la ampliación de su alcance, estas organizaciones deben nombrar un representante en la UE como punto de contacto con las Autoridades de supervisión y de los ciudadanos. En caso de ser necesario, el representante en la UE también puede ser objeto de acciones de supervisión por parte de las autoridades. La información de contacto del representante en la Unión debe proporcionarse a los interesados junto con la información sobre el tratamiento de sus datos personales[39].

36 Recomendamos que para obtener una visión amplia y acertada de esta normativa, puede consultarse: Aparicio Vaquero, J.P.: "La protección de datos que viene: el nuevo Reglamento General europeo", *Ars Iuris Salmanticensis: AIS: revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología*, ISSN-e 2340-5155, Vol. 4, N°. 2, 2016, pp. 27-34.

37 Pueden consultarse algunos comentarios sobre el Reglamento, entre otros, en: López Calvo, J.: *Comentarios al Reglamento Europeo de Protección de Datos*, Sepin, Madrid, 2017; VV.AA.: *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, coord., José López Calvo,Wolters Kluwer, Bosch, Madrid, 2019; VV.AA.: *Algunos desafíos en la protección de datos personales*, Alfredo Batuecas Caletrío (dir.), Juan Pablo Aparicio Vaquero (dir.), Editorial Comares, Granada, 2018.

38 VV.AA. *Protección de datos, Memento práctico,* dir. José Luis Piñar Mañas, Coord. Miguel Recio Gayo, Francis Lefebvre, Barcelona, 2022, p. 23.

39 https://www.aepd.es/es/preguntas-frecuentes/2-rgpd/1-de-aplicacion/FAQ-0202-cual-es-el-ambito-de-aplicacion-del-rgpd

Para poder hablar del tratamiento de uso de los datos personales, debemos partir de qué se entiende por tratamiento de datos y datos personales:

- El tratamiento de datos personales consiste en cualquier operación que se realice sobre los datos personales, "ya sea por procedimientos automatizados o no". En diferentes situaciones se puede hablar del tratamiento de datos, en el caso de "recogida de datos, registro, organización y estructuración de la información, conservación, adaptación, modificación, extracción, consulta de datos, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción" (art.4.2 RGPD).

- El dato personal pertenece al titular, también llamado afectado o interesado, y es "toda información sobre una persona física identificada o identificable" (art. 4.1 RGPD). Por tanto, los datos personales conforman la identidad digital de una persona que la identifican (nombre, apellidos, email, domicilio, etc.). Dentro de los datos de carácter personal hay una serie de datos catalogados como "datos sensibles" al afectar directamente a la vida de las personas. En este caso, queda prohibido el tratamiento de datos personales que revelen "el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física" (arts. 9 RGPD).

En relación a las figuras que intervienen en este tratamiento de datos, son las siguientes: titular, responsable del tratamiento de datos, el encargado del tratamiento, Delegado de Protección de Datos, la Autoridad de Control y otras figuras.

De igual modo, existe un principio básico en el tratamiento de los datos personales: el consentimiento, explícito y específico, que se debe otorgar por el usuario para cada fin (art. 4.11 RGPD). Sumado a lo anterior, el Reglamento añade una serie de principios de necesario cumplimiento para quien trata datos personales: Licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación de plazo de conservación, integridad y confidencialidad, responsabilidad proactiva (art. 5 RGPD).

Asimismo, el titular de los datos tiene la posibilidad de ejercitar una serie de derechos relacionados con los datos, como son: el derecho de acceso, derecho de rectificación, derecho de supresión, derecho de oposición, derecho a la limitación del tratamiento, derecho a la portabilidad de los datos, y no ser objeto de decisiones individuales automatizadas.

Por último, como cuestión a destacar, el RGPD prevé la posibilidad de que el titular de los datos pueda reclamar una indemnización por el tratamiento inadecuado de los datos personales (art.82 RGPD), tal y como veremos en un epígrafe posterior.

B) Ley Orgánica de Protección de Datos Personales y Garantías de Derecho Digitales.

Por su parte, en España se publica la Ley Orgánica de Protección de Datos Personales y Garantías de Derecho Digitales, que entró en vigor en diciembre de 2018. La normativa del RGPD es complementada por esta ley, asegurando los derechos digitales de los ciudadanos en cumplimiento de lo recogido a su vez en la Constitución Española, garantizando el pleno ejercicio de sus derechos. En este sentido, el preámbulo de la LOPDGDD recoge expresamente que: "la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 CE".

La LOPDGDD incluye medidas nuevas respecto a la LOPD de 1999, como[40]: la protección de los datos personales de personas fallecidas; medidas especiales de protección de datos para los menores de edad; responsabilidad proactiva por parte de los responsables del tratamiento de datos, en la misma línea que en el RGPD. También se establece un registro de actividades de tratamiento, se requiere el consentimiento informado y se amplían los derechos de los titulares de los datos (acceso, rectificación, supresión, limitación, portabilidad, oposición y derecho al olvido o desconexión digital). Se exige la notificación en caso de una brecha de seguridad. Por último, la ley prevé sanciones por incumplimiento de la normativa y como bloque de contenido adicional recoge y conceptualiza hasta diecisiete derechos digitales, los cuales quedan al margen de este estudio de manera concreta.

Asimismo, hay una serie de artículos concretos referentes a las redes sociales, lo que singulariza este escenario de Internet, reconociendo así que debe tener un tratamiento jurídico particular y diferenciado de otros escenarios virtuales. Podemos hacer referencia a preceptos como el art. 84 relativo a la protección de los menores en Internet y al art. 92 sobre la protección de datos de los menores en Internet; el art. 85.2, el cual prevé la necesidad por parte de los responsables de redes sociales y servicios equivalentes a adoptar protocolos para el que usuario

40 La Agencia Española de Protección de Datos publicó una sencilla guía sobre novedades de la LOPDGDD dirigidas al ciudadano: https://www.aepd.es/sites/default/files/2019-10/novedades-lopd-ciudadanos.pdf. Asimismo, por parte de la doctrina encontramos diversos comentarios a la LOPDGDD, entre otros: VV.AA.: *Protección de datos, Memento práctico,* Francis Lefebvre, Barcelona, 2022; VV.AA. *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, coord., José López Calvo ,Wolters Kluwer, Bosch, Madrid, 2019; Martínez Rodríguez, N.: "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales", *Ars Iuris Salmanticensis: AIS : revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología*, ISSN-e 2340-5155, Vol. 7, Nº. 1, 2019, pp. 254-259.

puede ejercitar el derecho de rectificación que atente contra el derecho al honor, la intimidad personal y familiar; el art. 94 regula el derecho al olvido en redes sociales y servicios equivalentes; art. 95 prevé el derecho de portabilidad en redes sociales y servicios equivalentes; art. 96 que regula el Derecho al testamento digital, en concreto en el punto 2, determina "las personas legitimadas en el apartado anterior podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones"; y por último, el art. 97 sobre las Políticas de impulso en los derechos digitales, también contextualiza su aplicación dentro de un modelo protagónico de redes sociales. Todo ello hace que se ensalce desde un punto de vista de técnica legislativa a las redes sociales como escenario virtual concreto en el que ejercitar una serie de derechos y del que se derivan a su vez obligaciones para los agentes implicados.

3. Responsabilidad civil de las plataformas sociales por el uso inadecuado de los datos personales de los usuarios.

Como hemos indicado, aunque aceptemos la "política de privacidad" sobre el uso de nuestros datos, puede ocurrir que las plataformas no realicen un uso adecuado del tratamiento de los datos personales de los usuarios, y el titular de los datos sufra un daño. Por ejemplo, una vez que el usuario tenga creada su identidad digital la plataforma ceda a terceros sus datos personales sin su consentimiento, o puede darse el caso que se produzca una brecha de seguridad, con la siguiente fuga de los datos personales de los usuarios[41], u otros supuestos, pues tal y como indica Platero Alcón también se derivaría responsabilidad "en el supuesto de que no se hubiera informado correctamente sobre el uso de los datos personales y los mismos, han sido consultados por terceros que no se encontraban autorizados en las políticas de privacidad o, como no, en supuestos donde la red social no cumple adecuadamente su deber de seguridad de datos personales"[42].

Por tanto, en base a lo anterior, ¿el titular de los datos podría solicitar una indemnización por los daños y perjuicios que le hayan podido ocasionar la plataforma por un uso inadecuado de sus datos personales? De dicho daño se

41 En los últimos años se han producido por parte de plataformas como Facebook, Twitter, entre otras, numerosas brechas de seguridad en el que se han filtrado datos de numerosos usuarios. https://theconversation.com/500-millones-de-afectados-por-la-brecha-de-datos-de-facebook-y-ahora-que-158496 [Fecha de consulta: 16 de septiembre de 2022].
Puede consultarse una guía de la AEPD sobre la brecha de seguridad: https://www.aepd.es/es/documento/guia-brechas-seguridad.pdf

42 Platero Alcón, A.: *Análisis de la normativa europea y española de protección de datos personales: régimen de responsabilidad civil derivado de un incorrecto tratamiento de dato personales*, Tesis doctoral, dirigida por Carlos Lasarte Álvarez (dir. tes.), Ángel Acebo Penco (codir tes.) Universidad de Extremadura, 2020, pp. 323 y 324.

deriva una responsabilidad civil[43], al margen de otros tipos de responsabilidad en los que se podría incurrir; y partiendo de que existe una relación contractual entre la plataforma y el usuario titular de los datos, se puede ejercitar una acción de responsabilidad civil contractual, con el fin de solicitar la reparación del daño sufrido.

El daño se reclamará en base al art. 82 RGPD, donde se recoge el derecho a la indemnización del afectado por los daños y perjuicios causados en el uso inadecuado de sus datos personales. Así dispone el precepto en su punto primero: "toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos".

Por tanto, este Reglamento protege los derechos de las personas que han sufrido daños y perjuicios a causa de un incumplimiento de la normativa y les da derecho a recibir una indemnización del responsable o encargado del tratamiento.

No obstante, el responsable o encargado del tratamiento puede estar exento de responsabilidad si demuestra que no es en modo alguno responsable de los daños y perjuicios causados. En caso de haya más de un responsable o encargado, o un responsable y un encargado, sean responsables de los daños y perjuicios causados, cada uno será considerado responsable en los mismos términos, garantizando así la indemnización efectiva del interesado, dándole más vías a este último de reclamar por el daño sufrido.

Conectado con la idea anterior, si un responsable o encargado ha pagado una indemnización total, tendrá derecho a reclamar a los demás responsables o encargados la parte correspondiente de acuerdo con las condiciones establecidas. Por último, las acciones judiciales para ejercer el derecho a indemnización se presentarán ante los tribunales competentes de acuerdo con el Derecho del Estado miembro.

En resumen, este precepto brinda una protección integral y efectiva al usuario que haya sufrido daños y perjuicios como resultado de una infracción, y que perfectamente puede ser extrapolable al caso de estudio en el que se centra el presente artículo.

43 Respecto a responsabilidad y daños puede verse: Llamas Pombo, E.: *Manual de Derecho Civil. Vol.VII. Derecho de Daños*, Eugenio Llamas Pombo (dir.), La Ley, Madrid, 2021.

De manera adicional, tal y como señalan autores como Platero Alcón y Álvarez Hernando[44], debemos tener en cuenta que el interesado de nacionalidad española también podría ejercitar otras acciones indemnizatorias apoyado en el art. 9.3 de la *Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*; acciones que resultarían compatibles con la acción recogida en el RGPD.

Por último, debemos hacer una matización respecto a la posibilidad de que la plataforma de red social goce de una exención de responsabilidad en este contexto. Según el RGPD si existiera un caso concreto, y por tanto no de aplicación de manera genérica o por defecto, en las que la plataforma en base a su consideración como prestador de servicios de intermediación acuda a lo dispuesto en los arts. 14 y ss. de la Ley 34/2002, de 11 de julio de Servicios de la Sociedad de Información y Comercio Electrónico (LSSICE)[45] para excluir su responsabilidad civil por daños causados en el tratamiento de datos personales. Tal y como indica Rubí Puig interpretando el articulado, los prestadores de servicios o almacenamiento de datos podrán exonerar su responsabilidad "siempre que no tengan conocimiento efectivo de que la actividad o la información almacenada por medio de una operación de tratamiento es ilícita o de que lesiona bienes o derechos de un tercero susceptible de indemnización, o, si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos'[46].

En este sentido, podemos observar cómo las causas son limitadas, indicando que el uso inadecuado de los datos tenía ya un origen ilícito y que la plataforma no ha tenido conocimiento efectivo del mismo o que, una vez enterado de tal situación, hace todo lo posible para corregirlo y evitar daños mayores. Esta forma de proceder, y esta situación concreta derivarían en un supuesto de exención de responsabilidad, siendo compatible a su vez con lo recogido en el art. 1.5 b) de la Directiva 2001/31/CE. Por tanto, y sin entrar al fondo en la casuística tan amplia que podría venir derivada de este supuesto, la manera de proceder proactiva del responsable ante una situación de este tipo, por contenido ilícito o daños a terceros, determinará que estemos o no ante un caso de exención de responsabilidad.

44 Platero Alcón, A.: *Análisis de la normativa europea y española de protección de datos personales: régimen de responsabilidad civil derivado.., cit.,* p. 172 ; Álvarez Hernando, J.: "Análisis jurídico de la acción de reclamación de una indemnización por haber sufrido daños y perjuicios derivados de una infracción en materia de protección de datos. Estudio del art. 82 RGPD", enero de 2019. En https://www.ac-abogados.es/analisis-juridico-de-la-accion-de-reclamacion-de-una-indemnizacion-por-haber-sufrido-danos-y-perjuicios-derivados-de-una-infraccion-en-materia-de-proteccion-de-datos-estudio-del-art-82-del-rgpd/ [Fecha de Consulta: 16 de septiembre de 2022].

45 https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

46 Rubí Puig, A.: "Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD", *Revista de Derecho Civil,* vol V, nº 4, 2018, pp. 80 y ss., disponible en http://www.nreg.es/ojs/index.php/RDC/article/view/354.

IV. RESPONSABILIDAD CIVIL DE LAS PLATAFORMAS EN EL METAVERSO: PERSPECTIVA DE FUTURO.

A día de hoy otro concepto que está de plena actualidad es el "Metaverso", y una de las cuestiones que se plantea es ¿cómo se constituye la identidad digital en el Metaverso? ¿Cómo evolucionará la responsabilidad de las plataformas en este nuevo mundo digital?

Brevemente, el Metaverso según Barrio Andrés "una aplicación de Internet que consiste en un ecosistema virtual y tridimensional (3D) en el que los usuarios interactúan entre ellos, desarrollan actividades de ocio (muy destacadamente, jugar a videojuegos o e-sports), entablan relaciones económicas o de cualquier otro tipo, como sucede hoy en la Red"[47].

En el metaverso tendríamos nuestros "yos virtuales" dentro un mundo virtual paralelo al real a través de la creación de avatares virtuales. Pero ¿a qué nos referimos exactamente con avatar en el metaverso? Según Park y Quim un avatar es un alter ego que ha cambiado su funcionalidad en el metaverso, pues "anteriormente, el avatar se usaba como una forma exagerada predefinida en el mundo virtual en lugar de reflejar el mundo real. Sin embargo, cambia gradualmente a una forma ideal que proyecta la apariencia exterior y refleja el ego"[48]. En el metaverso dichos avatares adquieren personalidad propia con vestimentas o complementos concretos y van difuminando poco a poco la distancia entre la identidad física y la identidad digital.

Así, en el metaverso la socialización mediante avatares nos permite reunirnos con nuestros amigos del mundo físico, con independencia de donde estén, para compartir actividades. Igualmente, también nos permite transitar por este universo y conocer gente, compartir actividades de ocio e intimar de diversas formas con nuestros iguales[49].

Igualmente, con el metaverso se habla de una nueva "identidad soberana", en la que a través de técnicas de blockchain los ciudadanos recuperarían la gobernanza sobre los datos que conforman su identidad digital.

En la web 3 a través de iniciativas como el metaverso o la cartera de identificación europea transfronteriza anteriormente señalada, se parte de una

47 Barrio Andrés, M.: "Metaverso: origen, concepto y aplicaciones", *Derecho Digital e Innovación*, Nº 12, Sección Doctrina, Segundo trimestre de 2022, Wolters Kluwer, LA LEY 6042/2022.

48 PARK, S. M., & KIM, Y. G.: "A Metaverse: Taxonomy, components, applications, and open challenges", *Ieee Access*, nº 10, 2022, págs. 4209-4251.

49 Bueno De Mata, F.: "Del metaverso a la metajurisdicción..", *cit.,* pp. 3 y ss.

identidad auto-soberana ya no se dependería de prestadores de servicios de la comunicación, sino que los usuarios serían los gobernantes de su propia identidad.

En la Web 3.0, se utilizará la tecnología blockchain, es descentralizada pero interoperable a la vez, es decir, vale para ser usada en cualquier tipo de plataforma electrónica sin que la misma guarde, recopile o gestione nuestros datos. La autogestión permite que una persona pueda autenticarse a sí misma, afirmar sus atributos de identidad y controlar declaraciones de identidad realizadas por terceros. Con esto, la responsabilidad es del individuo y las plataformas no son responsables al no alojar información sin un contrato de adhesión que apruebe esta exención, sino que se entenderá de forma implícita.

Diferente y complejo es el tema del metaverso puesto que no es lo mismo configurar un único metaverso como una nueva evolución de Internet, a hablar realmente de un multiverso configurado a través de plataformas, no es lo mismo que hablar de Metaverso como una evolución de la Red de Redes y con unos patrones tecnológicos determinados. Es decir, realmente para poder determinar cómo debiéramos resolver los conflictos en el metaverso y la responsabilidad que los mismos llevan aparejados, tal y como indica Bueno de Mata[50], es fundamental determinar si nos vamos a encontrar con un único metaverso o a un multiverso de plataformas intermediarias. En este sentido, si partimos de esta última opción como parece que será lo que finalmente ocurra, tendremos que acudir a una normativa mundial sobre esta realidad, que abogue por el uso de la identidad digital auto-soberana y que por tanto redunde en una exención de responsabilidad de las plataformas intermediarias al no tratar ellos propiamente la información y avanzar hacia la autogestión en el tratamiento de los datos por aplicación de la tecnología blockchain.

En definitiva, según la idea manifestada por el citado autor, nos encontramos ante un problema no estrictamente jurídico, sino que también se entrelazan en ellos cuestiones puramente económicas y empresariales en el manejo y posesión de datos de particulares.

V. CONCLUSIONES.

A modo de reflexión final, podemos afirmar que hoy en día nos encontramos ante un nuevo fenómeno en auge: el reconocimiento jurídico de la identidad digital. En este sentido, el concepto legal de identidad digital está en constante evolución y aún no existe una definición global y unificada. La regulación internacional de la

50 Bueno De Mata, F.: "Del metaverso a la metajurisdicción..", *cit.*, pp. 4.

identidad digital también es incierta, y aunque existen iniciativas para regularla, todavía queda mucho camino por recorrer.

Hoy en día este concepto está ligado a las redes sociales y al concepto de Web2. En este contexto, las plataformas digitales que ofrecen este servicio manejan nuestra información y, es por tanto medular, saber a qué tipo de responsabilidades se enfrentan y cuáles son las acciones que los usuarios poseen para reclamar un uso inadecuado en el tratamiento de los datos personales. En esta investigación hemos intentado ofrecer un panorama concreto de la responsabilidad derivada en este caso, siendo conscientes de que el tema puede plantear muchos interrogantes debido a la casuística tan grande que lleva aparejada.

Por último y unido a lo anterior, podemos observar como la tecnología blockchain y la identidad digital auto-soberana son parte de esta evolución tecnológica, y vienen llamados a revolucionar el esquema de responsabilidad anteriormente apuntado.

En este sentido, este modelo permitirá a los usuarios tener el control total y propio de su identidad sin la necesidad de intermediarios o proveedores de información tecnológicos, pero aún si un marco legal definido, en espera de que el Reglamento eIDAS2 sea aprobado. Si finalmente esta normativa entrara en vigor, conllevará una revolución social y tecnológica sin precedentes, que a su vez tendrá reflejo jurídico en muchos aspectos en el tratamiento de datos tal y como lo conocemos hoy en día.

Sin duda, nos encontramos ante un modelo con un potencial aún indescifrable, donde también encajará la futura web3 y los servicios de realidad virtual inmersiva. Todas estas cuestiones deberán ser desarrolladas a nivel legal en los próximos años, por lo que hoy en día nos encontramos en un terreno plagado de sombras y lagunas, que esperamos vean la luz con prontitud con el fin de garantizar un escenario legal seguro y garantista.

BIBLIOGRAFÍA

ALAMILLO DOMINGO, I.: "La identidad descentralizada como garantía de la privacidad en la vida digital", *La Ley privacidad*, N.º 5, Sección El foro de la privacidad, Tercer trimestre de 2020, Wolters Kluwer, LA LEY 9425/2020.

ÁLVAREZ HERNANDO, J.: "Análisis jurídico de la acción de reclamación de una indemnización por haber sufrido daños y perjuicios derivados de una infracción en materia de protección de datos. Estudio del art. 82 RGPD", enero de 2019, https://www.ac-abogados.es/analisis-juridico-de-la-accion-de-reclamacion-de-una-indemnizacion-por-haber-sufrido-danos-y-perjuicios-derivados-de-una-infraccion-en-materia-de-proteccion-de-datos-estudio-del-art-82-del-rgpd. [Fecha de Consulta: 16 de septiembre de 2022].

ALLENDE LÓPEZ, M.: *Identidad digital autosoberana,* 2020, Disponible en: https://www.icd.go.cr/portalicd/images/docs/uif/doc_interes/acerca_uif/IDENTIDADDIGITAL.pdf

ALLEN, C.: "the path to self-Sorevering Identity", en su blog *life With Alacrity*. A blog on social software, collaboration, trust, security, privacy, and internet tools, 25 de abril de 2106. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

APARICIO VAQUERO, J.P.: "La protección de datos que viene: el nuevo Reglamento General europeo", *Ars Iuris Salmanticensis: AIS: revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología*, ISSN-e 2340-5155, Vol. 4, Nº. 2, 2016, pp. 27-34.

"Cuestiones de derecho aplicable y responsabilidad de los prestadores de servicios de red social y de sus usuarios", en *torno a la privacidad y la protección de datos en la sociedad de la información*, Comares, Granada, 2015, pp.187-231.

ARK, S. M., & KIM, Y. G.: "A Metaverse: Taxonomy, components, applications, and open challenges", *Ieee Access,* nº 10, 2022, pp. 4209-4251.

BARRIO ANDRÉS, M.: "Metaverso: origen, concepto y aplicaciones", *Derecho Digital e Innovación*, Nº 12, Sección Doctrina, Segundo trimestre de 2022, Wolters Kluwer, LA LEY 6042/2022.

BUENO DE MATA, F.: "Del metaverso a la metajurisdicción: desafíos legales y métodos para la resolución de conflictos generados en realidades virtuales inmersivas", *Derecho de privacidad y derecho digital*, ISSN 2444-5762, Vol.7, Núm. 27, 2022, pp. 19-59.

-El derecho de acceso universal a internet: reconocimiento legal y perspectiva procesal", *Nuevos retos en materia de derechos digitales en un contexto de pandemia: perspectiva multidisciplinar*, Aranzadi, Navarra, 2022, pp. 69-89.

Faus Pujol, M.: *Práctico Obligaciones y Contratos*, Vlex.com, diciembre 2022.

Martínez Rodríguez, N.: "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales", *Ars Iuris Salmanticensis: AIS: revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología*, ISSN-e 2340-5155, Vol. 7, Nº. 1, 2019, pp. 254-259.

Merchán Murillo, A.: "Identidad digital Blockchain e Inteligencia Artificial: aspectos jurídicos de presente y futuro a debate", *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, ISSN-e 2444-8478, Vol. 7, Nº. 1, 2021, pp. 183-203.

López Calvo, J.: *Comentarios al Reglamento Europeo de Protección de Datos*, Sepin, Madrid, 2017.

Llanera González, P.: *Identidad digital. Actualizado a la Orden ETD/465/2021, de 6 de mayo (sobre métodos de identificación remota) y a la propuesta de Reglamento eIDAS2*, Bosch, Barcelona, 2021.

Llamas Pombo, E.: *Manual de Derecho Civil. Vol.VII. Derecho de Daños*, Eugenio Llamas Pombo (dir.), La Ley, Madrid, 2021.

Pérez Bes, F.: "Identidad y blockchain", en *Criptoderecho. La regulación de blockchain*, edición nº 1, LA LEY, 2018, LA LEY 13760/2018.

Platero Alcón, A.: *Análisis de la normativa europea y española de protección de datos personales: régimen de responsabilidad civil derivado de un incorrecto tratamiento de dato personales*, Tesis doctoral, dirigida por Carlos Lasarte Álvarez (dir. tes.), Ángel Acebo Penco (codir tes.) Universidad de Extremadura, 2020.

"la responsabilidad de las redes sociales: el caso de Ashley Madison", *Boletín Mexicano de Derecho Comparado*, nueva serie, año XLIX, núm. 150, septiembre-diciembre de 2017, pp. 1259-1288, https://revistas.juridicas.unam.mx/index.php/derecho-comparado/issue/archive

Puyol Montero, J.: *La tecnología «Blockchain» y la identidad digit*al, en: https://confilegal.com/20190325-125312. [Fecha de consulta: 5 de septiembre de 2022]

RUBÍ PUIG, A.: "Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD", *Revista de Derecho Civil,* vol V, nº 4, 2018, pp. 53-87, disponible en http://www.nreg.es/ojs/index.php/RDC/article/view/354.

VVAA.: *Identidad Digital: El nuevo usuario en el mundo digital*, Coordinación editorial de Fundación Telefónica: Rosa María Sáinz Peña, Planeta, Madrid, 2013.

VVAA.: "Diálogos para el futuro judicial XVII. Identidad digital y proceso judicial", coord. Álvaro Perea González (Letrado de la Administración de Justicia). *Diario La Ley*, Nº 9777, Sección Plan de Choque de la Justicia, Encuesta, 25 de enero de 2021, Wolters Kluwer.

VV.AA.: *Algunos desafíos en la protección de datos personales*, Alfredo Batuecas Caletrío (dir.), Juan Pablo Aparicio Vaquero (dir.), Editorial Comares, Granada, 2018.

VV.AA.: *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, coord., José López Calvo, Wolters Kluwer, Bosch, Madrid, 2019.

VV.AA.: *Protección de datos, Memento práctico,* dir. José Luis Piñar Mañas, coord. Miguel Recio Gayo, Francis Lefebvre, Barcelona, 2022.