Las transferencias de datos a través del Metaverso a la luz de los últimos acuerdos (UE - EE.UU.). El fenómeno "tú a Londres y yo a California"

Data transfers through the Metaverse in the light of the latest agreements (EU-US). The "parent trap" phenomenon

Jonatán Cruz Ángeles
Profesor Contratado Doctor de Derecho Internacional Público y Relaciones Internacionales
Universidad de Jaén
ORCID ID: 0000-0002-8648-5525

Recibido: 16.06.2023 / Aceptado: 10.07.2023
DOI: 10.20318/cdt.2023.8056

Resumen: Este artículo realiza un análisis exhaustivo de las transferencias extracomunitarias de datos, vitales para la implementación y gestión del Metaverso, con un enfoque particular en las regulaciones de la Unión Europea y Estados Unidos. Se enfoca en la repercusión de las decisiones jurídicas más cruciales del Tribunal de Justicia de la Unión Europea respecto a la protección de los datos personales de los ciudadanos europeos en estos espacios virtuales emergentes. Involucra un estudio detallado de la doctrina especializada para determinar si el Acuerdo recientemente revelado entre la Unión Europea y los Estados Unidos, el 10 de julio de 2023, es suficientemente robusto o si, en su defecto, es necesario investigar otras alternativas o medidas que deberían ser consideradas por gigantes tecnológicos como Meta. El objetivo último es dilucidar la extensión real y efectiva de los derechos a la privacidad y la salvaguarda transatlántica de los datos personales en el ámbito digital contemporáneo.

Palabras clave: Metaverso, transferencias transatlánticas de datos, normativa comunitaria, extraterritorialidad, escudo de protección de datos, protección de datos, Estados Unidos.

Abstract: This article conducts a comprehensive analysis of extra-EU data transfers, vital for the implementation and management of the Metaverse, with a particular focus on the regulations of the European Union and the United States. It focuses on the impact of the most crucial legal decisions of the European Court of Justice regarding the protection of European citizens' personal data in these emerging virtual spaces. It involves a detailed study of specialized doctrine to determine whether the recently unveiled Agreement between the EU and the U.S. on July 10, 2023 is sufficiently robust or whether, failing that, other alternatives or measures need to be investigated that should be considered by technology giants such as Meta. The ultimate goal is to elucidate the real and effective extent of privacy rights and transatlantic safeguarding of personal data in the contemporary digital realm.

Keywords: Metaverse, transatlantic data transfers, EU law, extraterritoriality, data protection shield, data protection, United States.

respetar, proteger y cumplir. V. La determinación de la jurisdicción en el Metaverso. 1. La necesidad de cooperación en el Metaverso. 2. La aplicación extraterritorial del Derecho de la Unión Europea. 3. La protección de datos como valor europeo. VI. La recolección (i)lícita de todo tipo de datos. VII. Los acuerdos transatlánticos en materia de protección de datos. VIII. El nuevo Acuerdo Transatlántico de Transferencia de Datos. IX. El Efecto Bruselas y la praxis estadounidense. X. Conclusiones.

I. Introducción

1. En la actualidad (2023), nos encontramos en la cúspide de una nueva era digital: la emergencia del Metaverso[1], un universo paralelo y digital que está moldeando un nuevo tipo de interacción humano-tecnológica[2]. Este fenómeno, caracterizado por su capacidad para trascender las fronteras geográficas y disolver las barreras entre lo virtual y lo físico, ha generado una serie de cuestiones jurídicas y éticas sin precedentes. En particular, ha llevado a un intenso debate sobre la privacidad de los datos y su transferencia entre diferentes jurisdicciones. Este artículo se propone examinar detalladamente esta cuestión, centrándose en el fenómeno de las transferencias transatlánticas de datos en el Metaverso. Para ello, abordamos lo que hemos denominado el fenómeno "Tú a Londres y yo a California", una metáfora que encapsula la complejidad de las cuestiones jurídicas y éticas que surgen en este entorno digital globalizado[3]. En este contexto, "Tú a Londres" puede simbolizar la estrategia de ciertas empresas de establecerse en el Reino Unido debido a la ventaja lingüística que representa para operar con la Unión Europea (UE). A pesar del Brexit, muchas empresas eligen el Reino Unido como base europea por el idioma inglés y las conexiones históricas y económicas con el continente, siempre teniendo en cuenta el marco regulatorio de protección de datos de la UE, incluido el Reglamento General de Protección de Datos (RGPD). Por otro lado, "Yo a California" puede ser visto como una referencia a la perspectiva de los Estados Unidos (EE.UU.), específicamente de Silicon Valley (ubicado en California), donde se encuentran la mayoría de los gigantes tecnológicos. La legislación estadounidense en materia de protección de datos difiere de la de la UE y a menudo es considerada más permisiva en términos de privacidad del usuario[4]. Esta metáfora pone de relieve los desafíos que enfrentan las empresas de tecnología al tratar

[1] G. Riva/B. K. Wiederhold, "What the metaverse is (really) and why we need to know about it", *Cyberpsychology, Behavior, and Social Networking*, vol. 25, nº 6, 2022, pp. 355-359. [En línea] Disponible en: https://doi.org/10.1089/cyber.2022.0124

[2] Véanse, *inter alia*, L. Angelini, M. Mecella, H.N. Liang, M. Caon, "Towards an emotionally augmented metaverse: a framework for recording and analysing physiological data and user behaviour". En: *13th Augmented Human International Conference*, 2020. https://doi.org/10.1145/3532530.3532546. N. Dozio, F. Marcolin, G. Scurati, L. Ulrich, F. Nonis, E. Vezzetti, G. Marsococi, A. La-Rosa, F. Ferrise, "A design methodology for affective virtual reality", *International Journal of Human-Computer Studies,* vol. 162, 2022. [En línea] Disponible en: https://doi.org/10.1016/j.ijhcs.2022.102791

[3] Apriorísticamente, el Metaverso, en tanto que entorno digital globalizado, plantea una serie de desafíos jurídicos y éticos complejos, *inter alia*: (1) Jurisdicción y aplicabilidad del Derecho: uno de los desafíos más significativos en el Metaverso es determinar qué normativas son aplicables en una plataforma que trasciende las fronteras nacionales. Por ejemplo, ¿se aplicaría la normativa de privacidad de datos de la UE a un ciudadano europeo que utiliza un servidor ubicado en EE.UU.? Estas cuestiones pueden ser especialmente complicadas dada la variedad de normativas existentes y la rápida evolución de la tecnología. (2) Protección de datos y privacidad: la UE y EE.UU. tienen enfoques distintos sobre la privacidad y protección de datos. Mientras que la UE ha establecido fuertes medidas de protección de datos con el Reglamento General de Protección de Datos, los EE.UU. carecen de una ley federal equivalente. Esto plantea cuestiones sobre cómo se deben proteger los datos personales en el Metaverso, especialmente cuando los datos cruzan nuestras fronteras. (3) Seguridad cibernética: el Metaverso, al ser una red digital, es vulnerable a los ataques cibernéticos. La protección contra tales amenazas y la atribución de responsabilidad cuando ocurren son cuestiones jurídicas complicadas que aún deben ser plenamente abordadas. (4) Derechos de propiedad intelectual: el Metaverso presenta nuevos desafíos para los derechos de propiedad intelectual, como los derechos de autor y las marcas comerciales. ¿Cómo se aplican estas normativas a los contenidos creados y compartidos en un espacio virtual global? (5) Ética y equidad: más allá de las cuestiones puramente jurídicas, el Metaverso también plantea cuestiones éticas. ¿Cómo se garantiza que este nuevo espacio digital sea inclusivo y accesible para todos, independientemente de su ubicación geográfica o nivel socioeconómico? ¿Cómo se abordan los problemas de sesgo y discriminación que pueden surgir con el uso de algoritmos e Inteligencia Artificial? La solución a estos desafíos requiere un enfoque holístico y colaborativo que incluya la cooperación internacional y la participación de diversas partes interesadas, incluidos los gobiernos y los principales *stakeholders* implicados, es decir, las empresas tecnológicas y los ciudadanos. La complejidad de estas cuestiones subraya la necesidad de un marco jurídico y ético sólido para guiar el desarrollo y uso del Metaverso.

[4] C.J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States,* Cornell University Press, 1992.

de operar entre estas dos jurisdicciones con regulaciones tan distintas. Este asunto es particularmente relevante en el Metaverso, donde la ubicación de los servidores y la transferencia de datos pueden resultar ambiguas debido a la naturaleza virtual y globalizada de este espacio. La falta de concordancia y armonización entre ambos ordenamientos jurídicos genera una inseguridad jurídica que puede obstaculizar el desarrollo y la expansión segura del Metaverso.

2. El presente estudio aspira a desentrañar y examinar los desafíos intrínsecos a la protección de datos en el Metaverso, enfocándose particularmente en las transferencias de datos entre la UE y los EE.UU. Para ello, nuestra investigación sigue un hilo argumentativo que empieza conceptualizando el Metaverso, esclareciendo sus características esenciales y su relación con la privacidad y la identidad virtual[5]. Además, profundizamos en las obligaciones y responsabilidades que surgen del marco legal europeo. Se indaga en los preceptos comunitarios de respeto, protección y cumplimiento, y cómo estos se aplican y adaptan al dinámico y, a menudo, nebuloso terreno del Metaverso. Parte de este análisis se centra en cómo la UE valora y protege los datos personales como un bien o un derecho fundamental[6]. La investigación avanza hacia una consideración detallada de los problemas de jurisdicción en el Metaverso[7]. Al tratarse de un entorno digital que trasciende fronteras geográficas, es crucial explorar la necesidad de cooperación global en la gobernanza del Metaverso y examinar la aplicabilidad extraterritorial del Derecho de la UE[8]. Finalmente, se analiza en profundidad la recolección de datos en el Metaverso, un asunto de creciente preocupación. Este análisis incluye tanto la recopilación legítima como ilegítima de datos, destacando las responsabilidades de las entidades que operan en el Metaverso y las posibles soluciones para mejorar la protección de los usuarios.

3. En una segunda parte de nuestra investigación, se hará un análisis exhaustivo de los acuerdos transatlánticos en materia de protección de datos, prestando especial atención al nuevo Acuerdo Transatlántico de Transferencia de Datos. Este acuerdo representa un hito importante en el desarrollo de un marco legal para las transferencias de datos transatlánticas y su análisis proporcionará una visión valiosa de las perspectivas futuras en este ámbito. Finalmente, reflexionaremos sobre el llamado "Efecto Bruselas" y cómo la práctica estadounidense puede ser influenciada o ajustada en función de los desarrollos legales europeos. Este análisis crítico buscará iluminar las tensiones y oportunidades que surgen de este diálogo transatlántico en torno a la protección de datos. En suma, el presente estudio se propone como una contribución vital al discurso jurídico en torno a la protección de datos en el Metaverso. Mediante un análisis exhaustivo y riguroso, se espera que este trabajo sirva como un recurso valioso para los legisladores, profesionales del Derecho y la tecnología, así como para cualquier persona, lego en Derecho, interesada en comprender las implicaciones legales y éticas de este nuevo universo digital.

II. Distinguiendo entre "Metaverso" y "metaversos"

4. La emergencia y popularización de los espacios digitales interactivos ha propiciado la aparición del concepto de Metaverso. Para disipar cualquier confusión que pueda surgir de las distintas interpretaciones de este término, resulta crucial hacer una distinción entre "Metaverso" y "metaversos". Esta diferenciación es especialmente relevante en discusiones académicas y jurídicas donde los matices son fundamentales. Cuando nos referimos al "Metaverso", con M mayúscula, aludimos a la idea global

[5] R. Di-Pietro/ S. Cresci, "Metaverse: security and privacy issues", en *3rd IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications,* TPS-ISA 2021, 2021, pp. 281-288. [En línea] Disponible en: https://doi.org/10.1109/TPSISA52974.2021.0003

[6] G.G. Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, 2014.

[7] Véanse, *inter alia*, U. Kohl, *Jurisdiction and the Internet: Regulatory Competence over Online Activity*, Cambridge University Press, 2007. U. Kohl, "Jurisdiction in Cyberspace", en N. Tsagourias, R. Buchan (eds), *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, 2015.

[8] F. Bignami/ G. Resta, "Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance", en E. BENVENISTI, G. NOLTE (eds.), *Community Interests across International Law*, Oxford University Press, 2018.

de un universo digital completamente integrado. Este Metaverso engloba la totalidad de los espacios digitales interactivos, las redes sociales[9], los videojuegos[10] y otras manifestaciones de realidad virtual y aumentada. En este sentido, el Metaverso puede ser entendido como una red o sistema digital global. Éste representa una versión de Internet tridimensional e inmersiva que trasciende las fronteras de las aplicaciones y plataformas individuales, abarcando una integración de todas las formas de realidad, desde la física hasta la virtual y la aumentada. Por otro lado, el término "metaversos", con m minúscula, se utiliza para referirse a los mundos digitales individuales o plataformas que existen dentro del marco más amplio del Metaverso. Cada uno de estos metaversos, aunque forma parte de la estructura mayor del Metaverso, posee sus propias características y reglas únicas. Así las cosas, los metaversos son espacios virtuales de interacción que, a pesar de estar interconectados, mantienen sus propias particularidades y rasgos diferenciadores. Éstos pueden abarcar desde juegos de realidad virtual y entornos laborales virtuales hasta redes sociales específicas y mundos digitales personalizados. Conceptualmente, es vital entender que tanto el Metaverso como los metaversos que lo componen son entidades dinámicas y en constante cambio, moldeadas tanto por las tecnologías que las posibilitan como por las interacciones y comportamientos de los usuarios que las habitan. De esta manera, los metaversos son tanto un producto de la tecnología como de la cultura, y la tensión entre estos dos factores puede dar lugar a una diversidad de experiencias y contextos.

5. En estos nuevos mundos virtuales, en tanto que juristas, el estudio de la privacidad y el reconocimiento de la identidad virtual en el contexto del Metaverso y los metaversos que lo constituyen supone un desafío particular. La proliferación de datos personales y la creciente integración de las identidades *on line* y *off line* nos obligan a reevaluar nuestras nociones tradicionales de privacidad. En este sentido, las obras de autoras como Julie E. Cohen y Helen Nissenbaum ofrecen ideas muy útiles. Cohen propone que la privacidad en el entorno digital debe enfocarse en preservar "espacios de reserva" para la autonomía personal y la construcción del yo[11]. Por otra parte, Nissenbaum sostiene que la privacidad debería garantizar un uso adecuado de la información personal según el contexto en el que se recolecta, una teoría conocida como "privacidad contextual"[12]. Además, el reconocimiento de la identidad virtual, como destaca Sherry Turkle, se vuelve crucial en el Metaverso y los metaversos[13]. La posibilidad de adoptar varias identidades y expresarse de maneras innovadoras y fluidas genera preguntas sobre el reconocimiento y la protección legal de estas identidades. El planteamiento de este tipo de cuestiones

[9] S. Kraus, D. K. Kanbach, P. M. Krysta, M. Steinhoff, N. Tomini, "Facebook and the creation of the metaverse: radical business model innovation or incremental transformation?", *International Journal of Entrepreneurial Behaviour and Research*, vol. 28, nº 9, 2022, pp. 52-77. [En línea] Disponible en: https://doi.org/10.1108/IJEBR-12-2021-0984

[10] J. Han, J. Heo, E. You, "Analysis of metaverse platform as a new play culture: focusing on Roblox and Zepeto", en *CEUR Workshop Proceedings*, 3026 (Computing4Human 2021), 2021, pp. 27-36. [En línea] Disponible en: https://pesquisa.bvsalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/pt/covidwho-1589569

[11] En su obra, Julie E. Cohen proporciona una valiosa contribución al debate sobre la privacidad en el entorno digital. Cohen aboga por la protección de los "espacios de reserva" que permiten la autonomía personal y la construcción de la identidad. Esta visión entiende la privacidad no sólo como un derecho a ocultar información, sino como un componente esencial del desarrollo y la autodeterminación individual en un mundo cada vez más interconectado. La capacidad de controlar el acceso a estos espacios, así como la capacidad de definir y moldear la identidad personal en el Metaverso, son considerados por Cohen como aspectos esenciales de la privacidad digital. Véase J.E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, Yale University Press, 2012.

[12] Helen Nissenbaum plantea la teoría de la "privacidad contextual". Según Nissenbaum, la privacidad no puede ser vista de manera absoluta, sino que su alcance y protección dependen del contexto específico en el que la información personal se recoge y utiliza. Este enfoque enfatiza la importancia de considerar las normas sociales, las expectativas y los roles específicos de cada contexto al evaluar si el uso de la información personal es apropiado o no. La privacidad contextual se convierte en una herramienta relevante en el Metaverso, donde diferentes metaversos pueden tener diferentes normas y expectativas sobre la privacidad. Véase H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009.

[13] Sherry Turkle hace hincapié en la importancia del reconocimiento de la identidad virtual en los entornos digitales. Para Turkle, la posibilidad de adoptar varias identidades y expresarse de maneras innovadoras y fluidas en el Metaverso genera preguntas sobre el reconocimiento y la protección legal de estas identidades. Las implicaciones de esta capacidad de cambio de identidad en el entorno virtual van más allá de la mera privacidad, alcanzando cuestiones de autenticidad, responsabilidad y derechos individuales. Véase S. Turkle, *Life on the Screen: Identity in the Age of the Internet*, Simon & Schuster, 1999.

requiere de un estudio más profundo sobre la (de)construcción de la *privacy* estadounidense, así como de la concepción europea del derecho a la protección de datos en espacios virtuales y será el tema principal que abordaremos en la siguiente sección de este trabajo.

III. La protección de la intimidad, la vida privada y la *privacy* en el Metaverso

6. La incursión en la era digital, reforzada por el surgimiento del Metaverso, ha infundido un nuevo significado al reconocimiento y protección del derecho a la privacidad y a la vida privada[14]. La expansión tecnológica, desde la aparición de Internet hasta el auge del Metaverso, en tanto que universo virtual que interconecta múltiples espacios digitales[15], ha propiciado la recopilación, almacenamiento, análisis y comercialización de enormes volúmenes de datos personales[16]. Este nuevo contexto añade un nivel extra de complejidad, albergando no sólo datos personales, sino también avatares e interacciones virtuales, incitando a la reevaluación de la definición de "privacidad" en una sociedad crecientemente digitalizada y virtual.

7. El análisis digital de la vida de una persona, que se extiende ahora al Metaverso, ha planteado preocupaciones globales acerca de la necesidad de adaptar nuestro marco jurídico comunitario a estos escenarios digitales y meta-digitales[17]. La evolución del derecho a la protección de la intimidad, vida privada y privacidad, tanto en la realidad física como en el Metaverso, es un proceso prolongado y complejo que involucra numerosos tratados internacionales, los cuales estudiaremos a continuación.

8. El primer hito en esta evolución es el artículo V de la Declaración Americana de los Derechos y Deberes del Hombre, que inspiró la redacción del artículo 12 de la Declaración Universal de Derechos Humanos de 1948[18]. Estos artículos, aunque no detallan cómo se deberían proteger estos derechos, establecen que "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia", marcando el comienzo de la privacidad como un derecho humano.

9. Posteriormente, en 1950, el Convenio Europeo de Derechos Humanos (CEDH) consagra en su artículo 8 el derecho al respeto de la vida privada y familiar, del domicilio y de la correspondencia[19].

---

[14] R. Leenes, "Privacy in the metaverse: regulating a complex social construct in a virtual world", en *IFIP International Federation for Information Processing*, vol. 262, 2008, pp. 95-112. [En línea] Disponible en: https://doi.org/10.1007/978-0-387-79026-8_7

[15] W.J. Au, "Taking new world notes: an embedded journalist's rough guide to reporting from inside the Internet's next evolution", *First Monday*, 2005. https://doi.org/10.5210/fm.v0i0.1562

[16] F. H. Cate, "The Changing Face of Privacy Protection in the European Union and the United States", *Indiana Law Review*, vol. 33, nº 1, 1999, p. 173.

[17] Para un estudio más detallado sobre la regulación intracomunitaria aplicable al Metaverso, *vid.* J. Cruz Ángeles, "Los guardianes de acceso al Metaverso. (Re)pensando el Derecho de la competencia de la Unión Europea", *Cuadernos de Derecho Transnacional*, vol. 15, nº 1, 2023, pp. 275-296; y también J. Cruz Ángeles, "Las obligaciones jurídico-comunitarias de las grandes plataformas proveedoras de servicios digitales en la era del Metaverso", *Cuadernos de Derecho Transnacional*, vol. 14, nº 2, 2022, pp. 294-318.

[18] La Declaración Universal de Derechos Humanos fue adoptada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948 en París. Esta declaración establece, en 30 artículos, los derechos humanos fundamentales que deben protegerse a nivel mundial. El artículo 12 específicamente se refiere al derecho a la privacidad. Aunque no es un tratado legalmente vinculante, ha inspirado una serie de tratados internacionales de derechos humanos, legislaciones nacionales y constituciones en todo el mundo.

[19] Originalmente, en 1950, el CEDH consagró en su artículo 8 el derecho al respeto de la vida privada y familiar, del domicilio y de la correspondencia. Este marco normativo, en su momento, establecía restricciones a este derecho sólo en situaciones específicas y en la medida que fuera necesario en una sociedad democrática. Sin embargo, cabe destacar que, cuando el legislador redactó el artículo 8, probablemente no contempló su aplicación a las complejidades y problemáticas contemporáneas que emergen con los desarrollos tecnológicos y digitales en nuestro mundo actual. La interpretación y aplicación del artículo, tal como fue redactado en aquel entonces, puede parecer limitada en su alcance frente a los desafíos actuales. A pesar de esto, gracias a la labor del Tribunal Europeo de Derechos Humanos (TEDH), como máximo intérprete del Convenio, ha habido un esfuerzo por contextualizar y adaptar el espíritu de este artículo a las necesidades contemporáneas. La interpretación dinámica y

Este Convenio establece un marco para la restricción de este derecho en situaciones específicas y en la medida que sea necesario en una sociedad democrática.

10. El artículo 17.1 del Pacto Internacional de Derechos Civiles y Políticos en 1966[20] y el artículo 11(2) de la Convención Americana sobre Derechos Humanos en 1969 reafirman la importancia de la privacidad y prohíben las interferencias arbitrarias o ilegales en la privacidad, la familia, el hogar y la correspondencia, así como los ataques ilegales a la honra y la reputación[21].

11. El último cuarto del siglo XX vio un cambio significativo en cómo se manejan los datos personales. Se desarrollaron regulaciones de protección de datos en Europa y EE.UU., como las Prácticas Justas de Información (FIPPs) establecidas en 1973 por el Departamento de Salud, Educación y Bienestar (DHEW) de los EE.UU. Estos principios influenciaron normativas emergentes de protección de datos en todo el mundo y se convirtieron en la inspiración para los principios de protección de datos de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en 1980[22].

12. El Convenio 108 del Consejo de Europa en 1981 se convirtió en el primer instrumento internacional legalmente vinculante en el campo de la protección de datos[23], y en el año 2000, la Carta de Derechos Fundamentales de la UE añadió protecciones adicionales para la privacidad y los datos personales[24].

13. A medida que avanzaba el siglo XXI, el Tratado de Funcionamiento de la UE (TFUE) en 2007 reconoció explícitamente la protección de los datos personales como un derecho fundamental, reflejando la creciente importancia de este tema en el contexto digital. Además, la Directiva de Protección de Datos de la UE, oficialmente conocida como Directiva 95/46/CE, fue otro hito importante en

progresiva del TEDH, a la luz de las realidades de nuestro tiempo, ha permitido que el artículo 8 siga siendo una norma efectiva y relevante para la protección de los derechos humanos en el contexto actual.

[20] El Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea General de las Naciones Unidas el 16 de diciembre de 1966, garantiza el derecho a la privacidad en su artículo 17.1. Para activar la protección de esta cláusula, los Estados Parte deben presentar informes periódicos sobre su implementación al Comité de Derechos Humanos de la ONU. Además, los individuos que consideren que han sufrido violaciones de su derecho a la privacidad pueden presentar comunicaciones individuales al Comité después de agotar los recursos internos disponibles en su país.

[21] La Convención Americana sobre Derechos Humanos, también conocida como el Pacto de San José, adoptada el 22 de noviembre de 1969, prohíbe las interferencias arbitrarias o abusivas en la vida privada, la familia, el hogar y la correspondencia en su artículo 11(2). Para garantizar el cumplimiento de esta cláusula, los Estados Parte deben presentar informes periódicos sobre su implementación a la Comisión y a la Corte Interamericana de Derechos Humanos. Además, los individuos que consideren que han sufrido violaciones de su derecho a la privacidad pueden presentar peticiones individuales, conocidas como "casos", ante la Comisión Interamericana de Derechos Humanos después de agotar los recursos internos disponibles en su país. En algunos casos, las decisiones de la Comisión pueden ser llevadas ante la Corte Interamericana para su revisión y emisión de un fallo o sentencia vinculante.

[22] Los principios de protección de datos de la OCDE se basan en una serie de valores fundamentales que deben tenerse en cuenta al tratar de datos personales. Estos principios son los siguientes: (1) limitación de la recopilación de datos, (2) calidad de los datos, (3) propósito específico, (4) consentimiento, (5) seguridad de los datos, (6) transparencia, (7) acceso y corrección y (8) responsabilidad. Estos principios han sido ampliamente adoptados en todo el mundo y han sentado las bases para el desarrollo de distintas normativas tanto nacionales como internacionales. La OCDE ha desempeñado un papel fundamental en la promoción de la privacidad y la protección de datos como derechos fundamentales en la era digital.

[23] El Convenio 108 del Consejo de Europa, adoptado en 1981, es un tratado que protege los derechos fundamentales de las personas en relación con el procesamiento automatizado de datos personales. Establece principios como la limitación de la recopilación de datos, el consentimiento informado, el acceso y corrección de datos y la seguridad de la información. Destaca por su enfoque en la cooperación internacional y ha sido complementado por otras normativas, como el RGPD.

[24] La Carta de Derechos Fundamentales de la UE garantiza una sólida protección a la privacidad y los datos personales en sus artículos 7 y 8. El artículo 7 protege el derecho al respeto de la vida privada y familiar, mientras que el artículo 8 garantiza el derecho a la protección de los datos personales. Estos preceptos establecen que los datos deben ser tratados de manera justa y transparente, y que las personas tienen derecho a acceder, corregir y eliminar sus datos. La Carta no sólo protege los derechos individuales, sino que también impone obligaciones a los Estados y las instituciones de la UE para respetar y proteger la privacidad y los datos personales de las personas (A. Mangas Martín (dir), *Carta de los Derechos Fundamentales de la Unión Europea. Comentario artículo por artículo,* Fundación BBVA, 2009).

la evolución del derecho a la privacidad y la protección de datos personales[25]. Adoptada en 1995, esta Directiva fue la primera iniciativa importante de la UE para regular la protección de datos personales. Aseguró que todos los Estados miembros de la UE tuvieran legislación similar en relación a la protección de datos para prevenir la interrupción del flujo de información personal intra y extracomunitaria. La Directiva 95/46/CE se centró en la protección de los individuos en relación con el procesamiento de datos personales y trató la libre circulación de tales datos. Estableció reglas claras y detalladas sobre la transparencia, el consentimiento legítimo, los derechos de acceso, rectificación y objeción, así como sobre las transferencias de datos a terceros países. Sin embargo, dado el rápido desarrollo de las tecnologías de la información y la digitalización, la Directiva 95/46/CE se volvió cada vez menos adecuada para manejar los desafíos emergentes en el campo de la protección de datos[26]. Esto llevó al desarrollo y adopción del RGPD en 2016, que abroga la Directiva 95/46/CE y establece un nuevo marco para la protección de datos en la UE[27]. En su artículo 4(1), este Reglamento define qué podemos considerar como un dato personal y establece reglas claras y estrictas sobre su procesamiento. Además, este instrumento proporciona un alto nivel de protección de los datos personales y otorga a los individuos un mayor control sobre sus propios datos.

14. Consideramos que el concepto de intimidad, vida privada y privacidad, aunque a menudo se utilizan de manera intercambiable, poseen matices distintos tanto en el ordenamiento jurídico comunitario, es decir, la UE, como en el estadounidense. Empezando por la intimidad, este término abarca los aspectos más personales e íntimos de la vida de un individuo, que incluyen su vida sexual, salud física y mental, y su vida familiar. En la UE, el derecho a la intimidad está resguardado bajo varios instrumentos legales, incluyendo la Carta de Derechos Fundamentales de la UE. En cambio, en los EE.UU., el derecho a la intimidad está menos claramente definido en la normativa federal[28], aunque sí existen leyes específicas en algunos Estados que protegen este derecho[29], así como normativas sectoriales específicas[30].

[25] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Texto íntegro disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A31995L0046

[26] G. G. Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, 2014.

[27] 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 (RGPD). Texto íntegro disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

[28] Aunque la Constitución de los EE.UU. no menciona explícitamente el derecho a la privacidad, la Corte Suprema ha interpretado la protección de la intimidad a partir de varias enmiendas, en casos famosos como Griswold v. Connecticut (1965), donde se defendió el uso de anticonceptivos en el matrimonio, y Roe v. Wade (1973), que resguardó el derecho de una mujer a tomar decisiones sobre su propio cuerpo, incluyendo la decisión de abortar. Sin embargo, estas interpretaciones pueden ser y han sido objeto de intenso debate y revisión (G. Nolte, "European and US Constitutionalism: Comparing Essential Elements" en G. Nolte (ed), *European and US Constitutionalism*, Cambridge University Press, 2005).

[29] La Constitución de California es única en su explícita inclusión del derecho a la privacidad entre sus disposiciones. En 1972, los votantes de California aprobaron una enmienda (conocida como Proposición 11) que añadió el derecho a la privacidad a la Declaración de Derechos de la Constitución del Estado. El Artículo 1, Sección 1 de la Constitución de California establece: "Todas las personas nacen libres e iguales en dignidad y derechos. Tienen derecho a la protección de la Ley y, como consecuencia de ello, tienen derecho a obtener seguridad, felicidad y privacidad." Este derecho a la privacidad protege a los ciudadanos de California contra invasiones no deseadas a su privacidad por parte del Gobierno, pero también de las empresas privadas. Ha sido interpretado para abarcar una variedad de temas, incluyendo la no divulgación de información personal y la autonomía personal. Ha permitido a los residentes de California desafiar las prácticas de recopilación de datos de las grandes empresas tecnológicas y otras formas de intrusión en la privacidad por parte de empresas privadas. En este sentido, vid. D. A. Carrillo, S. M. Duvernay, R. E. Rivera Aquino, B. V. Stracener, "California Constitutional Law: Privacy", *San Diego Law Review*, vol. 59, nº 119, 2022; y también C. Kelso, "California's Constitutional Right to Privacy", *Pepperdine Law Review*, vol. 19, nº 2, 1992.

[30] Por ejemplo, la Ley HIPAA regula los datos de salud, la Ley FERPA protege los datos de los estudiantes y la Ley COPPA regula la recopilación de datos de los menores en línea. Además, el principio de consentimiento, que es fundamental en la normativa europea, se interpreta y aplica de manera diferente en los EE.UU. Mientras que el RGPD exige un consentimiento claro y afirmativo, en los EE. UU., en muchos casos, las empresas pueden recopilar y utilizar datos a menos que los individuos se opongan explícitamente. Para profundizar en la cuestión, se recomienda E. Schweighofer, "Principles for US–EU Data Flow Arrangements" en D.J.B. Svantesson, D. Kloza (eds), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*, Intersentia, 2017.

Por otro lado, la vida privada engloba una esfera más amplia de la vida de un individuo. Aunque incluye la intimidad, también abarca otras áreas de la vida personal y social que una persona puede decidir mantener fuera del ámbito público. En el sistema europeo, este aspecto de la vida privada es protegido bajo el Artículo 8 del CEDH[31]. En EE.UU., la protección de la vida privada es menos explícita. Sin embargo, la Cuarta Enmienda de la Constitución protege a las personas contra búsquedas y confiscaciones no razonables, interpretándose esto como una forma de protección de la vida privada[32]. Por último, el concepto de privacidad posee un alcance aún más amplio, y en el contexto moderno suele referirse a la protección de los datos personales y la información privada. En este sentido, la UE ha promovido una protección intensiva de la privacidad de los datos mediante su normativa, como es el caso del RGPD. En los EE.UU., la privacidad de los datos está protegida de manera fragmentada, dependiendo del tipo de datos y del Estado en cuestión, y actualmente (2023) no existe una normativa federal integral en materia de privacidad de datos[33].

15. Estos tres conceptos, intimidad, vida privada y privacidad, si bien tienen áreas de superposición, mantienen un enfoque ligeramente diferente entre sí. La intimidad se refiere a los aspectos más personales y delicados de la vida de un individuo. Aquí se agrupan aquellos aspectos de nuestra existencia que elegimos compartir únicamente con personas de nuestro círculo más cercano, como nuestra salud física y mental, nuestras relaciones familiares y amorosas, o nuestros pensamientos y emociones más profundos. Por otra parte, la vida privada se despliega en un espectro más amplio, abarcando no sólo la intimidad, sino también otras dimensiones de nuestra vida personal y social que preferimos mantener al margen del escrutinio público. Esto puede incluir la dirección de nuestro domicilio, el colegio al que van nuestros hijos, o nuestras preferencias políticas y religiosas, *inter alia*. Aquí se sitúan todas aquellas elecciones que hacemos en nuestro día a día y que, aunque no sean necesariamente íntimas, no por ello deseamos que sean de dominio público. Por último, la privacidad se refiere más directamente a la protección de nuestros datos personales e información privada. En una era en la que la mayoría de nuestras interacciones ocurren a través de plataformas digitales, la privacidad se ha convertido en un asunto de vital importancia. Todos nuestros movimientos *online* dejan un rastro de datos que, sin las adecuadas medidas de seguridad, podrían ser utilizados de manera indebida[34].

16. Con la aparición del Metaverso, estas cuestiones de intimidad, vida privada y privacidad adquieren una nueva dimensión[35]. El Metaverso, entendido como un universo digital paralelo e interactivo en el que los usuarios pueden comunicarse en tiempo real a través de representaciones digitales de sí mismos o avatares, nos enfrenta a desafíos inéditos en la protección de estos derechos. En este escenario innovador, no sólo se ponen en riesgo nuestros datos e información personal, sino que también se expone nuestra identidad digital. Este concepto se refiere a la representación en línea de un individuo, incluyendo tanto datos personales como los elementos que definen su personalidad en el espacio digital, como los gustos, las opiniones y los comportamientos. Además, las interacciones y relaciones

[31] J. Akandji-Kombe, *Positive Obligations under the European Convention on Human Rights: A Guide to the Implementation of the ECHR*, Consejo de Europa, 2007.

[32] La Cuarta Enmienda de la Constitución de los EE.UU. establece lo siguiente: "El derecho de los habitantes de que su personas, casas, documentos y propiedades estén libres de búsquedas y confiscaciones irrazonables no será vulnerado, y no se expedirán órdenes sino con causa probable respaldada por juramento o afirmación, y describiendo particularmente el lugar a ser registrado, y las personas o cosas a ser confiscadas." Esta enmienda es fundamental en el marco legal estadounidense porque protege a los ciudadanos contra la intrusión del Gobierno en su vida privada sin una razón válida. Aunque no menciona explícitamente la "privacidad", ha sido interpretada por la Corte Suprema de los EE.UU. en diversas ocasiones como una protección contra las invasiones de la privacidad. Esta enmienda requiere que cualquier orden de búsqueda o arresto esté respaldada por una "causa probable", y limita las búsquedas y confiscaciones a lo que se especifica en la orden (T. P. Crocker, "The Fourth Amendment at Home, *Indiana Law Journal*, vol. 96, nº 1, 2020).

[33] Véanse, *inter alia,* D. j. Glancy, "The Invention of the Right to Privacy", *Arizona Law Review*, vol. 21, 1979. K.A. Bamberger, D.K. Mulligan, Privacy on the Ground: Driving Corporate Behavior in the US and Europe, MIT Press, 2015.

[34] B. Falchuk, S. Loeb, R. Neff, "The social metaverse: battle for privacy", *IEEE Technology and Society Magazine*, vol. 37, nº 2, 2018, pp. 52-61. [En línea] Disponible en: https://doi.org/10.1109/MTS.2018.2826060

[35] D. Banisar, S. Davies, "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Law and Developments", *John Marshall Journal of Computer and Information Law,* vol. 18, nº 1, 1999, p. 1.

virtuales también cobran una nueva importancia. Éstas se refieren a las conexiones y comunicaciones que los usuarios establecen en el espacio virtual, que pueden tener un impacto significativo en su vida *offline*. Las interacciones pueden incluir desde las conversaciones y actividades compartidas hasta las relaciones personales y profesionales que se forman en el Metaverso. Asimismo, nuestras actividades dentro de este espacio digital, que pueden abarcar desde la participación en eventos virtuales, la creación y comercio de bienes digitales, hasta la exploración y personalización de los propios espacios virtuales, también están expuestas. Por todo ello, es esencial que los creadores del Metaverso, los legisladores y los defensores de los derechos humanos colaboren para asegurar que la normativa en materia de protección de datos se respete, proteja y cumpla. Con esta visión en mente, en el próximo apartado, trataremos de identificar los desafíos y oportunidades que este nuevo entorno digital presenta y proponer soluciones eficaces y eficientes para garantizar el respeto de estos derechos fundamentales.

IV. Las obligaciones comunitarias de respetar, proteger y cumplir

17. La Segunda Guerra Mundial y el uso de datos contra determinados colectivos han dejado una profunda huella en la configuración del Derecho Comunitario y el ordenamiento jurídico estadounidense. Estos eventos históricos han influido en cómo se abordan cuestiones relacionadas con la libertad de expresión y la protección de los derechos individuales en ambos sistemas legales[36].

18. En el contexto de la Segunda Guerra Mundial, diversos regímenes totalitarios utilizaron la recopilación y el análisis de datos para perseguir y reprimir a grupos específicos de la sociedad. El uso sistemático de información personal permitió la identificación y discriminación de personas en función de su origen étnico, religión u otras características. Estas prácticas atroces llevaron a una creciente conciencia sobre la importancia de salvaguardar los derechos fundamentales de las personas y prevenir futuros abusos[37].

19. A nivel europeo, la experiencia de la Segunda Guerra Mundial impulsó la creación del Consejo de Europa y de la UE y la adopción de una serie de instrumentos legales destinados a promover la paz, la estabilidad y la protección de los derechos humanos en la región[38]. El CEDH, por ejemplo, establece un marco jurídico sólido para garantizar los derechos individuales, incluido el derecho a la libertad de expresión. Sin embargo, el enfoque comunitario también se caracteriza por la necesidad de equilibrar estos derechos con otros valores fundamentales, como la seguridad y el respeto a la dignidad humana.

20. Por otro lado, el Metaverso es un concepto emergente y de origen estadounidense que se refiere a un entorno virtual compartido, donde las personas pueden interactuar entre sí y con elementos digitales. A medida que el Metaverso se desarrolla, surgen cuestiones legales relacionadas con la libre expresión y los derechos individuales. En este contexto, no podemos pasar por alto que el ordenamiento jurídico norteamericano, basado en gran medida en la Constitución de los EE.UU., incluye en su primera enmienda la protección del derecho a la libre expresión. La tradición liberal, individualista y capitalista que ha moldeado la sociedad estadounidense también tendrá implicaciones en el Metaverso, ya que se espera que los principios de libertad de expresión y protección individual sean tenidos en cuenta en el

[36] E.R. Alo, "EU Privacy Protection: A Step towards Global Privacy", *Michigan State International Law Review,* vol. 22, 2014, p. 1095.

[37] Durante la Segunda Guerra Mundial, los regímenes fascistas utilizaron datos personales para perseguir y dañar a colectivos específicos. Estos regímenes recopilaban información personal a través de (1) sistemas de registro y clasificación, (2) tarjetas de identificación obligatorias, (3) censos y registros demográficos, así como (4) mediante el uso de informantes y colaboradores. Esta información se utilizaba para identificar a personas pertenecientes a grupos considerados indeseables, como judíos y disidentes políticos, y promover la discriminación y la represión. La utilización de datos personales con fines opresivos y discriminatorios durante ese período oscuro de la Historia es un recordatorio de la importancia de proteger la privacidad y los derechos individuales en la actualidad.

[38] Sobre este tema, vid. A. Saarenpaa, "Europa y la protección de los datos personales", *Revista Chilena de Derecho Informático*, nº 3, 2003, p. 21.

desarrollo de políticas y códigos de conducta en este entorno virtual. Así las cosas, todo parece apuntar a que, apriorísticamente, partimos del reconocimiento, en estos espacios, del derecho a la *privacy*, como "el derecho a que nos dejen en paz"[39].

21. No obstante, la Historia de los EE.UU. de América también ha mostrado cómo el uso indebido de datos y la violación de los derechos individuales pueden tener consecuencias catastróficas. Un ejemplo destacado es el programa de vigilancia masiva llevado a cabo por la Agencia de Seguridad Nacional (NSA) revelado por Edward Snowden en 2013[40]. Esta revelación generó un debate sobre la necesidad de equilibrar la seguridad nacional con la protección de la privacidad y los derechos individuales. En respuesta a estas preocupaciones, como veremos en los próximos apartados, los Estados miembros de la UE han adoptado un enfoque más sólido en la protección de datos personales, especialmente en relación con el Derecho Comunitario establecido por el RGPD[41].

22. Como punto inicial en este ejercicio de equilibrio de intereses, derechos y valores en lo relativo a la normativa aplicable en el Metaverso, partimos de la premisa de que los Estados miembros de la UE tienen una serie de responsabilidades bajo el Derecho Comunitario en la protección de datos, en particular de acuerdo con el RGPD y su aplicabilidad en estos mundos virtuales. Estas obligaciones se pueden categorizar en tres áreas: respetar, proteger y cumplir[42]. Primordialmente, los Estados miembros tienen el deber de respetar el RGPD en el contexto del Metaverso. Esto significa que deben abstenerse de interferir con los derechos de protección de datos de los usuarios del Metaverso y asegurar que su legislación nacional esté en línea con las directrices del RGPD. En este marco, la adaptación y aplicación del RGPD en el entorno del Metaverso puede necesitar la revisión y modificación de la normativa existente para crear nuevas categorías de datos, además de la adopción de normativas sectoriales específicas y/o acuerdos con terceros Estados que desarrollen la normativa existente, para garantizar su cumplimiento efectivo. Pues, en definitiva, es importante enfatizar que, aunque los Estados miembros tienen estas responsabilidades en virtud del RGPD, en principio, no poseen la autoridad para imponer directamente estas obligaciones a terceros Estados en relación con el Metaverso. Si bien pueden impulsar y promover la adopción de estándares de protección de datos similares en otros países con presencia en el Metaverso, no tienen la facultad de obligar a esos países a cumplir con lo dispuesto en el Reglamento[43].

---

[39] M. Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age", *Harvard International Law Journal*, vol. 56, nº. 1, 2015, p. 81.

[40] En 2013, Edward Snowden, un ex contratista de la Agencia de Seguridad Nacional (NSA) de EE.UU., desató uno de los mayores escándalos de vigilancia y protección de datos en la historia contemporánea. Snowden filtró una gran cantidad de información clasificada que reveló la existencia de programas de vigilancia masiva llevados a cabo por la NSA y otras agencias de inteligencia. Estas revelaciones impactaron profundamente en la percepción de la privacidad y los derechos individuales. Snowden filtró documentos que detallaban programas como el PRISM, que permitía a la NSA acceder a datos almacenados en compañías tecnológicas líderes, y el programa de recolección de metadatos de llamadas telefónicas, que recopilaba información sobre las comunicaciones de millones de ciudadanos estadounidenses. Estas revelaciones generaron preocupación y debate sobre la extensión de la vigilancia gubernamental y sus implicaciones para la privacidad. Tras filtrar los documentos, Snowden huyó de EE.UU. y buscó asilo en diferentes países. Inicialmente se refugió en Hong Kong y luego viajó a Rusia, donde finalmente obtuvo asilo temporal. Su caso generó tensiones diplomáticas entre EE.UU. y otros países, así como un debate intenso sobre su estatus como denunciante o traidor. El caso Snowden tuvo un impacto significativo en el debate global sobre la privacidad y la vigilancia. Sus revelaciones despertaron una mayor conciencia sobre la necesidad de salvaguardar los derechos individuales en la era digital y cuestionaron la legalidad y ética de los programas de vigilancia masiva. Además, las filtraciones de Snowden llevaron a una mayor demanda de transparencia y rendición de cuentas por parte de los gobiernos en relación con sus actividades de inteligencia. En este sentido, vid. D. Svantesson, D. Kloza, "Yet Another Book about Snowden and Safe Harbor?" en D. Svantesson, D. Kloza (eds), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*, Intersentia, 2017.

[41] I. Georgieva, "The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR", *Utrecht Journal of International and European Law*, vol. 31(80), 2015, p. 104.

[42] E. Watt, "The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance" en H. Rõigas y otros (eds), *9th International Conference on Cyber Conflict: Defending the Core,* NATO CCD COE Publications, 2017.

[43] M. Taylor, *Transatlantic Jurisdictional Conflicts in Data Protection Law. Fundamental Righs, Privacy and Extraterritoriality,* Cambridge University Press, 2023, pp. 46-49.

23. En segundo lugar, la obligación de proteger se refiere al deber del Estado miembro de prevenir las violaciones de los derechos de protección de datos por parte de terceros, incluyendo empresas privadas y entidades operando en el Metaverso. Esto implica el establecimiento de una autoridad de protección de datos independiente en cada Estado miembro, capaz de supervisar la aplicación del RGPD tanto en el mundo físico como en espacios digitales y el Metaverso, y de ejercer poderes de investigación y sanción. En este sentido, los Estados miembros deben asegurarse de que las organizaciones y entidades del Metaverso dentro de su jurisdicción cumplan con la obligación de notificar a la autoridad de protección de datos y, en ciertos casos, a los individuos afectados, cuando se produzca una infracción de la seguridad de los datos ya sea en el espacio tradicional o en el entorno del Metaverso. En este contexto, el Comité Europeo de Protección de Datos (EDPB, por sus siglas en inglés), una entidad creada por RGPD, juega un papel esencial. Este organismo permite una cooperación más estrecha entre las autoridades de protección de datos de los Estados miembros, fortaleciendo así el cumplimiento del deber de proteger. La EDPB ofrece orientación sobre la interpretación del RGPD, promoviendo una aplicación coherente en todo el bloque. Además, tiene un papel importante en el arbitraje de disputas entre autoridades nacionales en casos transfronterizos[44].

24. Finalmente, la obligación de cumplimiento implica que los Estados miembros tienen que implementar medidas proactivas para asegurar la protección de los datos en el Metaverso. Esto implica la necesidad de garantizar la colaboración y consistencia en toda la UE en la implementación del RGPD, que podría incluir el intercambio de información o la toma de decisiones colectivas en casos que tengan una repercusión directa o tangible, en tanto que actividad delictiva, en el mundo analógico. Además, los Estados miembros deben asegurar que los usuarios del Metaverso puedan ejercer sus derechos bajo el RGPD, como el derecho de acceso, rectificación, supresión ("derecho al olvido")[45], limitación del procesamiento, portabilidad de los datos y oposición. En este nuevo entorno digital, los Estados miembros también deben garantizar que las entidades que controlan el procesamiento de datos realicen una evaluación de impacto sobre la protección de datos cuando es probable que un tipo de tratamiento conlleve un alto riesgo para los derechos y libertades de los individuos en el Metaverso. Si la evaluación señala un alto riesgo, la autoridad de supervisión pertinente deberá ser consultada. Por añadidura, conviene destacar que los Estados miembros tienen la responsabilidad de promover la capacitación de las entidades encargadas de procesar datos en el Metaverso, así como la conciencia general de los ciudadanos sobre los riesgos, normas, salvaguardias y derechos relacionados con el procesamiento de datos personales en este novedoso contexto digital[46].

25. En esencia, estas responsabilidades son la columna vertebral que asegura que los datos personales sean manejados de manera segura y transparente en el entorno digital, especialmente en el Metaverso, un espacio de creciente interés y desarrollo. Éstas protegen los derechos esenciales de los individuos, entre los que se destacan la privacidad y la propiedad sobre su información personal[47]. La ejecución cuidadosa de estas obligaciones contribuye a la preservación de estos derechos en la interacción con plataformas digitales y experiencias de Metaverso. Además, al abogar por el uso responsable y la protección de los datos personales, estas obligaciones fortalecen la confianza en el mercado digital, incluido el Metaverso, dentro del contexto del Mercado Único Digital de la UE. Esta confianza es fundamental para el desarrollo y adopción de estas tecnologías emergentes, ya que garantiza a los usuarios que sus interacciones y transacciones en el Metaverso serán seguras y respetarán sus derechos fundamentales. La

[44] J. Akandji-Kombe, *Positive Obligations under the European Convention on Human Rights: A Guide to the Implementation of the ECHR*, Council of Europe Publishing, 2007.

[45] J. Ausloos, T*he Right to Erasure in EU Data Protection Law: From Individual Rights to Personal Protection,* Oxford University Press, 2020.

[46] M. Scheinin, "Characteristics of Human Rights Norms" en C. Krause, M. Scheinin (eds), *International Protection of Human Rights: A Textbook*, 2ª ed., Åbo Akademi University Institute for Human Rights, 2012.

[47] M. Zhou, M. A. A. M. Lenders, L. Cong, "Ownership in the virtual world and the implications for long-term user innovation success", *Technovation*, vol. 78, nº October, 2018, pp. 56-65. [En línea] Disponible en: https://doi.org/10.1016/j.technovation.2018.06.002

responsabilidad compartida entre los proveedores de servicios del Metaverso y las autoridades reguladoras es clave para lograr un equilibrio entre innovación y protección de datos personales. En consecuencia, el procesamiento seguro y transparente de los datos personales no sólo protege los derechos de los individuos, sino que también es una piedra angular para el crecimiento y la estabilidad del ecosistema digital, incluyendo las experiencias del Metaverso, dentro del mercado digital único de la UE.

V. La determinación de la jurisdicción en el Metaverso

26. La evolución de la jurisdicción[48], tanto en sistemas de Derecho continental europeos como en EE.UU., es un espejo de las transformaciones profundas y multifacéticas en nuestra sociedad, cada vez más inmersa en el Metaverso. La noción de jurisdicción[49], emergida del concepto romano de *imperium*, originalmente se limitaba a la autoridad de un soberano sobre un territorio y sus habitantes, y estaba asociada a la autoridad del Estado en el caso de los EE.UU. Esta visión se enfocaba en las jurisdicciones territorial y personal, delimitando la autoridad judicial según las fronteras físicas y las relaciones personales. No obstante, con la irrupción de la globalización y la metaversalización, que es la interconexión cada vez más estrecha entre sociedades físicas y virtuales, la jurisdicción ha tenido que readaptarse a estas novedades. En Europa, el Tribunal de Justicia de la UE (TJUE) ha asumido una jurisdicción exclusiva en ciertos asuntos, como las patentes o algunos aspectos de la protección de datos en Internet, que afectan a todos los Estados miembros de la UE. En paralelo, en EE.UU., la evolución del Derecho federal ha derivado en la idea de jurisdicción exclusiva. En este escenario, ciertas cuestiones, como los delitos federales, son competencia exclusiva de los tribunales federales, independientemente de la ubicación geográfica o virtual de la acción o la residencia de las partes. Adicionalmente, con el progreso de las tecnologías de la información y las comunicaciones en el Metaverso, la jurisdicción ha tenido que enfrentar el reto de la digitalización. Esto ha conllevado la aparición de conceptos como la jurisdicción funcional, que confiere competencia a un tribunal para abordar determinados tipos de casos en función de su naturaleza, sin importar la ubicación geográfica, virtual o la nacionalidad de las partes.

27. La jurisdicción exclusiva se refiere a la idea de que ciertos asuntos son de la competencia única de un Estado particular o tribunal. Por ejemplo, en el contexto del Metaverso y la UE, la jurisdicción exclusiva en cuestiones como la validez de las patentes de tecnologías de realidad virtual y aumentada se reserva al TJUE. Este privilegio también abarca cuestiones relativas a la regulación del Metaverso, en tanto que nueva generación de Internet y de las nuevas tecnologías emergentes. Un caso representativo es la decisión del TJUE en el caso de Google España contra la Agencia Española de Protección de Datos en 2014. Este fallo estableció el "derecho al olvido" en Internet, lo que significa que los individuos tienen derecho a solicitar a los motores de búsqueda como Google que eliminen los enlaces a información personal antigua o irrelevante y que entendemos que tendrá una aplicación directa en relación con la información almacenada en los servidores que garantizarán el funcionamiento del Metaverso[50]. Este fallo destacó la capacidad del TJUE para dictaminar sobre cuestiones relacionadas con la regulación de Internet, estableciendo un precedente legal en la materia en toda la UE[51].

[48] B.H. Oxman, "Jurisdiction of States", *Max Planck Encyclopedia of Public International Law*, última actualización: noviembre 2007, Oxford University Press.

[49] R.T. Ford, "Law's Territory: (A History of Jurisdiction)", *Michigan Law Review*, vol. 97, nº 4, 1999, p. 843.

[50] J. Ausloos, "European Court Rules against Google, in Favour of Right to Be Forgotten", *LSE Media Policy Project Blog,* 13 de mayo de 2014. [En línea] Disponible en: https://blogs.lse.ac.uk/medialse/2014/05/13/european-court-rules-against-google-in-favour-of-right-to-be-forgotten/.

[51] R.C. Post, "Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere", *Yale Law School*, Public Law Research Paper nº 598, 2017L; B. Van Alsenoy, M. Koekkoek, "Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the "Right to Be Delisted"", *International Data Privacy Law,* vol. 5(2), 2015, p. 105; así como S. Uncular, "The Right to Removal in the Time of Post-Google Spain: Myth or Reality under General Data Protection Regulation?", *International Review of Law, Computers & Technology,* vol. 33(3), 2019, p. 309.

28. La jurisdicción funcional en el Metaverso, por otro lado, se refiere a la competencia de un tribunal para tratar con ciertos tipos de casos basados en su naturaleza, sin importar la ubicación geográfica o la identidad de los avatares implicados. En el espacio digital y ahora extendido al Metaverso, esta jurisdicción funcional se ha manifestado en la competencia del TJUE para abordar casos relacionados con la privacidad y la protección de datos, sin importar dónde estén ubicadas las empresas en el plano analógico. El ejemplo paradigmático en el contexto de Internet que podría aplicarse al Metaverso es el caso Schrems II, donde el TJUE invalidó el marco del Escudo de la Privacidad UE-EE.UU. (*Privacy Shield*), alegando que no proporcionaba protección adecuada a los ciudadanos europeos contra la vigilancia del Gobierno de los EE.UU.[52]. Esta decisión, con ramificaciones que podrían extenderse al Metaverso, demuestra la capacidad y jurisdicción del TJUE para proteger los derechos digitales y metaversales de los ciudadanos europeos a nivel global. Sin embargo, la implementación de esta jurisdicción funcional también plantea desafíos significativos, principalmente debido a la necesidad de cooperación entre las autoridades intermetaversales. En el contexto del caso Schrems II, aunque la decisión fue tomada por el TJUE, la aplicación efectiva de dicha decisión en el Metaverso dependería en gran medida de la cooperación de las autoridades estadounidenses. Esto implica un alto grado de cortesía y diplomacia transatlántica para resolver problemas que puedan surgir. En este sentido, el contacto y la comunicación entre las diferentes autoridades intermetaversales son esenciales para manejar las complicaciones que puedan generarse durante la implementación de estas decisiones en el Metaverso[53]. En este ambiente de complejidad legal y política digital extendida al Metaverso, es vital que se establezcan y mantengan canales de comunicación efectivos y se priorice la cooperación intermetaversal. Sin embargo, este proceso puede ser lento y complicado, y a veces puede llevar a situaciones en las que las decisiones judiciales no se implementan completamente o de manera eficiente en el Metaverso.

29. Los conceptos de jurisdicción nacional[54], personal[55] y territorial[56], por otro lado, siguen siendo la base de los sistemas jurídicos en el plano analógico[57]. Sin embargo, con la aparición del Metaverso, estos conceptos están evolucionando para abordar nuevos desafíos. Los sistemas jurídicos tendrán que plantear si se adaptan conceptos clásicos como la jurisdicción universal en casos de delitos virtuales graves, y el principio de efecto en el Metaverso, según el cual un Estado podría reclamar jurisdicción sobre actos que tienen efectos dentro de su territorio virtual, incluso si fueron cometidos desde ubicaciones físicas en terceros Estados. Este principio ha encontrado aplicación en la protección de datos transatlánticos, especialmente en el contexto de Internet, donde los datos personales se procesan y comparten a una escala sin precedentes. Un caso notable fue la invalidación del acuerdo de *Safe Harbor* por parte del TJUE en el caso Schrems I[58]. Según este principio, entendemos que la UE podría afirmar su jurisdicción

[52] STJUE 16 julio 2020, *Facebook Ireland y Schrems*, C-311/18, ECLI:EU:C:2020:559.

[53] I. Ilyina, E. Eltikova, K. Uvarova, S. Chelysheva, "Metaverse - death to offline communication or empowerment of interaction?", en *Proceedings of the 2022 Communication Strategies in Digital Society Seminar,* 2022, pp. 117-119. [En línea] Disponible en: https://doi.org/10.1109/ComSDS55328.2022.9769144

[54] En referencia a la autoridad legal que un Estado posee para aplicar sus leyes dentro de sus límites geográficos, se habla de jurisdicción nacional. Este término alude a la competencia y facultad de los sistemas judiciales del país para poner en práctica la ley, mediar en conflictos y ejercer control sobre individuos y entidades en su territorio. Se considera bajo su amparo tanto a los ciudadanos nacionales como a los extranjeros presentes en sus confines.

[55] Por otro lado, al poder de un tribunal de emitir resoluciones que impacten directamente a una persona, corporación o entidad se le conoce como jurisdicción personal. Este tipo de jurisdicción se fundamenta en las relaciones que el demandado mantiene con la ubicación del tribunal. Dichas relaciones pueden consistir en residir en el lugar, tener un negocio en él, o en algunos casos, simplemente visitarlo. Si un tribunal carece de jurisdicción personal sobre un demandado, entonces sus fallos no pueden tener una vinculación legal obligatoria con éste.

[56] En cuanto al poder de un tribunal o un organismo gubernamental de ejercer autoridad en una zona geográfica concreta, nos referimos a la jurisdicción territorial. En este espacio delimitado, la entidad posee la capacidad de aplicar las leyes, interpretarlas y dispensar justicia. Como ejemplo de las restricciones de la jurisdicción territorial, podemos citar el caso del CEDH. Este Tratado internacional, diseñado para salvaguardar los derechos humanos, la democracia y el Estado de Derecho en Europa, se monitoriza a través del TEDH. Todos los países miembros del CEDH han aceptado la competencia de este tribunal en su territorio.

[57] M. Díez de Velasco, *Instituciones de Derecho Internacional Público*, 16ª ed., Tecnos, 2007.

[58] STJUE 6 octubre 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650.

sobre las empresas del Metaverso con sede en los EE.UU. que procesen datos personales de avatares de la UE, incluso si el procesamiento tiene lugar fuera de la UE, siempre que estos actos tengan efectos dentro de la UE, es decir, puedan afectar la privacidad y la protección de datos de los ciudadanos de la UE. De este modo, a pesar de las diferencias en las normativas de protección de datos entre los EE.UU. y la UE, las empresas estadounidenses que operan en el Metaverso europeo estarían obligadas a cumplir con el RGPD de la UE. Esto demuestra cómo el principio de efecto se configura como una tendencia en el creciente ecosistema digital del Metaverso.

30. Las tecnologías emergentes, en particular aquellas que posibilitan la transmisión de información y servicios más allá de las fronteras nacionales en el Metaverso, como la computación en la nube, están planteando desafíos significativos para la jurisdicción tradicional. La naturaleza descentralizada de los datos en el Metaverso, y su habilidad para ser almacenados y transferidos sin un punto de ubicación físico concreto, complican la determinación de la jurisdicción aplicable. Este obstáculo, claramente palpable en la protección de datos transmetaversales, resalta la creciente necesidad de adaptar las interpretaciones jurídicas convencionales a la realidad de la globalización digital en el Metaverso. En respuesta a este reto, se podrían considerar tres rutas alternativas: (1) reconocer y asumir la capacidad limitada de la UE para proteger los datos en el Metaverso como derecho fundamental; (2) reinterpretar el concepto clásico de jurisdicción para adaptarlo a la era digital en el Metaverso, expandiendo potencialmente la aplicación del principio de efecto; o (3) elevar la protección de datos en el Metaverso a la categoría de valor fundamental de la UE, concediéndole máxima prioridad en el diseño y promoción de políticas conexas.

1. La necesidad de cooperación en el Metaverso

31. Es crucial reconocer las limitaciones que la tecnología, la globalización y ahora el Metaverso imponen en la habilidad de la UE para proteger los datos personales como un derecho fundamental[59]. En el contexto del Metaverso, estas limitaciones se agravan particularmente por la falta de capacidad tecnológica para supervisar con precisión las decisiones tomadas por las autoridades europeas, como el Comité Europeo de Protección de Datos[60] y el TJUE. Esto se vuelve aún más desafiante sin la cooperación activa del Gobierno de los EE.UU. de América[61], un actor crucial en el desarrollo y la expansión del Metaverso. Este escenario podría instar a la UE a colaborar más estrechamente con otras jurisdicciones, incluyendo aquellas implicadas en el Metaverso, para desarrollar acuerdos internacionales que aborden la protección de datos y la privacidad en este nuevo ámbito digital.

32. El objetivo de este esfuerzo, ampliado ahora al ámbito del Metaverso, no sería sólo la estandarización de las leyes y regulaciones de protección de datos a nivel global, sino también la generación de una conciencia ciudadana sobre la importancia de proteger sus propios datos, especialmente en contextos digitales inmersivos. Esta necesidad adquiere un significado especial cuando se considera la Política Europea de Vecindad, articulada en el artículo 52 de la Carta de Derechos Fundamentales, que enfatiza la importancia de las relaciones cercanas y la cooperación con los países vecinos, extendiéndose ahora a los nuevos vecinos con los que podemos establecer relaciones y/o fomentarlas a través de nuevas formas de conexión como el Metaverso.

[59] En esta materia, vid. G. Zanfir, 'How CJEU's "Privacy Spring" Construed the Human Rights Shield in the Digital Age' en E. Kuzelewska y otros (eds), *European Judicial Systems as a Challenge for Democracy*, Intersentia, 2015.

[60] El Comité Europeo de Protección de Datos (CEPD) es una institución clave en el marco regulatorio de la privacidad en Europa. Se trata de una autoridad independiente encargada de salvaguardar los derechos fundamentales de los individuos en relación con el tratamiento de sus datos personales. El CEPD desempeña un papel vital al promover y supervisar el cumplimiento del RGPD en todos los Estados miembros de la UE. Además, proporciona orientación y asesoramiento técnico a las instituciones y organismos de la UE en materia de protección de datos. Sus funciones incluyen la emisión de dictámenes sobre cuestiones de relevancia en la privacidad, la cooperación con otras autoridades de protección de datos y la promoción de la coherencia y armonización en la aplicación del RGPD. En última instancia, el CEPD desempeña un papel crucial en la protección de la privacidad y la garantía de que los derechos fundamentales de las personas sean respetados en el entorno digital (artículos 68-76 del RGPD).

[61] H. Farrell, A. Newman, "The Transatlantic Data War", *Foreign Affairs*, 2016.

33. Determinar la responsabilidad en estos casos no es una tarea sencilla, especialmente en el entorno del Metaverso donde la jurisdicción y la identidad pueden ser fluidas[62]. Tradicionalmente, la responsabilidad se establece cuando: (1) se realiza una acción -o una omisión-, (2) ésta genera un daño y (3) podemos establecer una relación de causalidad directa entre la (in)acción y el daño causado. Sin embargo, este proceso se vuelve más complejo en casos relacionados con la transferencia transatlántica de datos y ahora con las interacciones dentro del Metaverso. Aquí, la causalidad puede ser difusa, ya que las acciones que generan el daño pueden ser realizadas por diversas entidades en diferentes jurisdicciones o espacios virtuales, y el daño puede manifestarse de maneras que son difíciles de medir o cuantificar. Esta complejidad añade otra capa de urgencia a la necesidad de colaboración y acuerdo internacional en la protección de datos y la privacidad en este nuevo universo digital.

34. Es más, determinar la responsabilidad de empresas y autoridades estatales en casos de transferencia masiva de datos transatlánticos -o entre entidades que operan usando plataformas intermediarias, prestadoras de servicios, autodenominadas o concebidas como metaversos- es un desafío considerable debido a la variabilidad de las legislaciones sobre protección de datos y privacidad entre regiones, las complejidades de la jurisdicción y aplicación de la ley en diferentes países y espacios virtuales, y la naturaleza técnica de la transferencia de datos. Además, debemos tener en cuenta las distintas interpretaciones de la normativa aplicable que pueden ser contradictorias o ambiguas entre jurisdicciones, la identificación de la entidad responsable para investigar, sancionar las violaciones de la protección de datos, así como la capacidad para rastrear y demostrar la transferencia de datos que pueden estar cifrados o ser difíciles de rastrear a la hora de determinar qué datos se transfirieron, cuándo y a dónde. Incluso en aquellos casos en los que se pueda demostrar que se transfirieron datos, puede ser difícil determinar si se violó la normativa aplicable en materia de protección de datos si éstos estaban suficientemente anonimizados o pseudonimizados, especialmente cuando estos datos existen y circulan a través del Metaverso.

2. La aplicación extraterritorial del Derecho de la Unión Europea

35. Por otra parte, también se podría considerar una reinterpretación del concepto tradicional de jurisdicción[63], en un intento de adaptarlo a los desafíos emergentes del Metaverso y la realidad digital. Varias teorías podrían ser útiles en este proceso de adaptación. La teoría de la territorialidad objetiva sostiene que un Estado puede ejercer su jurisdicción sobre cualquier asunto que ocurra en su territorio[64]. En el contexto del Metaverso, donde la protección de datos es crucial, esta teoría sugeriría que, si los datos son recogidos, almacenados o procesados en el Metaverso gobernado por la UE, la normativa comunitaria (como el RGPD) se aplicaría, sin importar la localización de la empresa que recopila estos datos[65]. Por otro lado, el principio de la personalidad subjetiva propone que un Estado tiene jurisdicción sobre sus ciudadanos independientemente de su ubicación en el Metaverso. Bajo esta teoría, las empresas de la UE que procesen datos personales a través de plataformas metavérsicas extracomunitarias seguirían estando sujetas al RGPD[66]. En lo que respecta a la teoría de la protección de intereses, se argumenta que un Estado tiene la autoridad para regular comportamientos en el Metaverso más allá de sus límites

[62] O. Bigos, "Jurisdiction over Cross-Border Wrongs on the Internet", *International and Comparative Law Quarterly,* vol. 54, nº 3, 2005, p. 585.

[63] Rt. Ford, "Law's Territory: (A History of Jurisdiction)", *Michigan Law Review*, vol. 97, nº 4, 1999, p. 843.

[64] L. Bartels, "The EU's Human Rights Obligations in Relation to Policies with Extraterritorial Effects", *European Journal of International Law*, vol. 25, 2015, p. 1071.

[65] En cambio, la teoría de la territorialidad subjetiva establece que un Estado tiene jurisdicción sobre acciones realizadas por sus ciudadanos, sin importar donde éstas ocurran. Es decir, un Estado puede ejercer su jurisdicción sobre un ciudadano que ha cometido un delito en el extranjero, debido a su ciudadanía con ese Estado. Por ejemplo, si un ciudadano de un país A comete un delito en el país B, el país A puede tener jurisdicción sobre el delito si aplicamos la teoría de la territorialidad subjetiva.

[66] Por otro lado, la teoría de la personalidad objetiva sostiene que un Estado tiene jurisdicción sobre personas extranjeras que cometen delitos contra sus ciudadanos, sin importar donde ocurran los hechos. Es decir, si un ciudadano de un país A es víctima de un delito cometido por un ciudadano de un país B en un tercer país C, el país A podría ejercer jurisdicción sobre el ciudadano del país B, de acuerdo a la teoría de la personalidad objetiva.

territoriales si estos comportamientos afectan a sus intereses esenciales, como la seguridad nacional. De acuerdo con esta teoría, la UE podría justificar la aplicación extraterritorial del RGPD en el Metaverso para proteger la privacidad y los derechos fundamentales de sus ciudadanos[67]. Y, por último, la doctrina de los efectos mantiene que un Estado puede regular comportamientos en el Metaverso incluso si ocurren fuera de su territorio, siempre y cuando estos comportamientos tengan efectos dentro de sus fronteras. Desde el prisma de la protección de datos en el Metaverso, esto permitiría a la UE regular la actividad de empresas extranjeras que ofrezcan bienes o servicios a personas a través del Metaverso en la UE, o que supervisen su comportamiento, incluso si estas empresas no tienen una presencia física en el territorio de uno de los Estados miembros. Cada una de estas teorías presenta sus propios desafíos, limitaciones y su aplicabilidad específica dependerá de toda una serie de factores *ad hoc*[68].

36. La interpretación de los artículos 2[69] y 3[70] del RGPD de la UE en el contexto del Metaverso plantea cuestiones importantes en términos de jurisdicción y la aplicabilidad global de estos principios[71]. En primer lugar, es esencial entender que el RGPD presenta una aplicación extraterritorial que desafía las concepciones convencionales de jurisdicción y soberanía[72], incluso en el vasto y descentralizado Metaverso. Estos artículos estipulan que cualquier ente, organismo o empresa, sin importar su ubicación geográfica o incluso su existencia en el Metaverso, que procese datos de individuos ubicados en la UE, está bajo el alcance del RGPD. Esto infiere que los Estados, e incluso las entidades dentro del Metaverso, no pueden ejercer jurisdicción en este asunto a menos que se les otorgue permiso explícito. Desde esta perspectiva, surgen preguntas sobre qué conexión debe existir para que las autoridades europeas puedan intervenir, incluso en el ámbito virtual del Metaverso. Aunque el RGPD no es completamente explícito en este punto, se podría argumentar que este vínculo puede estar determinado por el lugar de generación de los datos, el lugar donde se almacenan, el lugar donde generan impactos, o incluso, por la residencia o nacionalidad del titular de los datos, aunque dicha persona pueda estar interactuando desde un avatar en el Metaverso[73].

37. Asimismo, el RGPD hace una distinción esencial entre los términos "encargado" y "responsable" en relación con el tratamiento de datos[74]. El término "responsable del tratamiento" se refiere a una entidad u organización que determina los fines y los medios del tratamiento de datos personales. Es el responsable último de garantizar que el tratamiento de los datos se realice de acuerdo con las disposiciones legales y los principios del RGPD. En otras palabras, el responsable del tratamiento tiene el control y la toma de decisiones sobre los datos personales. Por otro lado, un "encargado del tratamiento"

---

[67] M. Hildebrandt, "Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace", *Toronto Law Journal*, vol. 63, nº 2, 2013, p. 196.

[68] O.J. Gstrein, A.J. Zwitter, "Extraterritorial Application of the GDPR: Promoting European Values or Power?", *Internet Policy Review*, vol. 10(3), 2021, p. 2; así como M. Hildebrandt, "Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace", *Toronto Law Journal*, vol. 63(2), 2013, p. 196.

[69] El alcance de aplicación del RGPD, según el artículo 2, abarca las actividades de tratamiento de datos personales en el contexto de las operaciones de una empresa o establecimiento en la UE. Esto se aplica tanto a organizaciones ubicadas en la UE como a aquellas fuera de ella que ofrezcan bienes o servicios a personas en la UE o realicen el seguimiento del comportamiento de individuos en la UE.

[70] Por otro lado, el artículo 3 del RGPD establece el alcance territorial de la normativa y su aplicabilidad. Según esta disposición, el RGPD se aplica a todas las organizaciones y empresas que procesen datos personales de personas ubicadas en la UE, independientemente de su ubicación geográfica. Es decir, las organizaciones establecidas en la UE y las que operan fuera de ella, pero tratan datos personales de ciudadanos de la UE están sujetas a las disposiciones del RGPD. Además, el artículo 3 también contempla el procesamiento de datos relacionados con la oferta de bienes o servicios a personas en la UE, así como el monitoreo del comportamiento de las personas dentro de la UE.

[71] P. De Hert, M. Czerniawski, "Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context", *International Data Privacy Law,* vol. 6, nº 3, 2016, p. 230.

[72] T. Corballis, M. Soar, "Utopia of abstraction: digital organizations and the promise of sovereignty", *Big Data and Society*, vol. 9, nº 1, 2022. [En línea] Disponible en: https://doi.org/10.1177/20539517221084587

[73] A. Gascón Marcén, "El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea", *Cuadernos de Derecho Transnacional,* vol. 13, nº 2, 2021, pp. 216-217.

[74] C. Alvarez Rigaudias, A. Spina, "Article 37: Designation of the Data Protection Officer", en C. KUNER et al. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary,* Oxford University Press, 2020.

es una entidad u organización que trata los datos personales en nombre del responsable del tratamiento. El encargado del tratamiento actúa bajo las instrucciones del responsable y debe cumplir con las disposiciones legales establecidas por el RGPD. El encargado del tratamiento no toma decisiones autónomas sobre el uso de los datos, sino que se limita a procesarlos de acuerdo con las instrucciones del responsable. Es importante destacar que tanto el responsable como el encargado del tratamiento tienen responsabilidades específicas en relación con la protección de datos personales. El responsable del tratamiento debe asegurarse de que se cumplan los principios fundamentales del RGPD, como la licitud, la transparencia, la limitación de la finalidad, la minimización de los datos y la seguridad. Además, el responsable del tratamiento es el encargado de obtener el consentimiento adecuado de los individuos cuyos datos se procesan, así como de garantizar el ejercicio de los derechos de los interesados. Por su parte, el encargado del tratamiento tiene la obligación de tratar los datos personales de manera segura y sólo de acuerdo con las instrucciones proporcionadas por el responsable. Debe implementar las medidas técnicas y organizativas apropiadas para proteger los datos y garantizar la confidencialidad, integridad y disponibilidad de la información. Además, el encargado del tratamiento debe informar al responsable sobre cualquier violación de datos que ocurra durante el proceso de tratamiento[75].

38. Teniendo en cuenta el impacto significativo de esta regulación europea, que se estima que ha servido como referente para el planteamiento y desarrollo de la legislación interna de más de 100 Estados[76], es razonable plantearnos: ¿podríamos inferir o derivar principios generales u obligaciones *erga omnes* en el Derecho Internacional a partir del RGPD, especialmente en el ámbito del Metaverso? Las obligaciones *erga omnes* hacen referencia a los deberes que los Estados tienen hacia la comunidad internacional en su conjunto. Posiblemente, dada la relevancia del RGPD, se esté esbozando un principio general de protección de datos en el Metaverso que obligue a todos los Estados a garantizar la seguridad de esta información en dicho universo virtual. En cualquier caso, lo que es innegable es que éste es un territorio inexplorado y emocionante para futuros debates jurídicos y regulatorios[77].

39. Enfrentar los desafíos de jurisdicción en las transferencias de datos transatlánticas en el Metaverso requiere un examen detallado de diversos factores mitigantes. Estos factores buscan aliviar las tensiones que emergen cuando una organización internacional como la UE intenta imponer sus normas de protección de datos a actividades que ocurren más allá de sus fronteras, provocando posibles conflictos de soberanía digital[78]. Uno de los elementos más críticos en estas circunstancias es la conexión con el ente territorial (Estado u organización internacional) que busca implementar su normativa. Esto implica determinar el grado de contacto o interacción que la actividad en cuestión tiene con dicho sujeto de Derecho Internacional en el Metaverso. Si existe una conexión sustancial, es probable que se autorice la aplicación de la normativa en cuestión. Éste sería el caso, por ejemplo, si una corporación de un metaverso administrado por una empresa estadounidense es, a su vez, propietaria de una empresa subsidiaria en un metaverso europeo y recolecta datos de avatares europeos o que se conectan desde uno de los Estados miembros de la UE.

40. No obstante, el interés legítimo juega un papel igualmente crucial en la resolución de estos conflictos[79]. Una empresa metavérsica puede tener un interés legítimo a la hora de proteger a sus avatares y los datos personales asociados a los mismos en el Metaverso, pero también puede existir un

[75] D. Svantesson, "Article 4(1)(a) "Establishment of the Controller" in EU Data Privacy Law – Time to Rein in This Expanding Concept?", *International Data Privacy Law,* vol. 6(3), 2016, p. 210.

[76] A. Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020.

[77] B. Van Alsenoy, "Reconciling the (Extra)territorial Reach of the GDPR with Public International Law" en G. VERMEULEN, E. LIEVENS (eds), *Data Protection and Privacy under Pressure: Transatlantic Tensions, EU Surveillance, and Big Data,* Maklu, 2017.

[78] K. Dear, "Beyond the 'geo' in geopolitics: the digital transformation of power", *The RUSI Journal,* vol. 166, nº 6-7, 2022. [En línea] Disponible en: https://doi.org/10.1080/03071847.2022.2049167

[79] H.L. Buxbaum, "Territory, Territoriality and the Resolution of Jurisdictional Conflicts", *American Journal of Comparative Law*, vol. 57, nº 2, 2009, p. 631.

interés igualmente legítimo en fomentar la libre circulación de datos, especialmente en el contexto del comercio digital en el Metaverso. Por lo tanto, se deben tener en cuenta ambos aspectos y equilibrar estos intereses divergentes.

41. Más allá del interés legítimo, es esencial considerar si es razonable aplicar la normativa de un determinado Estado u organización internacional a una situación particular en el Metaverso. Este aspecto implica sopesar el interés legítimo de la empresa metavérsica contra otros intereses que puedan estar en juego. Por ejemplo, si la implementación de una determinada normativa en el Metaverso resulta en una carga excesivamente gravosa para un gigante tecnológico, entonces puede ser razonable limitar su implementación.

42. Aunque la territorialidad constituye un principio fundamental en Derecho Internacional, en la era digital y aún más en el Metaverso, las fronteras físicas están difuminándose o, como mínimo, perdiendo relevancia[80]. En este contexto, estos factores atenuantes son de suma importancia para lograr un equilibrio entre la protección de los derechos individuales en el Metaverso y la necesidad de facilitar el comercio y la cooperación internacionales en estos entornos. Estos factores deberían ayudar a los legisladores y a los tribunales competentes a tomar decisiones equilibradas y justas en relación con los conflictos de jurisdicción en las transferencias de datos transatlánticas.

3. La protección de datos como valor europeo

43. Finalmente, otra opción podría ser considerar la protección de datos en el Metaverso como un valor de la UE. Este cambio implicaría reconocer la protección de datos en el Metaverso como un derecho humano esencial[81], equiparable a otros derechos como la libertad de expresión o el derecho a un juicio justo. Sin duda, este enfoque centrado en los derechos humanos podría proporcionar una mayor protección a los avatares de la UE en el Metaverso -conectados desde una IP europea, residentes o nacionales en uno de los Estados miembros-, aunque también podría generar tensiones con intereses comerciales y de seguridad digital. De acuerdo con el artículo 2 del Tratado de la UE (TUE), la Unión se fundamenta en valores como el respeto a la dignidad humana, la libertad, la democracia, la igualdad, el Estado de Derecho y el respeto de los derechos humanos[82]. Estos valores, que son comunes a los Estados miembros en una sociedad caracterizada por el pluralismo, la no discriminación, la tolerancia, la justicia, la solidaridad y la igualdad entre mujeres y hombres, abogan claramente por una protección de datos sólida y efectiva en el Metaverso, entendiendo ésta como una extensión necesaria de la dignidad humana y la libertad individual en este universo virtual. En el marco del artículo 3.5, la UE contribuye a la protección de los derechos humanos en sus relaciones con el mundo exterior, incluyendo el Metaverso. La protección de datos, reconocida como un derecho humano fundamental, podría proyectarse en estas relaciones para garantizar que se cumpla tanto dentro como fuera de la UE en el Metaverso. Asimismo, en función de lo dispuesto en el artículo 21.1, la acción de la Unión en la escena internacional busca consolidar y promover la democracia, el Estado de Derecho, los derechos humanos y los principios del Derecho Internacional. Con la elevación de la protección de datos en el Metaverso a la categoría de valor, este principio podría reforzarse, ya que un mayor nivel de protección de datos implicaría un fortalecimiento de la protección de los derechos humanos en estos mundos virtuales.[83] No obstante,

[80] J. Knox, "The metaverse, or the serious business of tech frontiers", *Postdigital Science and Education*, vol. 4, nº 2, 2022, pp. 207-215. [En línea] Disponible en: https://doi.org/10.1007/s42438-022-00300-9

[81] L. Bartels, "The EU's Human Rights Obligations in Relation to Policies with Extraterritorial Effects", *European Journal of International Law*, vol. 25, 2015, p. 1071.

[82] O.J. Gstrein, A.J. Zwitter, "Extraterritorial Application of the GDPR: Promoting European Values or Power?", *Internet Policy Review*, vol. 10, nº 3, 2021, p. 2.

[83] El artículo 21 del TUE contempla los principios fundamentales que pueden relacionarse con la ciudadanía europea. Reconoce y garantiza el derecho de todos los ciudadanos de la Unión a moverse y residir libremente en el territorio de los Estados miembros, así como el derecho de ser elegibles y votar en las elecciones municipales y al Parlamento Europeo en el Estado

es necesario encontrar un equilibrio entre esta protección y los posibles desafíos que puedan surgir en términos de intereses comerciales y de seguridad digital. El reto reside en garantizar una protección de datos efectiva en el Metaverso sin comprometer las libertades económicas y la seguridad que también son pilares fundamentales de la UE, incluso en estos nuevos espacios.

VI. La recolección (i)lícita de todo tipo de datos

44. El seguimiento intensivo de las *cookies* por parte de empresas estadounidenses ha planteado un dilema intrincado para la privacidad de los individuos en Europa. Este acto de recopilación de datos, que se lleva a cabo frecuentemente bajo la máscara de servicios ofrecidos gratuitamente, ha encendido un debate sobre la eficacia de las regulaciones europeas y la competencia de las autoridades relevantes para supervisar y administrar dichos datos. Esta situación desemboca en un problema complejo para la privacidad en el Metaverso. En un entorno digital interconectado y persistente como el Metaverso, el seguimiento y la recopilación de datos pueden ser aún más omnipresentes. Las mismas preocupaciones que existen en el mundo real sobre la capacidad de las autoridades europeas para controlar y gestionar estos datos se magnifican en el Metaverso, especialmente, en relación con aquellos datos personales que pueden comprometer la seguridad de los usuarios.

45. El RGPD representa la piedra angular para proteger la privacidad y la seguridad de los datos de los usuarios. Esta legislación se centra principalmente en la gestión y el uso de los datos personales, que están definidos como cualquier información que puede vincularse a un individuo identificable. Los elementos que pueden ser utilizados para establecer esta identificación son variados e incluyen, pero no se limitan a nombres, números de identificación, datos de ubicación y otros identificadores digitales. Los factores asociados con la identidad de una persona en los ámbitos físico, fisiológico, genético, mental, económico, cultural y social también entran en esta categoría, de acuerdo con el artículo 4(1) del RGPD[84]. En el contexto del Metaverso, una realidad virtual hiperconectada que integra aspectos físicos y digitales, la importancia del RGPD se intensifica. Los datos personales en el Metaverso no sólo pueden incluir información típica como nombres o ubicaciones, sino que pueden extenderse a datos más complejos y sensibles. Con este nuevo tipo de datos personales en juego, el RGPD proporciona un marco necesario para su gestión y protección. Asimismo, plantea nuevos desafíos en términos de cómo adaptar y ampliar las regulaciones actuales para afrontar la creciente complejidad y la naturaleza inmersiva de los datos personales en el Metaverso.

46. Dentro del universo de los datos personales, encontramos una clasificación específica que tiene una relevancia y sensibilidad especial, denominada como datos sensibles o de categorías especiales. Tal como lo señala el artículo 9(1) del RGPD[85], estos datos están compuestos por información que puede

miembro donde residen. Además, el artículo 21 del TUE prohíbe cualquier discriminación por motivos de nacionalidad, asegurando que todos los ciudadanos de la Unión gocen de igualdad de trato y oportunidades en los Estados miembros.

[84] El artículo 4.1 del RGPD define algunos de los conceptos fundamentales utilizados en el marco de esta legislación europea de protección de datos. Estos conceptos incluyen datos personales, tratamiento de datos, responsable del tratamiento, encargado del tratamiento, y muchas otras definiciones clave. El artículo 4.1 del RGPD establece una base común de terminología y comprensión para garantizar una interpretación uniforme y consistente de la normativa en todos los Estados miembros de la UE. Estas definiciones son esenciales para comprender y aplicar las obligaciones y derechos establecidos en el RGPD, y juegan un papel crucial en la protección de la privacidad y los datos personales de los individuos en el contexto digital actual.

[85] El artículo 9.1 del RGPD aborda una cuestión fundamental relacionada con el procesamiento de categorías especiales de datos personales. Estas categorías incluyen información sensible, como origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos para identificar de manera única a una persona, datos de salud o datos relativos a la vida sexual u orientación sexual. El artículo 9.1 establece que el procesamiento de estos datos está en principio prohibido, a menos que exista una base legal específica para ello. Esto resalta la importancia de proteger la privacidad y la integridad de estos datos especialmente sensibles, y destaca la necesidad de un consentimiento explícito por parte del titular de los datos o la existencia de una justificación legítima para su procesamiento. Esta disposición del RGPD tiene como objetivo garantizar un nivel elevado de protección de la privacidad y salvaguardar los derechos fundamentales de los individuos en relación con la gestión de sus datos personales más delicados.

desvelar aspectos críticos de la identidad de una persona, como su origen racial o étnico, las opiniones políticas que sostiene, sus creencias religiosas o filosóficas y hasta su afiliación a sindicatos. En el Metaverso, las fronteras de lo que se considera como datos sensibles se están expandiendo, engendrando nuevas categorías de información delicada y formas inéditas de obtenerla. La inmersión en los mundos virtuales puede revelar patrones de comportamiento, interacciones y preferencias que, aunque en principio pueden parecer triviales, pueden ofrecer una visión muy detallada y profunda de la psicología, emociones y tendencias de un usuario. Un ejemplo notable puede ser los metadatos de movimiento y localización dentro del Metaverso, que podrían revelar información sobre la personalidad o el estado de ánimo de un individuo. Además, nuevas formas de identificación únicas, como la voz o la forma de moverse en el espacio virtual, podrían considerarse como datos biométricos sensibles. Las reacciones emocionales a ciertos estímulos dentro del Metaverso, medidas por ejemplo a través de las respuestas biológicas o expresiones faciales capturadas por la realidad virtual, también pueden constituir un nuevo tipo de datos sensibles. Asimismo, en un Metaverso en el que la identidad digital puede ser tan o más relevante que la identidad física, los avatares y sus atributos pueden llegar a ser considerados como datos sensibles, en particular si reflejan características personales, preferencias de estilo de vida, o incluso orientaciones sexuales.

47. Para alcanzar una comprensión holística del ámbito de la protección de datos, es necesario profundizar en una categoría que se encuentra fuera del alcance del RGPD: los datos no personales. Estos datos, cuya singularidad radica en la incapacidad de ser asociados a una persona específica identificada o identificable, se manifiestan en dos formas: anónima o pseudonimizada. Los datos anónimos son aquellos que, desde su origen, no pueden asociarse a una persona, mientras que los datos pseudonimizados son datos personales que han sido procesados de tal manera que no pueden ser vinculados a una persona sin utilizar información adicional. El RGPD, en su artículo 4(5), establece que los datos pseudonimizados aún se consideran datos personales, pero admite que proporcionan una protección adicional para los derechos de las personas a las que se refieren los datos. Esta protección adicional facilita a los controladores y procesadores de datos cumplir con las normas de privacidad y protección de datos. No obstante, cuando hablamos de los datos no personales, el marco regulatorio se torna más flexible, permitiendo que estos datos puedan ser procesados y transferidos con una mayor libertad. Esto es crucial para el funcionamiento y desarrollo de diversas aplicaciones tecnológicas, especialmente en campos como las estadísticas y la inteligencia artificial. En el contexto del Metaverso, una realidad virtual compartida y persistente que incluye múltiples universos digitales, esta distinción entre datos personales y no personales es crucial. Los datos no personales podrían ser utilizados en el Metaverso para mejorar experiencias de usuario, desarrollar nuevas funcionalidades o alimentar sistemas de inteligencia artificial sin violar las normas de privacidad. Al no estar ligados a una persona identificable, estos datos aportan una gran cantidad de información que puede ser valiosa para entender comportamientos globales y tendencias en este espacio digital. Sin embargo, es importante destacar que, aunque estos datos otorgan mayor libertad de operación, su uso responsable sigue siendo una necesidad imperante para preservar la confianza y la seguridad en el Metaverso[86].

48. El RGPD proporciona un marco normativo claro y restrictivo, estableciendo exigencias precisas para las empresas que recopilan y utilizan datos personales. Una de las disposiciones fundamentales del RGPD es la obligación de que las empresas obtengan un consentimiento explícito e informado de las personas antes de recoger sus datos. Esto significa que los individuos deben ser conscientes de para qué se van a utilizar sus datos y dar su aprobación de forma clara y proactiva. Además, el RGPD prohíbe que las empresas utilicen los datos personales para fines distintos a los que se acordaron originalmente. Este principio de limitación de la finalidad protege a los individuos de un uso abusivo o no deseado de su información personal. A estas protecciones se suma el "derecho al olvido", una disposición que permite a las personas solicitar que sus datos sean borrados de las bases de datos de las empresas. Este derecho, también conocido como derecho de supresión, garantiza que los individuos puedan controlar su presencia digital y proteger su privacidad. En el contexto del Metaverso, las normas del RGPD adquieren una

[86] J. Cruz Ángeles, "La libre circulación de datos (no) personales en el mercado único digital europeo", en A. Emaldi Cirión, E. La Spina (coords), *Retos del Derecho ante un mundo global*, Tirant Lo Blanch, Valencia, 2020, pp. 747-771.

relevancia especial. Dada la naturaleza inmersiva y personalizada de las experiencias en el Metaverso, los datos personales son una pieza esencial para su funcionamiento. Las empresas que operan en este espacio deben, por lo tanto, implementar políticas y prácticas robustas de privacidad y protección de datos para cumplir con las normas del RGPD. El consentimiento informado y explícito para la recopilación de datos se vuelve aún más crucial en el Metaverso, donde las interacciones digitales pueden generar una gran cantidad de información personal. De igual manera, el respeto al principio de limitación de la finalidad garantiza que las experiencias personalizadas del Metaverso no comprometan la privacidad y los derechos de las personas. El "derecho al olvido", por su parte, tiene un papel especialmente importante en el Metaverso. En un mundo digital en constante evolución, la capacidad de los individuos para eliminar sus datos personales puede ser un medio efectivo para controlar su identidad digital y proteger su privacidad. Por lo tanto, las empresas que operan en el Metaverso deberán proporcionar a los usuarios las herramientas necesarias para ejercer dicho derecho, *inter alia*[87].

49. El caso Google Spain vs. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González en 2014 marcó un hito en el ámbito de la protección de datos personales en Europa. En esta Sentencia, el TJUE estableció el "derecho al olvido", permitiendo a los individuos solicitar a Google la eliminación de ciertos enlaces de los resultados de búsqueda que les conciernen. Este derecho, sin embargo, está lejos de ser absoluto, ya que debe equilibrarse con el interés público en tener acceso a la información. El alcance de este caso afectó no solo al tipo de datos personales que Google maneja, sino también a cómo y dónde se aplica dicha normativa. Como tal, la Sentencia se centró en la información personal considerada desactualizada, incorrecta o irrelevante[88]. A raíz de esta decisión, Google limitó inicialmente el derecho al olvido a las solicitudes provenientes de los Estados miembros de la UE, reflejándose en las versiones europeas de su motor de búsqueda. Esto abrió un debate sobre la aplicación territorial de la normativa en materia de protección de datos. La cuestión de la responsabilidad también fue fundamental en este caso. El TJUE estableció que Google es responsable de los datos que procesa y presenta en sus resultados de búsqueda. De modo que, si la información se considera incorrecta, irrelevante o ya no es relevante, Google tiene la obligación de eliminar los enlaces a dicha información, siempre y cuando se cumpla con la normativa europea[89].

50. Sin embargo, la complejidad se acentúa cuando consideramos tecnologías como el navegador Tor y VPNs, que pueden usarse para falsear los datos de geolocalización, y las diferencias en la legislación nacional, como en Francia, donde los individuos pueden solicitar la supresión de sus datos personales directamente ante las autoridades nacionales. También surge un problema con los países que otorgan la nacionalidad por la vía del *ius sanguinis* en lugar del *ius soli*, como Italia. Esto significa que las normas de protección de datos aplicables pueden variar dependiendo de la nacionalidad y residencia del individuo. Esta diversidad de situaciones requiere un análisis *ad hoc* para determinar la jurisdicción competente, teniendo en cuenta factores como la ubicación del individuo, la naturaleza de la información, su relevancia y si existe un interés público en su accesibilidad.

51. La creación de diferentes versiones de Google, basadas en sus distintos dominios como ".com", ".it", ".es", ".fr", entre otros, ha introducido una manera alternativa de manejar la información, lo que podría considerarse como una "fragmentación de la información". Esto se debe a que la legislación que rige el uso y gestión de la información puede variar considerablemente de un dominio a otro. Por ejemplo, el dominio internacional ".com" podría estar sujeto a normativas diferentes que las aplicables a los dominios específicos de cada país, como ".es" para España, ".it" para Italia, ".fr" para Francia, *inter*

[87] Sobre esta materia, vid. J. Ausloos, *The Right to Erasure in EU Data Protection Law: From Individual Rights to Personal Protection*, Oxford University Press, 2020.

[88] S. Kulk, F.Z. Borgesius, "Google Spain v. González: Did the Court Forget about Freedom of Expression?: Case C-131/12 Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González", *European Journal of Risk Regulation,* vol. 5(3), 2014, p. 389.

[89] D. Svantesson, "The Google Spain Case: Part of a Harmful Trend of Jurisdictional Overreach", *European University Institute Robert Schuman Centre for Advanced Studies Research Paper,* nº RSCAS 2015/45, 2015.

alia. Esta situación ha añadido una capa de complejidad en la interpretación y aplicación del "derecho al olvido" y las regulaciones de protección de datos en general. Específicamente, podría resultar desafiante para las personas entender y navegar por las diferentes normativas de protección de datos que pueden aplicarse según el dominio que estén utilizando. Entendemos que la estrategia o "modelo Google" sería perfectamente aplicable al Metaverso, un espacio digital interconectado que simula universos alternativos, esta "fragmentación de la información" puede presentar desafíos similares[90]. En un entorno donde los usuarios pueden moverse virtualmente entre distintos espacios digitales, las reglas de protección de datos podrían variar dependiendo del espacio digital o "dominio" en el que se encuentren. Además, en un Metaverso global, las distintas normativas en materia de protección de datos de diferentes jurisdicciones pueden entrar en conflicto, añadiendo aún más complejidad. Esto puede hacer que sea difícil para los usuarios entender sus derechos y para los proveedores de bienes y servicios en el Metaverso cumplir con todas las normativas aplicables. Por lo tanto, es esencial que se establezcan normativas claras y uniformes de protección de datos en estos espacios virtuales para proteger los derechos de los usuarios y proporcionar una experiencia de usuario segura y confiable.

52. El RGPD trae consigo una transformación significativa en las obligaciones que incumben a las empresas. Este marco normativo no se limita a requerir que las compañías se ajusten a la normativa, sino que va un paso más allá. El RGPD exige a las empresas demostrar de manera proactiva su conformidad con las disposiciones del Reglamento a través de una serie de acciones específicas. Una de estas medidas es la realización de Evaluaciones de Impacto de Protección de Datos (EIPD). Estas evaluaciones son análisis sistemáticos que las empresas deben llevar a cabo cuando planean implementar nuevas tecnologías o procesos que puedan tener un impacto significativo en la protección de los datos personales. Otra disposición importante del RGPD es la designación de un Delegado de Protección de Datos (DPD) o *Data Protection Officer* (DPO, por sus siglas en inglés). Esta figura desempeña un papel fundamental en garantizar el cumplimiento con las normas de protección de datos, ya que tiene la responsabilidad de supervisar las actividades de tratamiento de datos de la empresa y asesorar sobre el cumplimiento del RGPD. En el contexto del Metaverso, la aplicación de estas medidas adquiere una relevancia crucial. Esto puede implicar la realización de EIPD antes de implementar nuevas características o tecnologías en el Metaverso, para evaluar y mitigar los posibles riesgos para la protección de los datos personales. Además, la designación de un DPD puede ser esencial para asegurar que las prácticas de tratamiento de datos en el Metaverso se ajusten a las normativas y respeten los derechos de los usuarios. En última instancia, estas medidas pueden contribuir a generar un entorno de confianza y seguridad en el Metaverso, que proteja la privacidad de los usuarios y cumpla con las normas de protección de datos[91].

53. El RGPD tiene en sus disposiciones sanciones rigurosas para las empresas que no logren cumplir con sus requerimientos. La gravedad de estas sanciones se determina en función de la seriedad de la violación. Las empresas pueden enfrentar multas de hasta 20 millones de euros o el 4% de su facturación anual global, dependiendo de cuál de las dos cifras sea mayor. Estas penalizaciones no sólo evidencian la intensa importancia que la UE asigna a la protección de datos, sino que también funcionan como un potente incentivo para que las empresas tomen acciones concretas para asegurar su cumplimiento. Recientemente, empresas como Meta han sido sancionadas por violar las disposiciones del RGPD. El 22 de mayo de 2023, Meta fue penalizada con una multa de 1.200 millones de euros. No obstante, no ha sido la primera vez que ha tenido que enfrentar sanciones de esta índole. En 2022, Instagram, una de sus plataformas, ya fue multada con 405 millones de euros, mientras que, en 2021, WhatsApp, otra plataforma de la misma empresa, tuvo que hacer frente a una multa de 225 millones de euros.

[90] Véanse, *inter alia,* H. Ning, H. Wang, Y. Lin, W. Wang, S. Dhelim, F. Farha, J. Ding, M. Daneshmand, "A survey on metaverse: the state-of-the-art, technologies, applications, and challenges", *ArXiv*, 2021. [En línea] Disponible en: http://arxiv.org/abs/2111.09673. S. Park, Y. Kim, "A metaverse: taxonomy, components, applications, and open challenges", *IEEE Access,* vol. 10, 2022, pp. 4209-4251. [En línea] Disponible en: https://doi.org/10.1109/ACCESS.2021.3140175

[91] C. Álvarez Rigaudias, A. Spina, "Article 37: Designation of the Data Protection Officer", en C. Kuner y otros (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020.

54. La naturaleza global de Internet y el rápido crecimiento de las empresas de tecnología estadounidenses han propiciado un conflicto jurisdiccional en el terreno de la protección de datos. Aunque el RGPD se aplica a todas las empresas que operan en la UE, sin importar su ubicación geográfica, la aplicación efectiva de este Reglamento más allá de las fronteras europeas ha representado un desafío considerable. El RGPD fue concebido primordialmente para proteger a los ciudadanos europeos. No obstante, dado el carácter global de la recogida de datos, se puede interpretar que el RGPD tiene una vocación más amplia, o al menos expansiva. En teoría, si una empresa no europea recoge datos de un ciudadano de la UE, debería cumplir con el RGPD. Sin embargo, hacer valer esto en la práctica puede ser sumamente complicado. Las autoridades europeas tienen limitada capacidad para sancionar a empresas localizadas fuera de su jurisdicción. Además, las discrepancias entre la normativa de privacidad de datos en la UE y en los EE.UU. pueden generar situaciones en las que las empresas se ven atrapadas entre dos marcos legales divergentes. Estos conflictos jurisdiccionales podrían intensificarse en el Metaverso. Al ser un espacio digital global e interconectado que imita diferentes realidades, el Metaverso podría involucrar la recopilación y el procesamiento de datos de usuarios de todo el mundo. Las empresas que operan en el Metaverso tendrían que navegar por estas complejidades jurisdiccionales y garantizar que cumplen con las regulaciones de protección de datos en todas las regiones en las que operan. Esto podría implicar la adopción de un enfoque de "máximo cumplimiento", en el que se apliquen los estándares de protección de datos más rigurosos, como los del RGPD, independientemente de la ubicación del usuario. Sin embargo, esto puede resultar desafiante, dadas las diferencias entre las normativas en materia de protección de datos de diferentes jurisdicciones. Por tanto, sería conveniente adoptar un enfoque global y coherente para la regulación de la protección de datos en el Metaverso, que proteja la privacidad de los usuarios sin importar su ubicación geográfica.

55. La interacción entre la protección de datos y la globalización genera interrogantes relevantes sobre el futuro de la privacidad en el ciberespacio[92]. Si bien el RGPD puede interpretarse como un esfuerzo por extender la influencia de Europa en el ámbito de la privacidad de datos, es probable que su eficacia esté restringida sin una colaboración internacional sólida[93]. Podría ser necesario llegar a acuerdos globales para asegurar la privacidad de los datos en nuestro mundo hiperconectado actual. La universalidad de la normativa de protección de datos, al menos en cierta medida, podría ser indispensable para garantizar la protección de todos los ciudadanos, independientemente de la ubicación de las empresas que recolectan y utilizan sus datos. Aunque alcanzar este punto puede representar un camino largo y complejo, es un diálogo que debe continuar a medida que avanzamos en el siglo XXI. Cuando situamos este tema en el contexto del Metaverso, se intensifican las implicaciones. Como un espacio digital global e interconectado, el Metaverso abarca diferentes jurisdicciones y reúne a usuarios de todo el mundo. Las normas actuales de protección de datos, incluyendo el RGPD, pueden resultar insuficientes para regular de manera efectiva la privacidad de los datos en este nuevo espacio digital. En este sentido, la necesidad de acuerdos internacionales sobre la protección de datos puede ser aún más crucial en el Metaverso. Estos acuerdos podrían establecer estándares globales o principios generales para la recopilación, el uso y la protección de los datos personales en el Metaverso, garantizando la privacidad y los derechos de los usuarios en todo el mundo. El camino hacia estos acuerdos globales puede ser largo y lleno de desafíos. Sin embargo, es una conversación necesaria y urgente a medida que el Metaverso continúa desarrollándose y jugando un papel cada vez más prominente en nuestras vidas digitales.

VII. Los acuerdos transatlánticos en materia de protección de datos

56. Las relaciones entre la UE y los EE.UU., en lo que respecta a la protección de datos personales, han estado marcadas por el establecimiento y posterior anulación de dos acuerdos clave: el de

[92] L.A. Bygrave, *Data Privacy Law: An International Perspective*, Oxford University Press, 2014.

[93] U. Kohl, "Jurisdiction in Cyberspace" en N Tsagourias, R Buchan (eds.), *Research Handbook on International Law and Cyberspace,* Edward Elgar Publishing, 2015.

Safe Harbour (Puerto Seguro) y *Privacy Shield* (Escudo de la Privacidad)[94]. Estos acuerdos, nacidos con el objetivo de salvaguardar los datos personales de los ciudadanos de la UE durante su transferencia hacia los EE.UU., buscaban respetar las normativas europeas de protección de datos en este proceso transatlántico.

57. El primero de éstos, el Acuerdo de Puerto Seguro, fue una política adoptada por la Comisión Europea el 26 de julio de 2000 que permitía a las empresas de EE.UU. transferir datos personales de ciudadanos de la UE a los EE.UU., siempre y cuando demostraran que brindaban un nivel adecuado de protección de datos. *Safe Harbor* se basaba en una serie de principios a los que las empresas estadounidenses se comprometían a adherirse. Estos principios incluían el aviso (las empresas debían informar a las personas acerca de cómo se recopilan y usan sus datos), la elección (los usuarios debían tener la opción de optar por no participar si sus datos personales se iban a divulgar a terceros o usarse para un propósito distinto al original) y el acceso (los usuarios debían poder acceder a sus datos personales y corregirlos o eliminarlos si eran inexactos). Asimismo, también se establecieron procedimientos para resolver posibles disputas[95]. No obstante, la revelación en 2013 del caso Edward Snowden, que expuso la vigilancia masiva realizada por la Agencia de Seguridad Nacional (NSA) estadounidense, sembró la duda sobre si las medidas de protección y privacidad de los EE.UU. eran realmente suficientes[96]. La UE reaccionó ante esta situación con un profundo escepticismo, lo que llevó a una reconsideración de los acuerdos vigentes[97].

58. En el fallo del caso Schrems I, el TJUE estableció que el Acuerdo de Puerto Seguro no cumplía con una protección adecuada para los datos de los ciudadanos europeos[98]. Esta Sentencia condujo a la negociación de un nuevo acuerdo en 2016, el Escudo de Privacidad, que pretendía otorgar mayores garantías y un mayor nivel de protección de los datos transferidos[99]. Los principios rectores de este acuerdo incluían: aviso e información (las empresas deben informar a las personas sobre qué datos están recogiendo y cómo se utilizarán, incluyendo si los datos se transfieren a terceros), elección (los usuarios deben tener la opción de optar por no permitir que sus datos sean compartidos con terceros o utilizados para un propósito materialmente diferente al original para el cual fueron recogidos), responsabilidad por la transferencia posterior de datos (las empresas están obligadas a cumplir con los principios de *Privay Shield* incluso cuando los datos personales se transfieren a terceros), seguridad (las empresas deben tomar medidas razonables y apropiadas para proteger los datos personales de la pérdida, mal uso y acceso no autorizado), integridad y limitación de la finalidad de los datos (los datos personales deben ser relevantes para los fines para los que se van a utilizar y las empresas deben tomar medidas razonables para garantizar que los datos son precisos, completos y actualizados), acceso (los usuarios tienen el derecho de acceder a sus datos personales y de corregir, modificar o eliminar cualquier información que sea inexacta) y el derecho a interponer recursos, que se aplique la Ley e imputabilidad (las empresas deben proporcionar mecanismos para asegurar el cumplimiento de estos principios y proporcionar recursos para los usuarios que consideren que sus derechos no se han respetado). Sin embargo, en la Sentencia del 16 de julio de 2020, este acuerdo tampoco resistió el escrutinio legal en el caso Schrems II, y el TJUE dictaminó que la normativa vigente estadounidense no brindaba una protección suficiente[100].

---

[94] J.M. Assey, D.A. Eleftheriou, "The EU–US Privacy Safe Harbor: Smooth Sailing or Troubled Waters?", *CommLaw Conspectus*, vol. 9, 2001, p. 145.

[95] M. Schrems, "The Privacy Shield Is a Soft Update of the Safe Harbor", *European Data Protection Law Review*, vol. 2(2), 2016, p. 148; y también L. Colonna, "Article 4 of the EU Data Protection Directive and the Irrelevance of the EU–US Safe Harbor Program?", *International Data Privacy Law*, vol. 4(3), 2014, p. 203.

[96] A. Chander, U.P. LÊ, "Data Nationalism", *Emory Law Journal*, vol. 64, nº 3, 2015, p. 677.

[97] R. Carolina, "Why the EU Has Issued Relatively Few Data Protection Adequacy Determinations? A Reply", *Lawfare*, 13 enero 2017. [En línea] Disponible en: www.lawfareblog.com/why-eu-has-issued-relatively-few-data-protection-adequacy-determinations-reply.

[98] STJUE 6 octubre 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650.

[99] D. Cole, F. Fabbrini, "Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy across Borders", *International Journal of Constitutional Law*, vol. 14, nº 1, 2016, p. 220.

[100] STJUE 16 julio 2020, *Facebook Ireland y Schrems*, C-311/18, ECLI:EU:C:2020:559.

59. La revocación del Escudo de Privacidad tuvo una serie de consecuencias inmediatas para aquellas empresas que realizaban transferencias de datos extracomunitarias. Como recuerda el TJUE en la Sentencia Schrems II, el RGPD exige a los exportadores de datos que evalúen las condiciones que rigen las transferencias y que establezcan las medidas adecuadas para garantizar que estos datos estén sujetos a una protección sustancialmente equivalente a la garantizada en la UE. Tanto los controladores de datos como los procesadores que transfieren datos son responsables de estos requisitos[101]. De modo que, en la práctica, las organizaciones que transfieren los datos en aplicación de la legislación de los EE.UU. fueron las principales afectadas por esta Sentencia. Ante esta situación, se planteó que las autoridades de control de los Estados miembros de la UE no podían proporcionar respuestas individualizadas a las solicitudes de empresas y organizaciones que deseaban transferir datos a terceros países.

60. En ausencia del Escudo de Privacidad y de una decisión de adecuación válida, los mecanismos disponibles para las transferencias internacionales de datos resultaron ser las cláusulas contractuales tipo (en inglés, *Standard Contractual Clauses*, SCCs)[102] y las normas corporativas vinculantes (en inglés, *Binding Corporate Rules*, BCRs). No obstante, con arreglo a la Sentencia Schrems II, tanto unas como otras requieren de análisis para asegurar que se están proporcionando garantías adecuadas para la transferencia internacional de datos a terceros países que no cuentan con una decisión de adecuación de la Comisión Europea (entre ellos, EE.UU.). La mera existencia de cláusulas contractuales tipo no era suficiente, pues lo esencial era realizar una evaluación de las garantías existentes en la práctica. Cuando el destinatario de la transferencia no cumplía, o ya no podía cumplir, las garantías adecuadas que debían exigirse en el cumplimiento de cláusulas contractuales tipo de protección de datos (o de normas corporativas vinculantes), el TJUE señaló que "la suspensión de la transferencia de los datos o la rescisión del contrato es obligatoria para el responsable del tratamiento"[103].

61. Esta fase de inseguridad jurídica, posterior a Schrems II, concluyó el pasado 25 de marzo de 2022. En esa fecha, la Presidenta de la Comisión Europea Ursula von der Leyen y el Presidente de los EE.UU. Joe Biden acordaron los principios de un nuevo marco para la privacidad de datos entre estas dos potencias. Este marco busca promover los flujos de datos transatlánticos y abordar las preocupaciones identificadas por el TJUE[104]. Para alcanzar este objetivo, los equipos legales de ambos lados del Atlántico han dedicado varios meses a formular y materializar los detalles de este acuerdo, resultando en un nuevo marco legal. Finalmente, el 7 de octubre, el Presidente Biden firmó una orden ejecutiva titulada "Mejora de las salvaguardias para las actividades de inteligencia de señales de los EE.UU.". Junto con las regulaciones emitidas por el Fiscal General, esta orden ejecutiva restringe el acceso a los datos de la UE por parte de los servicios de inteligencia de EE.UU. y establece un Tribunal de Revisión de Protección de Datos. Esta acción constituye un hito crucial en el desarrollo del nuevo Acuerdo Transatlántico de Transferencia de Datos, que se examinará en profundidad en la siguiente sección del estudio[105].

[101] De acuerdo con el principio de responsabilidad, es la organización que realiza la cesión de datos quien debe evaluar si los datos transferidos al tercer país se beneficiarán de un nivel adecuado de protección. No corresponde a los tribunales ni a las autoridades de control realizar estas evaluaciones para todos los terceros países a los que se puedan transferir datos personales.

[102] Decisión de ejecución (UE) 2021/914 de la Comisión de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. Texto íntegro disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32021D0914

[103] STJUE 16 julio 2020, *Facebook Ireland y Schrems*, C-311/18, ECLI:EU:C:2020:559, apartado 140.

[104] Para más información, en cuanto al borrador, COMMISSION IMPLEMENTING DECISION of XXX pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, está disponible en https://commission.europa.eu/document/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en

[105] A. Chander, P.M. Schwartz, "Privacy and/or Trade", *University Chicago Law Review*, vol. 90, nº 1, 2023, p. 1.

VIII. El nuevo Acuerdo Transatlántico de Transferencia de Datos

62. El 10 de julio de 2023, las dos Grandes Potencias concluyeron sus negociaciones que culminaron en la adopción de la Decisión de Ejecución[106] de la Comisión Europea[107]. Esta Decisión establece toda una serie de reglas relativas a la transferencia de datos personales desde la UE hacia países terceros y organizaciones internacionales, bajo el paraguas del RGPD[108]. El objetivo principal de esta normativa es proteger la integridad de los datos personales durante su transferencia internacional, con el fin de asegurar un nivel de protección similar al que se otorga en la UE. La adopción de esta Decisión elimina la necesidad de autorización adicional para la transferencia de datos, siempre y cuando el tercer país ofrezca un nivel de protección que sea "esencialmente equivalente" al de la UE. El criterio de "equivalencia esencial" se determina mediante un análisis exhaustivo del sistema legal del tercer país, las regulaciones aplicables a los importadores de datos, y las salvaguardias relacionadas con el acceso a datos personales por parte de autoridades públicas[109].

63. La Sentencia Schrems II del TJUE, de 16 de julio de 2020, que anuló el acuerdo previo de transferencia de datos entre la UE y los EE.UU. debido a las limitaciones de protección de datos personales en el Derecho interno estadounidense, sirvió como un ejemplo clave en el establecimiento de requisitos para una nueva decisión de adecuación. En respuesta a Schrems II, se iniciaron conversaciones entre la Comisión y el Gobierno de los EE.UU. para una posible nueva decisión de adecuación. Como resultado, EE.UU. adoptó medidas para mejorar las salvaguardias de las actividades de inteligencia y actualizar el marco legal aplicable a las entidades comerciales que procesan datos transferidos desde la UE. Finalmente, la Comisión ha concluido que los EE.UU. garantizan un nivel de protección adecuado para los datos personales transferidos desde la UE a las organizaciones certificadas de los EE.UU., permitiendo así las transferencias de datos sin necesidad de una autorización adicional[110].

64. En relación con el Metaverso, esta decisión implica que los datos personales de los usuarios de la UE pueden ser transferidos de manera segura a entidades en los EE.UU. que operan en este espa-

[106] La elección del instrumento legal, en este caso, la Decisión de Ejecución, puede deberse a varias razones. (1) Eficacia inmediata: las Decisiones de Ejecución son vinculantes en su totalidad y entran en vigor de inmediato en todos los Estados miembros sin la necesidad de legislación adicional a nivel nacional. Esto garantiza una aplicación uniforme y rápida de las reglas en toda la UE. (2) Directamente aplicable a los destinatarios: las Decisiones de Ejecución pueden ser dirigidas a los Estados miembros, a grupos de Estados miembros o a individuos y entidades específicas. En este caso, la Decisión de Ejecución se aplica directamente a todas las entidades que manejan datos personales en la UE, lo que les impone obligaciones legales claras en relación con la transferencia de datos a terceros países. (3) Procedimiento eficiente: la adopción de una Decisión de Ejecución puede ser más rápida y eficiente que otros procedimientos legislativos, como la adopción de una Directiva, que requiere la transposición a las leyes nacionales de cada Estado miembro. (4) Garantía de conformidad: La Decisión de Ejecución se utiliza cuando es necesario garantizar que las disposiciones legales de la UE se apliquen de la misma manera en todos los Estados miembros. En este caso, se garantiza que la protección de los datos personales en las transferencias internacionales se maneje de manera uniforme en toda la UE. (5) Rápida respuesta a desarrollos globales: los avances tecnológicos y los cambios en las prácticas de transferencia de datos pueden requerir una respuesta rápida por parte de la UE. Una Decisión de Ejecución permite a la Comisión actuar de manera más rápida y decisiva. Es importante destacar que, aunque las Decisiones de Ejecución son efectivas y rápidas, se espera que la Comisión consulte a los comités de los Estados miembros y tenga en cuenta su posición, según el procedimiento de comitología. Este procedimiento garantiza que los Estados miembros puedan influir en la formación de la decisión.

[107] Decisión de Ejecución de la comisión de 10 de julio de 2023, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo al nivel adecuado de protección de los datos personales en el marco de privacidad de datos entre la UE y los EE.UU. Texto íntegro disponible en: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

[108] E. Fahey, *The Global Reach of EU Law*, Routledge, 2017.

[109] Este proceso implica una evaluación del marco legal y las prácticas de protección de datos en el país tercero, incluyendo las leyes de privacidad, los derechos de los individuos, la existencia de una autoridad de protección de datos, etc. Asimismo, este análisis también considera la existencia de medidas de seguridad adecuadas para proteger los datos personales contra el acceso no autorizado o ilegal.

[110] Este pasaje hace referencia a la posibilidad de transferir datos personales de la UE a los EE.UU. sin la necesidad de salvaguardias adicionales, como las Cláusulas Contractuales Estándar (CCE) o las Reglas Corporativas Vinculantes (BCR), gracias a la decisión de adecuación.

cio virtual. Para ello, bastará con que las empresas que brindan servicios en el Metaverso se adhieran a los requisitos de la Decisión para garantizar un nivel adecuado de protección de datos y mantengan la confianza de los usuarios.

65. El nuevo Marco de Protección de la Privacidad de los Datos UE-EE.UU. (DPF UE-EE. UU.) opera a través de un sistema de certificación y está sujeto a una revisión anual[111]. Se aplica a todas las organizaciones estadounidenses que actúan como responsables o encargados del tratamiento de datos personales[112], y su ámbito se extiende a cualquier dato personal transferido desde la UE a organizaciones en los EE.UU. que se adhieren a sus principios. El marco establece que los datos personales deben ser tratados de manera justa y legal y recolectados para fines específicos. También requiere que los interesados tengan la opción de oponerse al uso de sus datos para una nueva finalidad o su divulgación a un tercero. En el caso del tratamiento de categorías especiales de datos, tales como condiciones médicas, origen racial, opiniones políticas, creencias religiosas, afiliación sindical e información sobre la vida u orientación sexual, se requieren salvaguardias específicas. Los datos sensibles deben ser tratados con cuidado especial, y su uso para fines diferentes a los originalmente recolectados o autorizados posteriormente debe ser con el consentimiento explícito de las personas. En el Metaverso, la aplicación de este marco de protección de datos significa que las empresas que operan en este entorno virtual deben garantizar la protección de los datos personales de sus usuarios de acuerdo con estas directrices, fomentando la confianza y la seguridad en cualquiera de las manifestaciones de su interacción o actividad digital.

66. La precisión y minimización de los datos son principios cruciales para la protección de la información personal en el marco del nuevo Acuerdo. Los datos personales deben ser exactos, relevantes y limitados a lo que es necesario para el propósito por el que se están procesando[113]. Su conservación debe limitarse sólo al tiempo necesario para lograr los fines previstos, respetando así el principio de integridad y limitación de finalidad de los datos[114]. En el Metaverso, la gestión de los datos personales podría ampliarse a períodos más largos si sirve razonablemente a fines específicos como el archivo en interés público, periodismo, literatura y arte, investigación científica e histórica y análisis estadístico[115].

---

[111] La revisión anual es una característica clave de este marco y sirve para verificar que los EE.UU. siguen ofreciendo un nivel adecuado de protección de datos. Esto puede implicar el análisis de la legislación y las prácticas de los EE.UU., así como la evaluación del funcionamiento del sistema de certificación.

[112] En la legislación de la UE, los "datos sensibles" o "datos personales de categorías especiales" son un subconjunto de datos personales que están sujetos a protecciones más estrictas debido a su naturaleza. Según el RGPD de la UE, estos datos incluyen información sobre origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos procesados con el fin de identificar a una persona de manera única, salud, vida sexual u orientación sexual y condenas penales y delitos. El RGPD establece que el procesamiento de estos datos está en general prohibido, a menos que se aplique alguna de las excepciones previstas en el artículo 9.2 del RGPD. Algunas de estas excepciones incluyen el consentimiento explícito del individuo, la necesidad de procesar los datos para cumplir con las obligaciones y ejercer los derechos específicos del controlador en el campo del empleo y la seguridad social, la protección de los intereses vitales del individuo, o si los datos ya han sido publicados por el individuo. Esta categorización y protección de los "datos sensibles" se encuentra en el RGPD, específicamente en el artículo 9, titulado "Tratamiento de categorías especiales de datos personales". El RGPD es la pieza principal de la legislación de la UE en lo que respecta a la protección de datos personales y la privacidad.

[113] Principio de minimización de datos (Artículo 5.1.c del RGPD): este principio establece que los datos personales deben ser "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son procesados". En términos prácticos, significa que no se deben recoger o procesar más datos de los estrictamente necesarios para alcanzar el propósito definido. Este principio refuerza la noción de que el tratamiento de datos personales debe ser mínimo y restrictivo.

[114] Principio de limitación de la conservación (Artículo 5.1.e del RGPD): este principio estipula que los datos personales deben ser "conservados de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales". Es decir, los datos no deben ser almacenados indefinidamente después de que se hayan logrado los fines del tratamiento. Este principio también implica que los datos deben ser actualizados y/o eliminados si ya no son necesarios o si el individuo ha solicitado su eliminación.

[115] Casos excepcionales de conservación prolongada (Artículo 5.1.e del RGPD): en algunos casos, los datos personales pueden ser conservados durante un período de tiempo más largo, siempre que el tratamiento se realice únicamente con fines de archivo en interés público, investigación científica o histórica o fines estadísticos, de acuerdo con el artículo 89.1 del RGPD, siempre que se apliquen las medidas técnicas y organizativas apropiadas exigidas por el Reglamento para proteger los derechos y libertades del interesado.

Sin embargo, este procesamiento extendido debe hacerse con el consentimiento explícito del individuo y en conformidad con los principios de protección de datos[116]. En términos de seguridad, el Metaverso, como un entorno digital avanzado, debe garantizar la seguridad de los datos personales contra el tratamiento no autorizado o ilícito y contra la pérdida accidental, destrucción o daño[117]. Esto se logra a través del principio de seguridad, que exige la adopción de medidas de seguridad razonables y apropiadas, considerando los riesgos asociados con el procesamiento y la naturaleza de los datos[118].

67. Las organizaciones que aspiran a certificarse bajo el marco del Acuerdo deben plantear un compromiso público de adhesión a sus principios. Es esencial que estas entidades posean y apliquen políticas de privacidad sólidas y efectivas. Este proceso de certificación implica proporcionar al Departamento de Comercio (DoC)[119] información detallada sobre su estructura organizativa, propósitos de procesamiento de datos personales, tipo de datos que estarán bajo la protección de la certificación, método de verificación seleccionado, y la entidad con autoridad legal para garantizar el cumplimiento de los principios del Acuerdo. En el contexto del Metaverso, un universo virtual digital en expansión, la importancia de este proceso de certificación se intensifica. La certificación del DPF UE-EE.UU. no sólo sirve como una garantía de que una organización sigue un conjunto de normas y principios de protección de datos, sino que también se convierte en un distintivo de confianza para los usuarios del Metaverso que interactúan con estas organizaciones. Para continuar recibiendo datos personales de acuerdo con el DPF UE-EE.UU., las organizaciones deben ser parte de la lista del DPF del DoC y requerirán una renovación de la certificación de carácter anual. Si una organización decide abandonar el DPF, debe borrar todas las referencias que insinúen su participación continua en el Acuerdo. Esto es vital en el Metaverso, donde la confianza del usuario en las políticas de privacidad de una organización puede ser crítica para su éxito. El DoC se encarga de verificar el cumplimiento de todos los requisitos de certificación y confirmará que la organización tiene establecida una política de privacidad pública

[116] Consentimiento explícito (Artículo 4.11 del RGPD): el consentimiento explícito es uno de los fundamentos legales para el tratamiento de datos personales en la UE. Se define como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". Es esencialmente un acuerdo claro y directo de la persona para permitir el tratamiento de sus datos personales. Este consentimiento debe ser libre, informado, específico e inequívoco, y los interesados tienen el derecho de retirarlo en cualquier momento.

[117] Principio de seguridad (Artículo 5.1.f del RGPD): este principio sostiene que todos los datos personales deben ser procesados de manera que se asegure su seguridad, protegiéndolos contra el procesamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. Este principio implica que se deben implementar medidas técnicas y organizativas apropiadas para mantener la integridad y confidencialidad de los datos personales. Tales medidas pueden abarcar el uso de tecnologías de encriptación para proteger los datos cuando están en reposo o en tránsito, la implementación de software de seguridad como cortafuegos y antivirus, y el establecimiento de políticas de control de acceso para regular quién puede acceder a los datos. Además, este principio requiere la realización de evaluaciones regulares de riesgos y pruebas de seguridad para identificar y mitigar cualquier vulnerabilidad potencial que pueda poner en peligro la seguridad de los datos. De este modo, la aplicación efectiva del principio de seguridad puede requerir la adaptación y actualización constante de las medidas de seguridad en función de los cambios en los riesgos de seguridad y en el panorama de amenazas, así como de los avances en las tecnologías y las prácticas de seguridad.

[118] Medidas de seguridad (Artículo 32 del RGPD): este artículo estipula que los responsables del tratamiento y los encargados del tratamiento deben implementar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Estas medidas pueden incluir, entre otras, la pseudonimización y el cifrado de datos personales, la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resistencia de los sistemas y servicios de tratamiento, y un proceso para probar, examinar y evaluar regularmente la eficacia de las medidas de seguridad. La selección de las medidas debe basarse en una evaluación del riesgo que tenga en cuenta la naturaleza de los datos que se están procesando y los riesgos que conlleva su tratamiento.

[119] El Departamento de Comercio de los EE.UU. (DoC) es un organismo gubernamental que tiene una amplia gama de responsabilidades. En términos del Marco de Protección de la Privacidad UE-EE.UU., el DoC juega un papel esencial, ya que es el encargado de supervisar y administrar este marco. Esto implica asegurarse de que las empresas estadounidenses que reciben datos personales de la UE cumplen con los principios y requisitos establecidos en el marco. El DoC también mantiene una lista de las empresas que se han certificado bajo este marco, y proporciona un mecanismo para que las personas presenten quejas en caso de que sospechen que una empresa no está cumpliendo con sus obligaciones. Para más información véase: https://www.commerce.gov

adecuada. De ser necesario, el DoC también colaborará con la Comisión Federal de Comercio (FTC)[120] y el Departamento de Transporte (DoT)[121] para confirmar la supervisión efectiva de las organizaciones y resolver cualquier litigio.

68. El DoC implementa un monitoreo constante para asegurar la adhesión de las organizaciones a los principios del DPF UE-EE.UU., utilizando una variedad de mecanismos como "controles aleatorios"[122] y revisiones específicas en casos de posibles problemas de cumplimiento. En el Metaverso, la supervisión y cumplimiento son especialmente críticos debido a la naturaleza de interconexión y la cantidad de datos que se intercambian. Si una organización incumple los principios del DPF, será remitida a la autoridad competente para tomar acciones correctivas. Las infracciones persistentes pueden resultar en la eliminación de la lista del DPF[123], y la organización deberá eliminar o devolver los datos personales obtenidos bajo el Acuerdo.

69. El DoC tiene la responsabilidad de supervisar cualquier declaración falsa[124] de participación en el DPF UE-EE.UU. y el uso indebido de su marca de certificación[125]. Este control se realiza tanto proactivamente como en respuesta a denuncias, por ejemplo, las emitidas por las Autoridades de Protección de Datos (APD)[126]. En particular, el DoC lleva a cabo comprobaciones regulares para asegurar que las organizaciones (1) que se retiran del DPF UE-EE.UU., (2) no completan la re-certificación anual, (3) son eliminadas como participantes, o (4) no completan una certificación inicial, retiren todas las referencias al DPF UE-EE.UU. que podrían sugerir que la organización sigue activamente en el marco. En el contexto del Metaverso, el DoC puede incluso emplear búsquedas en línea para identificar menciones del DPF UE-EE.UU. en las políticas de privacidad de las organizaciones, con el fin de detectar y manejar declaraciones falsas de aquellas que nunca han sido parte del acuerdo. Para asegurar la protección de datos en la práctica, es esencial que existan autoridades independientes con competencias para supervisar y hacer cumplir las normas de protección de datos. En este caso, las organizaciones deben someterse a la jurisdicción de las autoridades estadounidenses competentes, como la FTC y el DoT. La FTC puede investigar el cumplimiento de los principios y las declaraciones falsas de adhesión a estos principios por parte de organizaciones que ya no están en la lista del DPF o que nunca se han certificado. Cuando se incumplen dichas órdenes, la FTC puede imponer sanciones civiles y otras medidas correctivas, lo cual puede resultar crítico para mantener la integridad del Metaverso.

70. El derecho a recursos eficientes, uno de los pilares esenciales del nuevo Acuerdo, se erige como un instrumento crucial para garantizar la protección de los datos de los individuos en la nueva era

[120] La Comisión Federal de Comercio (FTC) es una agencia independiente del Gobierno de los EE.UU., cuya misión es proteger a los consumidores y mantener la competencia en la economía del país. La FTC logra esto a través de la aplicación de las leyes antimonopolio y de protección al consumidor. En el contexto del Marco de Protección de la Privacidad UE-EE.UU., la FTC juega un papel crucial, ya que puede tomar medidas de cumplimiento contra las empresas que no respetan sus obligaciones bajo el marco. La FTC también tiene la facultad de investigar y llevar a cabo acciones legales contra las empresas que se involucran en prácticas comerciales desleales o engañosas. Para más información véase: https://www.ftc.gov/es.

[121] El Departamento de Transporte de los EE.UU. (DoT) es la agencia federal encargada de supervisar y coordinar todos los medios de transporte en el país. Esto incluye la regulación de la aviación, el ferrocarril, la navegación marítima, las carreteras y el transporte público. Aunque el DoT no tiene un papel directo en el Marco de Protección de la Privacidad UE-EE.UU., puede estar involucrado en la supervisión de las empresas de transporte que manejan datos personales y que se han certificado bajo el marco. Para más información véase: https://www.transportation.gov

[122] Los controles aleatorios son una serie de inspecciones sin previo aviso que realiza el DoC con el objetivo de garantizar el cumplimiento de las obligaciones establecidas en el DPF UE-EE.UU. por parte de las organizaciones certificadas.

[123] La lista del DPF es una lista pública mantenida por el DoC que enumera todas las organizaciones que han sido certificadas y están en conformidad con los principios del DPF UE-EE.UU.

[124] La declaración falsa de participación en el DPF UE-EE.UU. se refiere a cualquier reclamación incorrecta o engañosa hecha por una organización que afirma estar certificada y en conformidad con los principios del DPF UE-EE.UU., cuando en realidad no es así.

[125] Las Autoridades de Protección de Datos (APD) son instituciones o entidades públicas independientes encargadas de supervisar la correcta aplicación de la normativa de protección de datos en un territorio específico.

[126] La marca de certificación del DPF UE-EE.UU. es el logo o insignia proporcionado a la organización por el DoC que indica que cumplen con los principios del DPF UE-EE.UU.

digital y, particularmente, en el Metaverso, en tanto que un universo digital en expansión. Este principio impulsa el derecho de las personas a recurrir a mecanismos de resolución independientes, efectivos y accesibles para solucionar disputas relacionadas con la gestión de sus datos. La esencia de este principio reside en su naturaleza efectiva y accesible, permitiendo que los usuarios que habitan el Metaverso presenten quejas y exijan reparaciones por infracciones sin costo alguno. En este sentido, las organizaciones que operan dentro del Metaverso y están certificadas bajo el DPF UE-EE.UU. deben proveer dichos mecanismos de reparación. Estos mecanismos pueden ser proporcionados tanto en la UE como en los EE.UU. y pueden incluir la cooperación con las APD de la UE, la resolución alternativa de litigios[127] o los programas de privacidad desarrollados por el sector privado. En el mundo virtual del Metaverso, donde los datos de los usuarios son un componente esencial para la experiencia del usuario, estos mecanismos son especialmente relevantes. El DPF UE-EE.UU. establece un marco que asegura que los usuarios puedan presentar reclamaciones ante la organización, un organismo de resolución de litigios designado por la organización, las APD nacionales, el DoC de los EE.UU. o la FTC de los EE.UU. Para una comunicación más fluida, las organizaciones deben proporcionar una respuesta a los usuarios dentro de los 45 días desde la recepción de la reclamación. En el Metaverso, la rapidez y eficiencia de estos procesos son vitales para mantener la confianza y seguridad de los usuarios.

71. Los mecanismos de reparación establecidos por el DPF UE-EE.UU. también incluyen la posibilidad de acudir a arbitrajes vinculantes[128], proporcionando un mecanismo de última instancia en caso de que los otros canales de resolución de quejas o recursos no hayan proporcionado una resolución satisfactoria. En el Metaverso, este tipo de resoluciones vinculantes pueden ser de especial relevancia dada la complejidad y la rapidez de evolución de las tecnologías y los escenarios que pueden surgir. Es

[127] En el contexto de la protección de datos y las transferencias entre la UE y los EE.UU., la resolución alternativa de litigios desempeña un papel crucial. Este enfoque permite que los usuarios y las organizaciones aborden y resuelvan disputas de manera eficiente, sin recurrir a los costosos y a menudo prolongados procesos judiciales. En el marco del nuevo Acuerdo, las organizaciones tienen la responsabilidad de proporcionar a los usuarios el acceso a estos mecanismos sin coste alguno. Esto significa que si un usuario de la UE tiene una queja sobre cómo una organización certificada bajo el DPF UE-EE.UU. está manejando sus datos personales, tiene derecho a utilizar uno de estos mecanismos para resolver la disputa. Ello puede implicar mediación, en la que un tercero neutral ayudará a las partes a entender el punto de vista de la otra y a explorar posibles soluciones; o puede implicar arbitraje, donde las partes presentan sus argumentos y pruebas a un árbitro o panel de árbitros que tomarán una decisión vinculante o no vinculante. En el contexto del Metaverso, el papel de los métodos alternativos de resolución de controversias es especialmente importante. Dado que el Metaverso es un universo digital en constante expansión con una gran cantidad de intercambio de datos, las futuras disputas sobre la gestión de los datos personales son más que probables. Aquí, estos métodos proporcionar una vía rápida y eficiente para la resolución de disputas, lo cual es crucial en un entorno digital donde las expectativas de los usuarios para una resolución rápida son altas. Por último, es importante destacar que, independientemente del mecanismo elegido, el hecho de que las organizaciones deben proporcionar una respuesta a las reclamaciones de los usuarios dentro de los 45 días desde la recepción de la reclamación. Esta eficiencia temporal contribuye a mantener la confianza de los usuarios en las organizaciones que operan en el Metaverso, y refuerza la integridad de este universo digital.

[128] El Anexo I del Acuerdo, titulado "Modelo Arbitral", establece los procedimientos y condiciones para el arbitraje de reclamaciones relacionadas con datos cubiertos por el Marco de Protección de Datos UE-EE.UU. Se proporciona como un medio rápido, independiente y justo para resolver las reclamaciones por violación de los Principios del DPF que no se han resuelto por otros mecanismos. El alcance del arbitraje está limitado a determinar si una organización ha incumplido sus obligaciones en virtud de los Principios en relación con una persona, y si tal incumplimiento persiste total o parcialmente sin resolver. El arbitraje no se aplica a las excepciones a los Principios o a una afirmación sobre la adecuación del DPF. El Panel del Marco de Privacidad de Datos UE-EE.UU., compuesto por uno o tres árbitros, está facultado para resolver de forma equitativa cuestiones no monetarias y específicas para cada persona (como acceso, corrección, eliminación o devolución de los datos personales) con el objetivo de evitar la posible violación de los Principios. Antes de solicitar el arbitraje, una persona debe seguir ciertos pasos, como plantear la infracción a la organización, utilizar el mecanismo de recurso independiente previsto en los Principios, y plantear la cuestión al Departamento a través del APD. Las decisiones del arbitraje son vinculantes y, una vez invocado, el individuo renuncia a la opción de solicitar reparación por la misma infracción alegada en otro foro, a menos que no se haya invocado la opción de arbitraje. Las partes pueden solicitar la revisión judicial y la ejecución de las decisiones arbitrales de acuerdo con la ley de EE.UU., bajo la Ley Federal de Arbitraje. Sin embargo, las decisiones no pretenden funcionar como precedentes vinculantes para otras partes. El panel de arbitraje será seleccionado a partir de una lista de árbitros preparada por el Departamento y la Comisión, elegidos por su independencia, integridad y experiencia. El Anexo proporciona también detalles sobre los procedimientos de arbitraje, que incluyen cómo un individuo puede iniciar un arbitraje, cómo garantizar que no se reciben remedios o procedimientos duplicados, la acción paralela de la FTC, la no participación de ciertas autoridades en los arbitrajes, y el lugar y la forma de participación en el arbitraje.

fundamental que los usuarios del Metaverso estén al tanto de sus derechos y de las vías de reparación disponibles. Asegurar el cumplimiento de estos principios en el Metaverso no sólo requiere la existencia de estos mecanismos, sino también una concienciación constante y un compromiso por parte de las organizaciones para cumplir con los principios de privacidad y protección de datos en este nuevo entorno digital.

72. La Comisión Europea ha profundizado en la evaluación de las limitaciones, salvaguardias, supervisión y los recursos individuales disponibles en la legislación estadounidense con respecto a la recolección y uso posterior de datos personales transferidos a controladores y procesadores en los EE.UU. por autoridades públicas para intereses públicos, particularmente para fines de aplicación de Derecho Penal y seguridad nacional. En este análisis, se han establecido criterios claves que incluyen, en primer lugar, que cualquier limitación al derecho a la protección de datos personales debe estar estipulada por la ley y, en segundo lugar, que estas leyes deben proporcionar garantías mínimas para que las personas cuyos datos han sido transferidos tengan la capacidad de proteger eficazmente sus datos personales contra el riesgo de abuso. En particular, se debe permitir a las personas la oportunidad de tomar acciones legales ante un tribunal independiente e imparcial para acceder a sus datos personales u obtener su rectificación o eliminación. Aplicando estos principios al marco del Metaverso, se puede inferir que las mismas reglas se aplicarían a los datos personales recopilados y utilizados dentro de estos espacios virtuales. Esto significa que las autoridades públicas de los EE.UU. sólo pueden acceder y utilizar estos datos si cumplen con los criterios y salvaguardias previamente mencionados. En términos concretos, las autoridades estadounidenses pueden acceder a los datos personales procesados por organizaciones certificadas de los EE. UU. que se transfieran desde la Unión para fines de aplicación de Derecho Penal, siguiendo los procedimientos establecidos. Estos procedimientos incluyen la emisión de una orden de registro o incautación por parte de un juez basada en una "causa probable", la emisión de citaciones por un gran jurado en el contexto de investigaciones de ciertos delitos graves, y varias bases jurídicas que permiten el acceso a los datos de las comunicaciones. Estos procedimientos también aplicarían al acceso y uso de datos personales dentro del Metaverso, dada la naturaleza interactiva y transaccional de estas plataformas virtuales. Por lo tanto, los operadores del Metaverso basados en los EE.UU. deben adherirse a estas mismas reglas y procedimientos al manejar los datos personales de los usuarios. Asimismo, la Comisión Europea también ha señalado que el Departamento de Justicia de los EE.UU. ha proporcionado garantías sobre las limitaciones y salvaguardias aplicables, las cuales son detalladas en el Anexo VI de la Decisión[129]. Entendemos que estas garantías también serían aplicables en el contexto del Metaverso, proporcionando una capa adicional de protección para los usuarios y sus datos personales dentro de estos espacios digitales.

73. Cuando una empresa tecnológica opere en un escenario real o virtual como el Metaverso y comparta información personal con entidades no gubernamentales, se deben considerar varios factores. Éstos incluyen las obligaciones legales y regulatorias, los riesgos asociados con el intercambio de información y la necesidad de una evaluación de privacidad exhaustiva. Si se comparte información con una entidad extranjera, se deben adoptar salvaguardas adicionales para garantizar la privacidad de los datos y el cumplimiento de los requisitos de privacidad. Cuando el FBI opera en un entorno virtual, debe

[129] El Anexo VI se centra en describir las restricciones legales y regulativas existentes en los EE.UU. con respecto al acceso a los datos por parte de las autoridades gubernamentales y civiles o reguladoras. Una disposición clave subraya que, si una entidad está bajo una obligación legal y posee una orden judicial, tiene derecho a disputar cualquier requisito de revelación de información que considere excesivamente gravoso. En complemento a estas limitaciones legales, el Fiscal General ha emitido directrices adicionales que establecen más restricciones al acceso de las fuerzas del orden a los datos. Una de estas directrices relevantes es la Directriz del Fiscal General para las Operaciones Nacionales del FBI, que insta al uso de los métodos de investigación menos invasivos y hace hincapié en la protección de la privacidad, las libertades civiles y la reputación de los individuos. El Anexo VI también documenta restricciones significativas al acceso a datos por parte de las autoridades civiles y reguladoras. Estas entidades pueden requerir registros empresariales, pero su autoridad se ve limitada por sus estatutos fundacionales y la revisión judicial independiente previa a cualquier acción legal. Además, las empresas tienen la posibilidad de impugnar las solicitudes de datos basándose en leyes sectoriales específicas y el tipo de datos que manejan. Por último, se señala que cualquier potestad que las agencias administrativas tengan para confiscar registros físicos de una empresa debe cumplir con los requisitos establecidos en la Cuarta Enmienda.

seguir las mismas reglas que en el mundo real, incluyendo las pautas establecidas en las Directrices del Fiscal General para las operaciones nacionales del FBI (AGG-DOM) y en la Guía de Operaciones e Investigaciones del FBI (DIOG). Toda información recogida, ya sea en un contexto penal o civil, puede ser utilizada para fines regulatorios si se recoge legalmente y es relevante para dichas funciones. De manera similar, cualquier información recolectada puede ser utilizada en otra investigación del FBI, siempre y cuando esté legalmente permitido[130].

74. El Congreso de los EE.UU. tiene la facultad de realizar investigaciones centradas en empresas americanas que operan en el Metaverso, al igual que en el mundo físico. A través de citaciones, puede obtener testimonios y documentos, y recibir informes regulares de los organismos de supervisión de la aplicación de la Ley. Asimismo, tiene acceso a las evaluaciones de impacto de la protección de datos personales llevadas a cabo por las agencias en virtud de la Circular OMB nº A-130[131]. Con esta información, puede supervisar y tomar medidas legislativas para corregir problemas identificados. Este marco de supervisión se aplica tanto en el mundo real como en el Metaverso, y asegura que las autoridades estén sujetas a un escrutinio independiente y eficaz. Asimismo, los usuarios tienen la opción de interponer recursos judiciales y administrativos si se violan sus derechos de privacidad y protección de datos personales.

75. La legislación de los EE.UU. establece restricciones y salvaguardas con respecto al acceso y uso de datos personales en el Metaverso para la seguridad nacional. Estas restricciones están respaldadas por mecanismos de supervisión y apelación que cumplen con los requisitos establecidos en la cláusula 89 de la Decisión[132]. De modo que los datos personales transferidos desde la Unión a las organizaciones DPF UE-EE.UU. en el Metaverso pueden ser recogidos por las autoridades estadounidenses con fines de seguridad nacional sobre la base de diferentes instrumentos jurídicos, sujetos a condiciones y salvaguardas específicas.

---

[130] Para mayor información acerca de este tipo de procedimientos y las cuestiones éticas que generan véase, *inter alia,* el enfrentamiento entre Apple y el FBI en 2016, relacionado con el caso del tiroteo de San Bernardino perpetrado por Syed Rizwan Farook y su esposa. El FBI solicitó a Apple su colaboración para desbloquear el iPhone de Farook y poder acceder a su contenido, en aras de profundizar su investigación del atentado. Sin embargo, Apple se opuso firmemente a esta petición, argumentando que tal acción podría vulnerar la privacidad de sus usuarios y contradecir los valores democráticos que la empresa defiende. Su principal preocupación radicaba en la creación de un "backdoor" o "puerta trasera", un método alternativo de acceso a un iPhone sin necesidad de contraseña. Según Apple, si este software llegara a caer en manos erróneas, podría ser utilizado para desbloquear cualquier iPhone, no solo el de Farook. La propuesta del FBI consistía en que Apple modificara el System Information File (SIF), que es el software utilizado en los dispositivos de Apple, creando uno nuevo específicamente para el iPhone de Farook. Este nuevo software permitiría introducir un número ilimitado de contraseñas para intentar desbloquear el smartphone. Este enfrentamiento, que se considera un hito en la delimitación entre la protección de datos y la seguridad nacional, recibió diversos puntos de vista. Figuras como Edward Snowden y Sundar Pichai, CEO de Google, expresaron su apoyo a Apple, destacando la importancia de la privacidad del usuario. Por el contrario, personalidades como el entonces candidato a la Presidencia de EE.UU., Donald Trump, criticaron la postura de Apple. En la actualidad (2023), el caso podría seguir escalando a instancias judiciales superiores, incluso hasta el Tribunal Supremo de EE.UU. Se espera que Apple mantenga su oposición frente a la orden judicial. La resolución de este conflicto podría sentar un precedente importante en relación a la privacidad del usuario y la seguridad nacional.

[131] Circular OMB A-130, Gestión de la información como recurso estratégico. Texto íntegro disponible en: https://www.whitehouse.gov/omb/information-for-agencies/circulars/

[132] Decisión de ejecución de la Comisión de 10 de julio de 2023 de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo al nivel adecuado de protección de los datos personales en el marco de privacidad de datos entre la UE y los EE.UU. (89) En particular, toda limitación al derecho a la protección de datos personales debe estar prevista por la ley o normativa y la base jurídica que permite la injerencia en tal derecho debe definir por sí misma el alcance de la limitación al ejercicio del derecho de que se trate. Además, para cumplir el requisito de proporcionalidad, según el cual las excepciones y limitaciones a la protección de datos personales sólo deben aplicarse en la medida estrictamente necesaria en una sociedad democrática para alcanzar objetivos específicos de interés general equivalentes a los reconocidos por la Unión, dicha base jurídica debe establecer normas claras y precisas que regulen el alcance y la aplicación de las medidas en cuestión e imponer garantías mínimas para que las personas cuyos datos hayan sido transferidos dispongan de garantías suficientes para proteger eficazmente sus datos personales contra el riesgo de abuso. Además, estas normas y garantías deben ser jurídicamente vinculantes y exigibles por los particulares. En particular, los interesados deben tener la posibilidad de emprender acciones legales ante un tribunal independiente e imparcial para acceder a sus datos personales u obtener la rectificación o supresión de los mismos.

76. La Orden Ejecutiva (OE) 14086[133] impone una serie de requisitos para las actividades de inteligencia de señales en EE.UU., estipulando que deben estar basadas en la ley o en autorización presidencial y deben cumplir con la legislación estadounidense. Esta regulación establece la necesidad de un equilibrio entre las necesidades de seguridad nacional y la privacidad y las libertades civiles de los individuos. Para garantizar este equilibrio, estas actividades están sujetas a supervisión. Además, la OE 14086 limita las razones por las cuales se pueden recoger datos personales. Los datos sólo pueden recopilarse para promover una prioridad de inteligencia específica y deben ser proporcionales a dicho propósito. Estas líneas de trabajo son desarrolladas por el Director de Inteligencia Nacional y aprobadas por el Presidente. Una vez establecida la prioridad, hay requisitos adicionales para decidir si la acción concreta está justificada. En primer lugar, la información sólo puede recogerse si es necesaria para avanzar en una prioridad de inteligencia específica. Si se considera necesaria, la recopilación debe ser lo más limitada posible y no debe afectar de manera desproporcionada a la privacidad ni a las libertades civiles. La OE 14086 también establece que la recogida de datos dentro de los EE.UU. debe ser siempre selectiva. La recogida masiva sólo puede llevarse a cabo fuera de EE.UU., y sólo cuando la información necesaria no puede obtenerse razonablemente mediante la recogida selectiva. La recopilación de datos transferidos a una organización estadounidense también está sujeta a limitaciones y salvaguardas específicas bajo la Sección 702 de la FISA[134]. Un tribunal independiente (FISC) supervisa estas operaciones de recogida de datos y puede apelar decisiones ante el Tribunal de Revisión de la Vigilancia de Inteligencia Extranjera (FISCR) y, en última instancia, ante el Tribunal Supremo de los EE.UU. En relación con el Metaverso, es crucial tener en cuenta que estos mundos virtuales, que pueden incluir tecnologías de realidad virtual (VR)[135], realidad aumentada (AR)[136], e Internet, puede involucrar la recopilación y el uso de grandes cantidades de datos personales[137]. Estos datos pueden ser de gran valor para las actividades de seguridad nacional, pero también plantean preocupaciones significativas de privacidad. Por lo tanto, la OE 14086 y las regulaciones similares pueden tener implicaciones significativas para el Metaverso. Por un lado, pueden limitar la recopilación y el uso de datos personales en el Metaverso con fines de seguridad nacional. Por otro lado, pueden proporcionar salvaguardas para proteger la privacidad y las libertades civiles de los usuarios del Metaverso[138]. De este modo, aunque las reglamentaciones como la OE 14086 pueden representar ciertos desafíos para las operaciones de seguridad nacional, también pueden ayudar a garantizar que el Metaverso se desarrolle de una manera que respete la privacidad y las libertades civiles, alineándose así con los valores democráticos y los derechos humanos.

77. El tratamiento de los datos personales obtenidos por las agencias de inteligencia estadounidenses se rige por un conjunto de rigurosas y exhaustivas salvaguardias. Entre estas se encuentra la obligación de proporcionar una sólida seguridad para los datos recolectados, lo que se logra mediante

[133] Mejora de las salvaguardias para las actividades de inteligencia de los EE.UU. Documento presidencial de la Oficina Ejecutiva del Presidente de 14 de octubre de 2022. Orden Ejecutiva (OE) 14086. Texto íntegro disponible en: https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities

[134] La Ley de Vigilancia de Inteligencia Extranjera (FISA, por sus siglas en inglés), promulgada en 1978, regula las actividades de vigilancia de inteligencia extranjera y establece procedimientos para la recolección de dicha información, creando además el Tribunal de Vigilancia de Inteligencia Extranjera (FISC) para supervisar este proceso. En 2008, se introdujo la Sección 702, que autoriza la recopilación de inteligencia enfocada en ciertos tipos de información extranjera, como datos relacionados con el terrorismo internacional. Esta sección permite la recolección de datos de individuos no estadounidenses que se encuentren razonablemente fuera de los EE.UU., pero también prevé procedimientos para minimizar la retención e intercambio de información relacionada con ciudadanos estadounidenses. No obstante, en situaciones en las que la seguridad nacional está en juego, se permite compartir información relevante, y se han introducido medidas adicionales para garantizar que cualquier consulta de la información adquirida bajo la Sección 702 cumpla con la Cuarta Enmienda. Texto íntegro disponible en: https://www.fbi.gov/investigate/how-we-investigate/intelligence/foreign-intelligence-surveillance-act-fisa-and-section-702

[135] J. Dionisio, W. Burns Iii, R. Gilbert, "3D virtual worlds and the metaverse: current status and future possibilities", *ACM Computing Surveys*, vol. 45, nº 3, 2013. [En línea] Disponible en: https://doi.org/10.1145/2480741.2480751

[136] P. A. Rauschnabel, R. Felix, C. Hinsch, H. Shahab, F. Alt, "What is XR? Towards a framework for augmented and virtual reality", *Computers in Human Behavior*, vol. 133, 2022. [En línea] Disponible en: https://doi.org/10.1016/j.chb.2022.107289

[137] E. Dincelli, A. Yayla, "Immersive virtual reality in the age of the metaverse: a hybrid-narrative review based on the technology affordance perspective", *The Journal of Strategic Information Systems*, vol. 31, nº 2, 2022, p. 101717. [En línea] Disponible en: https://doi.org/10.1016/j.jsis.2022.101717

[138] F. Bignami, "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining", *Boston College Law Review*, vol. 48, 2007, p. 609.

la implementación de medidas como la autenticación multifactorial, el cifrado y la restricción de acceso solamente al personal autorizado y capacitado. Además, estas agencias deben adscribirse a los estándares de la Comunidad de Inteligencia para asegurar la precisión y objetividad de los datos, considerando la posibilidad de fuentes de información alternativas y manteniendo la imparcialidad en su análisis. Otra de las salvaguardias concierne a los períodos de conservación de datos. De acuerdo con la Orden Ejecutiva 14086, se estipula que los datos personales de los individuos no estadounidenses deben ser conservados por los mismos períodos que los datos de los ciudadanos estadounidenses. Paralelamente, la difusión de los datos recogidos está regida por normativas específicas y rigurosas, permitiéndose únicamente cuando se cumplen una serie de requisitos exigentes[139]. Además, para garantizar una supervisión efectiva, las agencias de inteligencia están obligadas a mantener una adecuada documentación sobre la recopilación de información, lo que proporciona una trazabilidad y transparencia en sus operaciones. Las salvaguardias previamente mencionadas se ven reforzadas por requisitos más amplios de protección y manejo de datos personales, que se originan en regulaciones como la Circular A-130 de la Oficina de Administración y Presupuesto (OMB), la Ley de Administración Electrónica[140], la Ley Federal de Registros[141] y las directrices del Comité de Sistemas de Seguridad Nacional (CNSS)[142]. La labor de las agencias de inteligencia está sujeta a la supervisión de diversas entidades, tanto internas como externas. Entre las internas se encuentran los funcionarios encargados de la intimidad y las libertades civiles dispersos en diversos departamentos con responsabilidades en materia de aplicación del Derecho Penal[143], los Inspectores Generales de cada servicio[144], la Junta Asesora de Inteligencia del Presidente (PIAB)[145] y la Junta

[139] *The Attorney General's Guidelines for Domestic FBI Operations* (AGG-DOM), Sección VI, B y C; FBI *Domestic Investigations and Operations Guide* (DIOG) del FBI. En cuanto a los fundamentos para la difusión de información, tanto la AGG-DOM como la DIOG del FBI establecen diversas circunstancias en las que el FBI puede estar legalmente obligado a divulgar información, como puede ser el caso de un acuerdo internacional. Además, el FBI está autorizado a compartir información con otras agencias de EE.UU., siempre que la divulgación esté alineada con los fines para los que se recopiló la información y esté en relación con las responsabilidades de estas agencias. Asimismo, el FBI puede compartir información con comités del Congreso y con agencias extranjeras, siempre que la información esté relacionada con sus responsabilidades y que la divulgación sea compatible con los intereses de EE.UU. Por otro lado, la divulgación también puede ser necesaria en situaciones de especial importancia, como proteger la seguridad de personas o bienes, prevenir un delito o una amenaza para la seguridad nacional, siempre y cuando dicha divulgación esté alineada con el fin para el que se recopiló la información.

[140] La Ley de Administración Electrónica de 2002 (*E-Governement Act of 2002*) trata de mejorar la gestión de los registros electrónicos del Gobierno federal de EE. UU., incluyendo el establecimiento de estándares para la creación, manejo y disposición de registros electrónicos. El texto íntegro se encuentra disponible en: https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

[141] Gestión de registros por agencias federales (44 USC Capítulo 31). Texto íntegro disponible en: https://www.archives.gov/about/laws/fed-agencies.html

[142] El Comité de Sistemas de Seguridad Nacional (CNSS) establece políticas, directivas, instrucciones, procedimientos operativos, guías y avisos de seguridad cibernética a nivel nacional para los departamentos y agencias del Gobierno de los EE.UU. para la seguridad de los sistemas de seguridad nacional. Proporciona un foro integral para la planificación estratégica y la toma de decisiones operativas para proteger NSS y aprueba la publicación de productos e información de INFOSEC a gobiernos extranjeros.

[143] Los funcionarios designados para la privacidad y las libertades civiles se encuentran ubicados en varios departamentos. Aunque el alcance específico de las responsabilidades de estos funcionarios puede variar dependiendo de la normativa que les autoriza, generalmente supervisan los procesos para asegurar que el departamento o entidad correspondiente tenga en cuenta las preocupaciones de privacidad y libertades civiles y haya establecido los procedimientos adecuados para atender las quejas de personas que creen que se han violado su privacidad o libertades civiles. Los líderes o jefes de cada departamento o entidad deben asegurar que los encargados de la privacidad y las libertades civiles tengan los recursos y materiales necesarios para cumplir su mandato, y que tengan acceso a todo el material y personal necesario para desempeñar sus funciones, además de ser informados y consultados sobre los cambios de política propuestos. Estos responsables deben informar regularmente al Congreso, en particular sobre el número y tipo de quejas recibidas y un resumen de cómo se resolvieron, las revisiones e investigaciones realizadas y el impacto de sus actividades.

[144] El Inspector General independiente supervisa las actividades del Departamento de Justicia, incluyendo el FBI. Los Inspectores Generales, que son independientes por estatuto, son responsables de llevar a cabo investigaciones, auditorías e inspecciones independientes de los programas y operaciones del Departamento. Tienen acceso a todos los registros, informes, auditorías, revisiones, documentos, recomendaciones u otros materiales relevantes, incluso mediante citación si es necesario, y pueden tomar declaraciones. Aunque las recomendaciones de los Inspectores Generales para adoptar medidas correctivas no son vinculantes, sus informes, incluidos los que se refieren a las medidas de seguimiento (o a la falta de las mismas) suelen hacerse públicos y enviarse al Congreso, que puede ejercer su función de supervisión basándose en esta información.

[145] El *Intelligence Oversight Board* (IOB), establecido en el marco del *President's Intelligence Advisory Board* (PIAB), tiene

de Supervisión de la Privacidad y las Libertades Civiles (PCLOB)[146]. Más allá de estos mecanismos de supervisión internos en el Poder Ejecutivo, existen instancias de supervisión externas, como los comités específicos del Congreso de EE.UU[147]. La Ley FISA añade, además, toda una serie de requisitos adicionales de información[148]. Este entramado regulatorio adquiere una relevancia crucial en el contexto del Metaverso, un escenario en el que las barreras físicas se diluyen y la información circula sin limitaciones geográficas. Dada la diversidad y el nivel de detalle de los datos que pueden recogerse en el Metaverso, es fundamental garantizar su seguridad y privacidad. Las agencias de inteligencia tienen la responsabilidad de adherirse a los mismos estándares y regulaciones al recabar y procesar datos personales en el Metaverso, asegurando la transparencia, la precisión, la seguridad y la protección de los derechos ciudadanos. Pese a ello, el marco legal actual ha suscitado críticas y debates en lo que respecta a la protección de la privacidad y los derechos civiles, en particular en relación con la vigilancia de ciudadanos estadounidenses y la transparencia de las actividades de la FISC. A medida que el Metaverso continúa desarrollándose, estos debates seguirán siendo de gran relevancia y necesarios para garantizar una adecuada protección de los derechos de los ciudadanos en este novedoso entorno digital.

78. El Acuerdo UE-EE.UU. contempla una vía específica de reparación para aquellos usuarios de la UE que deseen emprender acciones legales ante un tribunal independiente e imparcial con poderes vinculantes[149]. El interesado en cuestión deberá plantear una reclamación ante una APD competente en un Estado miembro de la UE, proporcionando un acceso fácil y en el idioma nativo del individuo. Una vez verificados los requisitos de admisibilidad, la queja o recurso se canaliza al mecanismo de resolu-

como responsabilidad supervisar el cumplimiento de la Constitución y todas las normas aplicables por parte de las autoridades de inteligencia de EE.UU. El PIAB, que funciona como un órgano consultivo de la Oficina Ejecutiva del Presidente, consta de 16 miembros que son nombrados por el Presidente y provienen de fuera del Gobierno estadounidense. El IOB está compuesto por hasta cinco miembros, los cuales son designados por el Presidente de entre los miembros del PIAB. Según la Orden Ejecutiva 12333, los líderes de todas las agencias de inteligencia están obligados a informar al IOB sobre cualquier actividad de inteligencia que se tenga razones para creer que pueda ser ilegal o que contradiga una Orden Ejecutiva o Directiva Presidencial.

[146] Los integrantes de la Junta de Supervisión de la Privacidad y las Libertades Civiles (PCLOB) deben ser elegidos únicamente basándose en sus habilidades profesionales, logros alcanzados, prestigio público, conocimientos en el ámbito de las libertades civiles y la privacidad, así como su experiencia pertinente, sin considerar su filiación política. En ningún momento el Consejo puede contar con más de tres miembros que sean afiliados al mismo partido político. Aquellos designados como miembros del Consejo no pueden ocupar cargos electos, ni ser funcionarios o empleados del Gobierno Federal mientras estén en el Consejo, excepto en su papel como miembros del mismo.

[147] Los comités específicos del Congreso de EE.UU., como el Comité de Inteligencia del Senado y el Comité de Inteligencia de la Cámara de Representantes, llevan a cabo la supervisión periódica de diferentes maneras, en particular, mediante audiencias, investigaciones, revisiones e informes. Además, también se realizan audiencias de supervisión periódicas dirigidas a entidades como el FBI y el Departamento de Justicia (DoJ).

[148] La Ley de Vigilancia de Inteligencia Extranjera de 1978 (FISA). Texto íntegro disponible en: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286#:~:text=FISA%20prohibits%20surveillance%20of%20or,50%20U.S.C.

[149] Se instaura un mecanismo de recurso específico según la Orden Ejecutiva (OE) 14086, que se complementa con el Reglamento del Fiscal General que crea el Tribunal de Revisión de la Protección de Datos. Este mecanismo se encarga de gestionar y resolver las quejas individuales relacionadas con las actividades de inteligencia de señales de los EE.UU. Cualquier ciudadano de la UE puede presentar una queja a través de este mecanismo si considera que se ha producido una supuesta violación de la legislación estadounidense que regula dichas actividades (como la OE 14086, la Sección 702 de la FISA, la OE 12333) y que esta violación ha afectado de manera negativa a sus intereses de privacidad y libertades civiles. Este mecanismo de recurso está disponible para individuos de países u organizaciones regionales de integración económica que el Fiscal General de EE.UU. haya designado como "Estados cualificados". El 30 de junio de 2023, la UE y los tres países de la Asociación Europea de Libre Comercio que, juntos, conforman el Espacio Económico Europeo, fueron designados por el Fiscal General, según la Sección 3(f) de la OE 14086, como "Estado cualificado". Esta designación se realiza sin perjuicio del artículo 4(2) del TUE. Los funcionarios de privacidad y libertades civiles están situados en diversos departamentos y su papel es fundamental para salvaguardar estos aspectos. Sus responsabilidades, aunque pueden variar en función de la legislación que los autoriza, suelen implicar la supervisión de procedimientos para garantizar que el departamento o entidad correspondiente atienda adecuadamente las inquietudes sobre privacidad y libertades civiles, y responda a las quejas de individuos que consideren que se han vulnerado dichos derechos. Las autoridades de cada departamento deben garantizar que estos funcionarios cuenten con los recursos y materiales necesarios para cumplir con sus tareas, y que dispongan del acceso a todo el personal y material requerido para desempeñar sus funciones. Además, deben ser notificados y consultados sobre los cambios propuestos en las políticas. Estos encargados tienen la responsabilidad de informar regularmente al Congreso, proporcionando datos sobre el número y la naturaleza de las quejas recibidas, cómo se han resuelto éstas, las investigaciones realizadas y el impacto de sus actividades.

ción a través de la Secretaría del Consejo Europeo de Protección de Datos. La Oficina del Asesor de Libertades Civiles y Privacidad (CLPO) de la Oficina del Director de Inteligencia Nacional (ODNI)[150] es la encargada de realizar la investigación inicial. En el contexto del Metaverso, la CLPO del ODNI puede solicitar la cooperación de las agencias de inteligencia para acceder a la información necesaria, garantizando así un examen completo y sin interferencias. Como parte de su revisión, la CLPO determina si se ha violado la normativa pertinente y decide la reparación adecuada, que puede incluir medidas como el cese de la recopilación ilegal de datos en el Metaverso, la eliminación de los datos obtenidos ilícitamente, la limitación del acceso a los datos recogidos legalmente sólo al personal debidamente capacitado o la retirada de informes de inteligencia que contienen datos adquiridos sin autorización legal. Si el demandante no está de acuerdo con las decisiones de la CLPO, tiene derecho a apelar al Tribunal de Revisión de la Protección de Datos (DPRC)[151], un tribunal independiente compuesto por al menos seis jueces nombrados por el Fiscal General. Este tribunal revisa las decisiones de la CLPO y tiene la responsabilidad de garantizar la protección de la privacidad y las libertades civiles, aspectos críticos en un entorno digital y colaborativo como el Metaverso. Finalmente, el DPRC puede determinar que no hay evidencias de que se hayan llevado a cabo actividades de inteligencia de señales relacionadas con los datos personales del demandante, ratificar las decisiones de la CLPO o, en caso de desacuerdo, emitir sus propios fallos. Este mecanismo de resolución destaca la importancia de un entorno digital seguro y la protección de datos en la era del Metaverso, estableciendo procesos claros y accesibles para la resolución de quejas y violaciones de la privacidad y las libertades civiles.

79. El DPRC se encarga de emitir decisiones escritas, por mayoría de votos, en caso de que se detecte una violación a las normas de protección de datos. Las medidas correctivas pueden incluir desde la eliminación de datos recolectados de forma ilegal, hasta la supresión de resultados de consultas inadecuadas o la limitación del acceso a datos recolectados legalmente. La decisión del DPRC es definitiva y vinculante, y puede llevar a acciones coercitivas adicionales, si el FISC lo considera necesario. Por ejemplo, si una empresa o individuo recopila ilegalmente datos personales dentro del Metaverso, el DPRC podría emitir una decisión que requiere la eliminación de dichos datos, restringir el acceso a los mismos, o incluso retirar informes de inteligencia generados a partir de esta información recolectada de manera no autorizada. La Oficina de Privacidad y Libertades Civiles del DoJ se encarga de mantener un registro de todas las revisiones realizadas por el DPRC y todas las decisiones emitidas. Este registro sirve como un precedente no vinculante para futuros casos. Además, se mantiene un registro de cada denunciante, y para aumentar la transparencia, se verifica periódicamente si la información relativa a una revisión del DPRC ha sido desclasificada y, de ser así, se notifica a la persona correspondiente. En términos de supervisión, el funcionamiento del mecanismo de recurso está sujeto a una revisión anual por parte de la PCLOB. Esta entidad independiente evalúa, *inter alia*, si las reclamaciones han sido

[150] La Oficina del Director de Inteligencia Nacional (ODNI) es una entidad del Gobierno de los EE.UU., establecida en respuesta a los eventos del 11 de septiembre de 2001. Fue creada bajo la Presidencia de George W. Bush mediante la Orden Ejecutiva 13354 y fue fortalecida por el Congreso de los EE.UU. con la aprobación de la Ley de Reforma de Inteligencia y Prevención del Terrorismo (IRTPA) de 2004. Estas reformas tenían como objetivo principal mejorar la inteligencia relacionada con el terrorismo y optimizar su gestión en todo el país. La misión de la ODNI es liderar el esfuerzo nacional para proteger a los EE.UU. del terrorismo. Esto se logra a través de la integración, el análisis y el intercambio de información que impulsa la acción de todo el Gobierno y logra los objetivos nacionales en la lucha contra el terrorismo. La visión de la ODNI es ser la fuente indispensable de experiencia en la lucha contra el terrorismo en un entorno de amenazas en constante evolución. Busca liderar una empresa de lucha contra el terrorismo unificada, ágil y resistente. Los valores de la ODNI incluyen la excelencia en la ejecución de sus responsabilidades, la integridad en todas sus operaciones, la diversidad de pensamiento y enfoque, el liderazgo en la dirección de la estrategia de lucha contra el terrorismo, y el establecimiento de asociaciones sólidas con otros organismos de Gobierno y entidades relevantes.

[151] Para garantizar la integridad e imparcialidad del Tribunal de Revisión de la Protección de Datos (DPRC), se establece que los jueces sólo pueden ser destituidos por el Fiscal General por causas justificadas, las cuales pueden incluir comportamiento indebido, comisión de delitos, incumplimiento de deberes o incompetencia. Este mecanismo de resolución es especialmente pertinente en el contexto del Metaverso, un entorno compartido y colaborativo de realidad virtual. Dado el creciente uso del Metaverso y la recolección de datos a gran escala que conlleva, este proceso ofrece un recurso legal para los ciudadanos de UE que consideren que sus derechos de privacidad y libertades civiles han sido violados por las actividades de los servicios de inteligencia de EE.UU.

procesadas de manera oportuna, si se ha obtenido pleno acceso a la información necesaria y si se han respetado las salvaguardas sustantivas. El resultado de esta revisión se presenta en un informe que se hace público en una versión no clasificada, permitiendo la participación y escrutinio de la ciudadanía. Además del recurso específico establecido, todas las personas tienen acceso a los tribunales ordinarios de EE.UU., lo que abre una amplia gama de posibilidades para defender sus derechos en cuanto a la protección de datos se refiere. La implementación de estos mecanismos en el Metaverso asegurará la protección de los datos personales, garantizará la transparencia y permitirá a los usuarios del Metaverso acceder a vías de recurso efectivas en caso de violaciones de sus derechos de protección de datos. A medida que el Metaverso continúa desarrollándose y expandiéndose, será crucial que estas salvaguardas y mecanismos de responsabilidad se implementen para asegurar que el acceso y uso de datos personales esté limitado a lo que es estrictamente legal, legítimo, necesario y proporcional.

IX. El Efecto Bruselas y la *praxis* estadounidense

81. El fenómeno conocido como "Efecto Bruselas" se refiere a la influencia de la legislación comunitaria, especialmente aquella que se origina en Bruselas, la capital administrativa de la UE, en las políticas y prácticas más allá de sus fronteras. Este efecto es evidente en una variedad de áreas, destacando especialmente en la protección de datos[152]. El éxito del "Efecto Bruselas" en la esfera de protección de datos se puede atribuir a varias razones clave. En primer lugar, a la confianza y satisfacción que los consumidores europeos tienen en las normativas de la UE en materia de protección de datos. En segundo lugar, a las multas o sanciones efectivamente impuestas por las autoridades y tribunales a nivel nacional y comunitario, lo que refuerza la seriedad y el alcance de las regulaciones. Por último, también se debe a la evolución de las propias empresas, que han desarrollado una cultura de protección de datos en respuesta a estas normativas. Un claro ejemplo de esto es la acción tomada por Microsoft en respuesta a la Sentencia Schrems, que modificó su política de privacidad el mismo día que se emitió el veredicto. Este acto demuestra cómo la influencia de la regulación europea puede cambiar las prácticas de empresas globales, reflejando su verdadero alcance y poder.

82. Tras el estudio del nuevo Acuerdo UE – EE.UU., la pregunta clave sería: ¿se ha adoptado el RGPD como la política de privacidad de datos estándar en los EE.UU. de América? La respuesta a esta cuestión es un tanto compleja. Si la adopción de estándares europeos se concibe como un requisito *sine qua non* a la hora de poder establecer relaciones comerciales, entonces, indudablemente, sí. Las empresas estadounidenses que operan en territorio europeo deben cumplir con el RGPD, lo que efectivamente convierte a esta legislación en su política de privacidad de datos *de facto* en estas circunstancias. El RGPD, con sus estrictas normas y altas sanciones para aquellos casos en los que se detecten violaciones de privacidad de datos, ha establecido un estándar global de protección de datos. Esto ha forzado a muchas empresas, incluso aquellas establecidas fuera de Europa, a adaptar sus políticas y prácticas para cumplir con estas regulaciones. Como resultado, se podría decir que el RGPD ha influenciado fuertemente las políticas de privacidad de datos a nivel mundial, incluyendo los EE.UU. Y, en relación con el Metaverso, el impacto del RGPD es aún más significativo. El Metaverso, un espacio digital interconectado que está emergiendo rápidamente, plantea nuevas y desafiantes cuestiones sobre la privacidad y protección de datos. El modelo establecido por el RGPD, con su énfasis en la protección del individuo y la responsabilidad de las organizaciones, podría proporcionar una base sólida para la regulación de datos en el Metaverso. De modo que, si los EE.UU., o cualquier otro tercer Estado, decidiera establecer una normativa aplicable en los mundos virtuales contraria a los principios rectores del RGPD, debería elegir entre crear una partición de dicho espacio -no accesible desde Europa- o debería estudiarse la po-

[152] A. Bradford, *The Brussels Effect: How the European Union Rules the World*, *cit.*, 2020; debiendo hacer igualmente referencia a este mismo autor unos años antes en A. Bradford, "The Brussels Effect", *Northwestern University Law Review*, vol. 107(1), 2012.

sibilidad de que el propio usuario interesado, a sabiendas de que no se encuentra en un "espacio seguro", pudiera renunciar a sus derechos de forma expresa.

83. Esta situación nos lleva a reflexionar sobre la legitimidad y el alcance de la influencia de un tribunal europeo en la modificación del comportamiento de una empresa, independientemente de su ubicación geográfica[153]. La normativa europea no sólo tiene un impacto significativo en los residentes, ciudadanos y empresas europeas, sino que también afecta a las empresas globales, incluyendo a las estadounidenses. Este alcance transnacional de la legislación europea, aunque pueda parecer excesivo a algunos, es un reflejo de nuestra creciente interconexión global. En un mundo donde las empresas operan a través de fronteras y los datos se mueven libremente, las regulaciones de un territorio pueden y, de hecho, deben tener un impacto más allá de sus propias fronteras para ser efectivas. Este escenario plantea importantes cuestiones sobre el control y la soberanía[154] en la era digital. ¿Hasta dónde debe llegar la jurisdicción de una entidad legal sobre las empresas que operan en su territorio? ¿Cómo se equilibran los derechos de las empresas para operar libremente con la necesidad de proteger la privacidad y los derechos de los ciudadanos? La relación con el Metaverso es particularmente relevante aquí. En el Metaverso, un espacio digital global interconectado, estas preguntas adquieren una nueva dimensión. ¿Quién tiene la autoridad para regular en este espacio? ¿Cómo se aplica la jurisdicción en un mundo sin fronteras físicas? Es probable que las respuestas a estas preguntas se basen, al menos en parte, en las lecciones aprendidas de las actuales normativas de protección de datos como el RGPD. En este sentido, apriorísticamente, todo parece apuntar a que el Metaverso nace modelado por las regulaciones y normativas comunitarias en materia de protección de datos personales.

84. El éxito de las relaciones comerciales entre la UE y los EE.UU. ha permitido la transferencia efectiva de principios legales, los cuales se han materializado en siete pilares fundamentales en el nuevo Acuerdo UE-EE.UU[155]. El primero es el principio de notificación[156], que garantiza a las personas claridad y transparencia sobre el manejo de sus datos personales, resaltando el énfasis del RGPD en proteger los derechos de los ciudadanos. En segundo lugar, el principio de elección[157] da a los individuos el poder de controlar si su información personal puede ser compartida con terceros o utilizada para fines distintos a los que se recogió originalmente, mostrando cómo la influencia jurídica de la UE, gracias a su fuerte posición de mercado, ha permitido una amplia difusión de sus regulaciones. El tercer principio, responsabilidad por transferencias[158], refleja cómo esta influencia ha fomentado la adopción de normas de protección de datos que se reconocen y aplican más allá de las fronteras de la UE. Este principio sostiene que las organizaciones son responsables de la seguridad de la información transferida a terceros. El cuarto principio, seguridad[159], se alinea con los acuerdos transfronterizos que permiten la transferencia segura de datos entre países, siempre respetando los derechos de los ciudadanos. Este principio exige la implementación de medidas de seguridad adecuadas para proteger la información personal. El quinto principio, integridad y limitación de la finalidad[160], es similar a los acuerdos de adecuación que

[153] Véanse M. Brkan, "Data Protection and European Private International Law: Observing a Bull in a China Shop", *International Data Privacy Law*, vol. 5, nº 4, 2015, p. 257. M. Brkan, "The Unstoppable Expansion of EU Fundamental Right to Data Protection: Little Shop of Horrors?", *Maastricht Journal of European and Comparative Law*, vol. 23, nº 5, 2016, p. 812. M. Brkan, "The Court of Justice of the EU, Privacy and Data Protection: Judge-Made Law as a Leitmotif in Fundamental Rights Protection", en M. BRKAN, E. PSYCHOGIOPOULOU (eds.), Courts, *Privacy and Data Protection in the Digital Environment*, Edward Elgar Publishing, 2017. M. Brkan, "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way through the Maze of the CJEU's Constitutional Reasoning", *German Law Journal,* vol. 20, nº 6, 2019, p. 864.

[154] S. Besson, "Sovereignty", en *Max Planck Encyclopedia of Public International Law*, última actualización: abril 2011. [En línea] Oxford University Press.

[155] G. Buttarelli, "The EU GDPR as a Clarion Call for a New Global Digital Gold Standard", *International Data Privacy Law*, vol. 6, nº 2, 2016, p. 77.

[156] RGPD. Artículo 12. Transparencia de la información, la comunicación y las modalidades de ejercicio de los derechos del interesado.

[157] RGPD. Artículo 7. Condiciones para el consentimiento.

[158] RGPD. Artículo 44. Principio general para las transferencias.

[159] RGPD. Artículo 32. Seguridad del tratamiento.

[160] RGPD. Artículo 5. Principios relativos al tratamiento de datos personales.

reconocen y respetan protecciones de privacidad de datos equivalentes en diferentes jurisdicciones. Las organizaciones deben asegurarse de que la información personal sea relevante, precisa y limitada al propósito para el cual se recogió. En sexto lugar, el principio de acceso[161] asegura que los individuos puedan acceder, corregir, modificar o eliminar su información personal si es inexacta o se procesa en contra de los principios, de manera similar a los "puertos seguros" que garantizan un nivel adecuado de protección de datos en las transferencias internacionales de datos. Finalmente, el séptimo principio, cumplimiento y responsabilidad[162], obliga a las organizaciones a establecer mecanismos para garantizar el cumplimiento de estos principios y a investigar y resolver quejas sobre el tratamiento de datos personales. Este principio demuestra que, aunque la normativa de protección de datos pueda variar entre los EE.UU. y la UE, se espera que las organizaciones escojan la mayor protección posible.

85. En los últimos años, la incertidumbre jurídica derivada de la ausencia de un acuerdo definitivo entre las autoridades europeas y estadounidenses ha generado un impacto significativo en la conducta de las empresas norteamericanas. Este escenario ha propiciado la adopción de innovadoras estrategias por parte de estas compañías para adecuarse a las circunstancias. Twitter, como una ilustración precisa de este fenómeno, ha reubicado su base de operaciones central en Irlanda. Esta decisión se puede interpretar como una iniciativa para alinear sus operaciones con las regulaciones de la UE en materia de privacidad y protección de datos. El traslado refleja un esfuerzo de las compañías por buscar la seguridad jurídica en un territorio que ofrece regulaciones más claras y estables. En una dirección similar, Dropbox ha emprendido un proceso de transformación para proporcionar a sus usuarios opciones avanzadas en cuanto a la configuración de la privacidad de sus datos. Este cambio representa una adaptación a las demandas del mercado, que ha visto el surgimiento de competidores que priorizan la privacidad del usuario. Por otro lado, Meta ha invertido en el desarrollo de varios centros de operaciones en Europa, ubicando gran parte de su actividad en su sede en el Reino Unido[163]. A pesar de que este país ya no es miembro de la UE, mantiene una alineación con su legislación de protección de datos. Esta táctica de Meta puede interpretarse como una respuesta a la necesidad de operar en un marco regulatorio que otorgue certeza legal. El nuevo Acuerdo entre la UE y los EE.UU. se presenta como una potencial solución para estas preocupaciones. Sin embargo, queda por determinar si este pacto será suficiente para satisfacer las exigencias del TJUE. De lo contrario, se corre el riesgo de que se derogue el "escudo de privacidad", lo que volvería a situar a las empresas en un estado de inseguridad jurídica. En este sentido, el futuro de las relaciones transatlánticas en términos de protección de datos sigue siendo una cuestión abierta y de importancia crucial para las empresas globales que operarán en el Metaverso.

X. Conclusiones

86. El Metaverso, como concepto emergente, introduce un nivel completamente nuevo de complejidad a las cuestiones de protección de datos y privacidad. Es un espacio digital compartido, una convergencia de realidades físicas y virtuales prácticamente replicadas, en el que los datos personales se recopilan y utilizan de manera inherente. Este fenómeno resulta en un escenario en el que las ideas tradicionales de ubicación y jurisdicción pueden verse desafiadas y potencialmente volverse menos relevantes. En el Metaverso, los datos pueden ser generados y recopilados en un lugar, pero luego accedidos y utilizados en un contexto digital completamente diferente. Un dato puede ser recopilado en un espacio virtual, almacenado en un servidor en un lugar físico diferente, y luego accedido y utilizado por un usuario en otro lugar. Para ilustrar este escenario, podemos retomar lo que hemos denominado el fenómeno "Tú a Londres y yo a California", en referencia a una película de Disney en la que dos hermanas

[161] RGPD. Artículos 15 a 22. Derecho de acceso del interesado, derecho de rectificación, derecho al olvido, derecho a la limitación del tratamiento, notificación de rectificación o supresión de datos personales o de limitación del tratamiento, derecho a la portabilidad de los datos y derecho de oposición.

[162] RGPD. Artículos 24 y 58. Responsabilidad del responsable del tratamiento y competencias de las autoridades de control.

[163] B. Egliston, M. Carter, "Critical questions for Facebook's virtual reality: data, power and the metaverse", *Internet Policy Review*, vol. 10, nº 4, 2021. [En línea] Disponible en: https://doi.org/10.14763/2021.4.1610

gemelas separadas al nacer se encuentran en un campamento de verano y deciden intercambiar lugares para reunirse con los progenitores que nunca conocieron. El título original, "The Parent Trap", evoca una trama de confusión y complejidad, que también es un reflejo preciso de los desafíos que enfrentamos en la protección de datos en el Metaverso. De la misma manera que las gemelas se intercambian, creando una red de interacciones y relaciones que trascienden las fronteras geográficas y culturales, los datos en el Metaverso pueden ser recopilados, almacenados y utilizados a través de fronteras y jurisdicciones, creando un "laberinto" de protección de datos a través del que los reguladores y los usuarios deben navegar. En el Metaverso, los datos pueden ser generados en un lugar A, almacenados en otro lugar B y, finalmente, ser consultados o utilizados en otro lugar C completamente diferente ubicado a miles de kilómetros de distancia. Esto introduce una nueva dimensión a la protección de datos, ya que los reguladores ahora necesitan considerar no sólo en qué continente se recopilan los datos, sino también dónde se almacenan y cómo y dónde se utilizan. Este desafío se ve agravado por la naturaleza intrínsecamente global del Metaverso. Dado que se trata de un espacio digital sin fronteras físicas, no se limita a las jurisdicciones nacionales o regionales. Esto plantea problemas sobre qué normativas y principios de protección de datos deberían aplicarse, y cómo se deberían aplicar en un espacio que trasciende las fronteras geográficas y las jurisdicciones. Por ejemplo, si los datos de un usuario residente en Europa se almacenan en un servidor ubicado en los EE.UU. y se utilizan en un entorno digital desarrollado en Asia, ¿qué normativas de protección de datos se aplican? ¿Son las de la UE, las de los EE.UU., las de Asia, o alguna combinación de las tres? La respuesta a estas preguntas no está clara y podría depender de varios factores, incluyendo dónde se generan los datos, dónde se almacenan, dónde y cómo se utilizan, y la ubicación de la sede de la empresa o el proveedor de servicios que recopila y procesa los datos. Además, si un usuario del Metaverso interactúa con un avatar u objeto digital que pertenece a otro usuario de una jurisdicción diferente, ¿qué normativas de protección de datos se aplican? ¿Son las de la jurisdicción del primer usuario, las del segundo usuario, o ambas? Nuevamente, las respuestas a estas preguntas pueden ser complejas y dependen de varios factores. Estos desafíos subrayan la necesidad de un enfoque más coherente y armónico para la regulación de la protección de datos en el Metaverso. Es probable que se necesite un enfoque multinivel que combine elementos de las normativas de protección de datos nacionales, regionales y globales, y que tenga en cuenta las características y necesidades específicas del Metaverso. Este enfoque también debe ser flexible y capaz de adaptarse a los rápidos cambios y desarrollos en la tecnología y las prácticas de uso del Metaverso.

87. Para entender por qué el nuevo acuerdo entre la UE y EE.UU. puede ser visto como un "paso más en esta dirección", es decir, en la construcción de un enfoque multinivel hacia la protección de datos, es crucial entender el contexto de la relación de protección de datos entre estas dos entidades. Históricamente, la UE y los EE.UU. han tenido enfoques muy diferentes hacia la protección de datos y privacidad. Mientras que la UE ha enfatizado los derechos de los individuos sobre sus datos personales a través de regulaciones como el RGPD, los EE.UU. han adoptado un enfoque más sectorial, con leyes específicas para ciertas industrias y tipos de datos, pero sin una normativa federal de privacidad general. Esta discrepancia ha provocado tensiones y desafíos, especialmente en lo que respecta a la transferencia de datos entre la UE y los EE.UU. Esto culminó en la anulación del acuerdo de *Safe Harbor* en 2015 y del *Privacy Shield* en 2020 por parte del TJUE, debido a preocupaciones sobre la capacidad de las empresas estadounidenses de garantizar un nivel adecuado de protección de datos para los ciudadanos de la UE, particularmente en relación con la vigilancia del Gobierno de los EE.UU. En este contexto, el nuevo Acuerdo entre la UE y los EE.UU. sobre protección de datos sería un importante paso adelante en la construcción de un enfoque multinivel hacia la protección de datos. Este nuevo Acuerdo podría proporcionar un marco coherente y armonizado para la transferencia de datos entre las dos regiones, respetando tanto los principios de protección de datos de la UE como las prácticas de protección de datos de los EE.UU. Esto es particularmente relevante en la era del Metaverso, donde las transferencias de datos son intrínsecamente globales y no se limitan a una sola jurisdicción. En caso de que, finalmente, el nuevo Acuerdo fuese aceptado por el TJUE, podrían establecer estándares comunes para la protección de datos, proporcionar garantías suficientes contra la vigilancia excesiva del Gobierno y establecer mecanismos para la rendición de cuentas y la reparación en caso de violaciones de la privacidad. También

podría ofrecerse una mayor claridad y certidumbre para las empresas que operan en el Metaverso, permitiéndoles transferir y procesar datos de manera más segura y eficiente. Además, este Acuerdo también podría sentar las bases para una mayor cooperación y armonización en otros aspectos de la regulación de datos en el Metaverso, como la gestión de los derechos de propiedad sobre los datos, los avatares y los objetos digitales, y la regulación de las prácticas comerciales y de publicidad en el Metaverso. No obstante, conviene recordar que cualquier acuerdo entre la UE y los EE.UU. también debe ser flexible y capaz de adaptarse a los rápidos cambios y desarrollos en la tecnología y las prácticas de uso del Metaverso. Esto podría implicar el establecimiento de mecanismos de revisión y actualización regulares, la incorporación de principios de privacidad desde el diseño y por defecto y la promoción de un diálogo continuo entre las partes interesadas para abordar los nuevos desafíos y oportunidades en la protección de datos y privacidad en estos nuevos mundos digitales.

88. Las ideas propuestas por autoras como Julie E. Cohen, Helen Nissenbaum y Sherry Turkle representan vías interesantes de pensamiento que podrían impactar significativamente las futuras regulaciones del Metaverso. La visión de Cohen sobre la privacidad y la tecnología sugiere que las normativas existentes podrían no ser del todo adecuadas para tratar las formas emergentes y evolutivas de las interacciones en el Metaverso. Su concepto de 'autonomía informada' resalta la importancia de dar a los usuarios el control total sobre sus datos, lo cual indica una necesidad de revisión y mejora en las normativas actuales de privacidad y protección de datos, como las estipuladas en el nuevo Acuerdo entre la UE y los EE.UU. Por otro lado, la teoría de la privacidad contextual de Nissenbaum introduce un matiz crucial en el entendimiento de las expectativas de privacidad. La naturaleza de la interacción y la relación entre los datos y su contexto podrían ser muy diferentes en el Metaverso en comparación con otros entornos digitales. En este sentido, la privacidad contextual podría requerir una revisión de los principios que sustentan el Acuerdo entre la UE y los EE.UU., para que sean capaces de adaptarse a los distintos contextos del Metaverso. A su vez, Turkle ofrece una visión de cómo las tecnologías digitales, como el Metaverso, reconfiguran nuestra socialización y formación de identidades. Este hecho podría desafiar nuestras concepciones convencionales de autoexpresión y relación, y potencialmente requerir la creación de regulaciones que aborden específicamente estos aspectos en el Metaverso. Por tanto, el Acuerdo entre la UE y los EE.UU. podría requerir una revisión para abordar cuestiones como el derecho a la anonimidad o a la pseudonimización, el derecho al olvido o el derecho a la protección de la(s) identidad(es) virtual(es) en el Metaverso. En términos críticos, la aplicación de estas teorías sugiere que el Acuerdo entre la UE y los EE.UU., aunque representa un paso importante, podría necesitar de una actualización o modificación para reflejar mejor las realidades únicas y cambiantes del Metaverso. Estas teorías indican que las cuestiones de privacidad y protección de datos en el Metaverso son complejas y multifacéticas, y que las regulaciones deben ser flexibles y capaces de adaptarse a estos retos. Esto podría requerir un replanteamiento de los principios y normas existentes, y la adopción de un enfoque más dinámico y contextualizado hacia la regulación de la privacidad y la protección de datos en el Metaverso.

89. El Acuerdo actual entre la UE y los EE.UU. puede entenderse como una extensión del RGPD en tanto que incorpora muchos de los principios fundamentales y enfoques hacia la protección de datos y la privacidad que se encuentran en el mismo. La aceptación de este nuevo Acuerdo por parte de las autoridades estadounidenses puede interpretarse como una concesión a regañadientes a la presión de las decisiones del TJUE, que ha sentado precedentes importantes en la defensa de la privacidad de los datos en el contexto transatlántico. El acuerdo contempla una vía específica de reparación para los usuarios de la UE que se ven afectados por la transferencia y el tratamiento de sus datos, lo que refleja una aplicación extraterritorial del Derecho de la UE. Esta disposición sugiere que los principios del RGPD están siendo elevados a un rango de norma de *jus cogens* o a un rango de valor en el marco del Derecho Comunitario. Esta elevación de los principios del RGPD podría verse como la creación de una especie de "custodia compartida" de los datos en las transferencias transatlánticas. En este acuerdo, los EE.UU. han aceptado que la UE establezca las reglas del juego. Sin embargo, es probable que este marco evolucione con el tiempo a medida que el Metaverso y las cuestiones de privacidad y protección de datos que plantea evolucionen. Es concebible que, a medida que el Metaverso se desarrolla y se vuelve

más complejo, la regulación de la protección de datos y la privacidad también se vuelva más compleja y matizada. Podríamos ver la aparición de categorías de espacios dentro de los Metaversos, cada uno con sus propias normas y regulaciones. Estas categorías podrían distinguirse en función de la actividad que se lleva a cabo en la plataforma del metaverso específico. Además, podríamos ver una evolución hacia una regulación más similar a la que tiene EE.UU., que es multisectorial, en lugar de la aproximación más general de la UE. Esto podría resultar en diferentes conjuntos de normas y regulaciones para diferentes tipos de actividades o interacciones en el Metaverso. Finalmente, como está ocurriendo con Google, podríamos ver una situación en la que diferentes espacios del Metaverso tienen diferentes normas y regulaciones dependiendo del país desde el que un usuario se conecte. Esto podría dar a los usuarios la opción de elegir, directa o indirectamente, el régimen jurídico al que se someten. Este enfoque podría ser más adaptativo y flexible, pero también podría plantear sus propios desafíos en términos de coherencia y aplicabilidad de las normas.

90. Nos encontramos ante una nueva era en la protección de datos y la privacidad, y aunque podamos trazar algunas líneas sobre cómo se podrían abordar estos desafíos únicos del Metaverso, hay que tener en cuenta que apenas estamos rozando la superficie de este universo emergente. Hay mucho por aprender, descubrir y debatir. En este contexto, aunque las normativas ya establecidas como el RGPD y acuerdos de transferencia de datos transatlánticos puedan constituir la base para la regulación del Metaverso, es bastante posible que veamos surgir normativas innovadoras y enfoques que se ajusten al carácter singular y desafiante de este naciente universo digital. Sin embargo, este recorrido nos lleva a una pregunta fundamental: ¿está realmente legitimado el TJUE para impulsar este tipo de normativas? En la compleja diplomacia de la era digital, esta cuestión subraya el delicado equilibrio entre la promoción de la protección de datos y el respeto a la soberanía de las naciones y sus propios marcos legales. Es crucial considerar que estamos presenciando una especie de "diplomacia de protección de datos". En esta diplomacia, las jurisdicciones y los entes reguladores están estableciendo nuevas formas de negociar y entender el alcance de las diferentes normativas en un entorno tan complejo y sin fronteras como es el Metaverso. Sea como fuere, es innegable que nos encontramos tan sólo en los albores de este fenómeno de (des)localización de los datos. Aún hay mucho que debatir, aprender y adaptar. Las innovaciones tecnológicas, la creciente integración y uso del Metaverso, y las interacciones dinámicas entre los reguladores, los proveedores de servicios del Metaverso y los usuarios influirán en la configuración del marco regulatorio. Esto es sólo el principio. El futuro del Metaverso es una ruta desconocida y emocionante que exigirá seguimiento, adaptación y evolución constantes. Así que, como sociedad global interconectada, se nos presenta el reto y la oportunidad de diseñar este nuevo espacio digital, resguardando que los principios de privacidad y protección de datos no se dejen de lado en este futuro en ciernes.