VICERRECTORADO DE DOCENCIA E
INNOVACIÓN EDUCATIVA
VNiVERSiDAD D SALAMANCA

MEMORIA JUSTIFICATIVA [PID2022/058]

«Metaverso y derecho: implicaciones éticas y jurídicas más allá de los horizontes de la privacidad»

Prof. Dr. Daniel Terrón Santos

Curso académico 2022/2023

Tabla de contenido

1. PRESENTACIÓN DE LA INICIATIVA DESARROLLADA

El vertiginoso avance digital ha encontrado su última manifestación en el metaverso[1], el cual constituye el nuevo objeto de conquista de las grandes corporaciones tecnológicas que aspiran a diseñar un mundo virtual altamente inmersivo que dibuja multitud de nuevos horizontes y posibilidades para el conjunto de la población.

La aparición de este nuevo fenómeno caracterizado por la combinación de elementos físicos y digitales permitirá a los usuarios interactuar y realizar transacciones en mundos totalmente digitales, lo que constituye una importante fuente para la innovación, la creatividad o el despliegue de la economía digital[2], entre otras muchas cuestiones[3]. De igual forma, el metaverso lleva aparejado consigo el despliegue de multitud de nuevas tecnologías y productos (gafas virtuales[4], guantes hápticos[5], etc.) y la puesta en marcha de intensos procesos de recopilación, almacenamiento y utilización de datos personales de la ciudadanía, lo que a todas luces representa un nuevo desafío regulatorio y contribuirá a tensionar aún más el binomio desarrollo tecnológico-privacidad.

A este respecto, centrando nuestra atención en la esfera de la protección de datos de carácter personal son múltiples los interrogantes que plantea el despliegue

---

[1] El metaverso no es un concepto novedoso. Para encontrar su formulación primigenia conviene remontarse hasta 1992, momento temporal en el que Neal Stephenson lleva a cabo la publicación de su novela de ciencia ficción *Snow Crash*, donde humanos y avatares interactúan en un entorno puramente virtual.

[2] Se estima que, en 2025, el metaverso global podría estar valorado en más de $280 billones de dólares.

[3] En palabras de NISA ÁVILA, "el Metaverso es una revolución social, industrial, tecnológica y sobre todo legal. El estado y sus herramientas protectoras deben evolucionar hacia una realidad que se está imponiendo y va a surgir con una fuerza que puede hacer *tambalear el Estado de derecho actual* (…) El derecho es un vertebrador social y como tal debe proteger a sus ciudadanos en cualquier ámbito o situación e impedir la dilución del Estado por una falta de adaptación de la norma a tiempos donde la tecnificación será prácticamente completa". *Vid.* NISA ÁVILA, J.A., "El Metaverso: conceptualización jurídica, retos legales y deficiencias normativas", disponible en: https://bit.ly/3OfUBkP (última consulta el 15 de junio de 2023).

[4] A este respecto recuérdese que, en 1968, Ivan Shuterland y David Evans diseñaron las primeras gafas de realidad virtual con adaptación al movimiento del usuario. Tiempo después, en 1987 Jaron Lanier y Tom Zimmerman desarrollaron el primer guante de datos creando el primer hardware y software asociado al campo de la realidad virtual háptica, o campo de datos hápticos.

[5] La aparición exponencial de dispositivos conectados que podemos usar para controlar aspectos relativos al bienestar y la salud ha dado lugar al concepto de Internet de los Cuerpos (Internet of Bodies, IoB) o cuerpo conectado. El uso de estos dispositivos para monitorizar distintos parámetros de nuestro cuerpo tiene como resultado el tratamiento de datos biométricos y de salud con indudables ventajas, pero también implica nuevos riesgos para la privacidad y, en determinadas circunstancias, pueden llegar a comprometer la integridad física de la persona usuaria. Se puede definir conceptualmente el Internet de los Cuerpos como el uso de dispositivos conectados a Internet que monitorizan y/o actúan sobre todas o algunas de nuestras constantes vitales y otros datos biométricos, así como otros indicadores de salud como actividad física, calidad del sueño, actividad deportiva o sedentarismo. Todo esto son datos personales que van a ser analizados, explotados, almacenados, y en definitiva procesados de muy diversas formas, por diferentes personas responsables y encargadas del tratamiento. *Vid.* AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *IoT (II): Del Internet de las Cosas al Internet de los Cuerpos*, Madrid, 2021. Disponible en: https://bit.ly/3ba8YZU (última consulta el 15 de junio de 2023).

de este fenómeno: ¿cumplirán estos nuevos productos inteligentes con las exigencias establecidas en la ambiciosa regulación en materia de protección de datos personales? ¿qué tipología de tratamientos de datos personales comportará este nuevo universo digital? ¿cuál será el grado de importancia y protagonismo que se confiera a la privacidad en el diseño de estos nuevos productos y servicios digitales?

Sin perjuicio de acometer iniciativas reguladoras específicas pro futuro, orientadas a embridar los claroscuros que envuelven el metaverso, y del esperado desarrollo del Paquete Digital Europeo[6], conviene recordar que la actual regulación en materia de protección de datos de carácter personal, presidida por el poderoso Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos —RGPD—) constituye un importante dique de contención frente a los anhelos de los gigantes tecnológicos de servirse de nuevos datos de los usuarios.

Sentada esta premisa, y partiendo de los distintos pronunciamientos de las autoridades de control europeas en la materia[7], la presente iniciativa formativa aspira

---

[6] Momento en el que nos encontramos nuevamente en tiempo de tribulación, en el que se está gestando no solamente el tercer acuerdo transatlántico para la transferencia de datos personales de los ciudadanos europeos entre Estados Unidos y la Unión Europea, conocido *como Trans-atlantic data privacy framework*; sino también los distintos hitos normativos que darán forma al esperado Paquete Digital de la Unión Europea. Junto a este hito, destacan otro conjunto de instrumentos jurídicos con los que se pretende garantizar la soberanía digital del proyecto de integración europeo e instaurar un auténtico mercado único digital, como ocurre en el supuesto concreto de la Ley de gobernanza de datos, la Ley de servicios digitales, el Reglamento sobre mercados digitales y la Estrategia de Ciberseguridad de la Unión Europea. Más allá de este conglomerado de iniciativas y transformaciones normativas se prevé, de igual forma, el despliegue de un importante volumen de inversiones e instrumentos presupuestarios necesarios para dotar de efectividad esta transición digital, incluidos los programas de cohesión, el instrumento de apoyo técnico y el Programa Europa Digital. Así mismo, cabe destacar el acuerdo de los colegisladores de que un mínimo del 20% del montante total de inversiones derivadas del Mecanismo de Recuperación y Resiliencia debe apoyar la transición digital con la finalidad de contribuir a sustentar este programa de reformas avanzando con ello en la consecución de los objetivos del Decenio Digital de Europa. *Vid*. COMISIÓN EUROPEA, *Brújula Digital 2030: el enfoque de Europa para el Decenio Digital*, Bruselas, 2021, pág. 2 [COM(2021) 118 final].

[7] A este respecto, entre otros, conviene recordar el Dictamen 8/2014 sobre la evolución reciente del Internet de las Cosas (IOT en sus siglas en inglés), donde el anterior Grupo de Trabajo del artículo 29 exponía que los principales problemas de intimidad y protección de datos derivados del uso de estos dispositivos estaban estrechamente imbricados con la falta de control y la asimetría de la información, la calidad del consentimiento del usuario, las conclusiones extraídas de los datos y readaptación del tratamiento original, la revelación invasiva de pautas de comportamiento y perfiles, las limitaciones de la posibilidad de permanecer en el anonimato cuando se hace uso de estos servicios o los riesgos para la seguridad de la información. *Vid*. GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos*, adoptado el 16 de septiembre de 2014, págs. 7-11 (WP 223).

Tiempo después, el Supervisor Europeo de Protección de Datos publicaba un informe sobre gafas inteligentes y protección de datos en el que se ponían de relieve los peligros que dichos dispositivos pueden llegar a ocasionar en lo relativo a la privacidad y protección de datos personales de los usuarios, así como de terceros: (i) falta de control de datos por parte de los usuarios y especialmente por parte de los no usuarios; (ii) imposibilidad de consentir y ser informado adecuadamente, principalmente para los no usuarios; (iii) inferencias derivadas de datos y reutilización; (iv) análisis intrusivo del comportamiento y elaboración de perfiles; (iv) limitaciones y falta de anonimato debido a la alta identificabilidad de la información que se procesa (imágenes faciales, videos, grabaciones de sonido o incluso la posibilidad de que los propios dispositivos identifiquen a las personas que están a su

a clarificar los principales problemas que entraña el despliegue del metaverso desde el prisma de la intimidad y la protección de datos de carácter personal (licitud del tratamiento, falta de control y asimetría de la información, calidad del consentimiento del usuario, ausencia de privacidad desde el diseño y por defecto, etc.), poniendo de relieve la plena operatividad del sistema europeo de tutela jurídica de los derechos de la privacidad y la conveniencia de revigorizar el enfoque de riesgo[8] que subyace y vehicula el mismo, como presupuesto indispensable para garantizar la dignidad y seguridad de la persona en este nuevo universo digital altamente inmersivo.

2. EQUIPO DE TRABAJO

El equipo de trabajo encargado del desarrollo e implementación del Proyecto de Innovación Docente 2022/058, «*Metaverso y derecho: implicaciones éticas y jurídicas más allá de los horizontes de la privacidad*», coordinado y supervisado por el Prof. Dr.

---

alcance mediante el reconocimiento facial y de voz y las señales de Wi-Fi y Bluetooth); (v) procesamiento de categorías especiales de datos, que requiere salvaguardias especiales, etc. *Vid.* EUROPEAN DATA PROTECTION SUPERVISOR, *Technology report 1: Smart glasses and data protection*, Bruselas, 2019, pág. 7. Disponible en: https://bit.ly/2AYHdOV (última consulta el 15 de junio de 2023).

Destacables resultan también, los comunicados emitidos por las autoridades de control en materia de protección de datos de Irlanda e Italia, emitidos a propósito de la puesta en marcha de Facebook View (glasses), nuevo producto que mediante el uso de controles activados por voz (dato biométrico), permite al usuario de las gafas grabar videos cortos y tomar fotos para publicar en las redes sociales. Las famosas Ray-Ban Stories comenzaron a comercializarse en España el pasado 17 de marzo de 2022. Junto a su lanzamiento, el gigante tecnológico Meta ha creado una campaña de comunicación en varios países de la Unión Europea para explicar el funcionamiento de estas gafas inteligentes, al tiempo que hace un llamamiento a sus usuarios para que hagan un empleo razonable de las mismas, especificando, por ejemplo, en qué situaciones conviene no hacer uso de las capacidades que ofrecen las gafas. En otras palabras, desde la corporación tecnológica se deja a la buena voluntad de los usuarios la preservación de la privacidad, cuestión escabrosa que en el medio plazo puede dar lugar a la incoación de un nuevo procedimiento sancionador contra Meta por vulnerar —una vez más— la actual regulación europea en materia de protección de datos de carácter personal.

[8] La gestión del riesgo está formada por un conjunto de acciones ordenadas y sistematizadas con el propósito de controlar las posibles (probabilidad) consecuencias (impactos) que una actividad puede tener sobre un conjunto de bienes o elementos (activos) que han de ser protegidos. La gestión del riesgo precisa de un análisis, es decir, una reflexión crítica y objetiva de un tratamiento, requiere, por tanto, tomar decisiones que se han de plasmar en hechos concretos (controles) que minimicen el impacto sobre los activos hasta unos niveles tolerables. *Vid.* AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*, Madrid, 2021, pág. 12.

Recuérdese a este respecto que, las normas ISO 31000:2018 e ISO 31010:2019, definen el concepto de "riesgo" como el "efecto de la incertidumbre sobre la consecución de objetivos" entendiendo como tal efecto cualquier desviación positiva o negativa sobre lo previsto inicialmente, teniendo en cuenta que los objetivos pueden ser de distinto tipo según el ámbito de actividad de una organización.

Por su parte, conviene precisar que el RGPD demanda la identificación, evaluación y mitigación, realizadas de una forma objetiva, del riesgo para los derechos y libertades de las personas en los tratamientos de datos personales (Considerandos 76 y 77, respectivamente). La mitigación ha de realizarse mediante la adopción de medidas técnicas y organizativas que garanticen y, además, permitan demostrar la protección de dichos derechos (art. 24 RGPD). Estas deberán determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento. Además, dichas medidas se revisarán y actualizarán cuando sea necesario. En definitiva, el RGPD exige un proceso de gestión del riesgo para los derechos y libertades de los interesados, que necesariamente debe estar documentado en virtud del principio de responsabilidad proactiva o "accountability" (art. 5.2 RGPD).

Daniel Terrón Santos, ha estado integrado por el siguiente plantel docente:

- **MARCOS M. FERNANDO PABLO.** *Catedrático de Derecho Administrativo de la Universidad de Salamanca*
- **JOSÉ MARÍA LAGO MONTERO.** *Catedrático de Derecho Financiero y Tributario de la Universidad de Salamanca*
- **MARÍA ÁNGELES GUERVÓS MAÍLLO.** *Profesora Titular de Derecho Financiero y Tributario de la Universidad de Salamanca*
- **ROSA MARÍA ALFONSO GALÁN.** *Profesora Titular de Derecho Financiero y Tributario de la Universidad de Salamanca*
- **ISABEL GIL RODRÍGUEZ.** *Profesora Titular de Derecho Financiero y Tributario de la Universidad de Salamanca*
- **MARCOS IGLESIAS CARIDAD.** *Profesor Contratado Doctor de Derecho Financiero y Tributario de la Universidad de Salamanca*
- **NORA LIBERTAD RODRÍGUEZ PEÑA.** *Contratada posdoctoral "Margarita Salas" de la Universidad de Salamanca*
- **ALICIA RODRÍGUEZ SÁNCHEZ.** *Personal Investigador en Formación (USAL) del Área de Derecho Penal de la Universidad de Salamanca*
- **IRENE GONZÁLEZ PULIDO.** *Contratada posdoctoral "Margarita Salas" de la Universidad de Salamanca*
- **ANA GARCÍA GARCÍA.** *Personal Investigador en Formación (JCYL) del Área de Derecho del Trabajo y la Seguridad Social de la Universidad de Salamanca*
- **JOSE LUIS MATEOS CRESPO.** *Profesor Asociado del Área de Derecho Constitucional de la Universidad de Salamanca*
- **LIDIA GARCÍA MARTÍN.** *Profesora Ayudante del Área de Derecho Administrativo de la Universidad de León*
- **JUAN FRANCISCO RODRÍGUEZ AYUSO.** *Profesor Ayudante Doctor del Área de Derecho Administrativo de la Universidad Nacional de Educación a Distancia*
- **JOSE LUIS DOMÍNGUEZ ÁLVAREZ.** *Profesor Asociado del Área de Derecho Administrativo de la Universidad de Salamanca*
- **LUIS MIGUEL SÁNCHEZ GIL.** *Profesor Asociado del Área de Personalidad, Evaluación y Tratamiento Psicológico de la Universidad de Salamanca*
- **PILAR TALAVERA CORDERO.** *Investigadora predoctoral de la Universidad de Salamanca*

3. LISTADO DE ASIGNATURAS EN LAS QUE SE HA IMPLEMENTADO EL PROYECTO DE INNOVACIÓN DOCENTE

A continuación, se enumeran los planes de estudio y asignaturas a través de las que se han articulado las diferentes actividades que conforman el PID2022/058, las cuales fueron seleccionadas meticulosamente para que estuvieran estrechamente vinculadas con la finalidad de la iniciativa de innovación docente y contribuyeran en mayor medida a enriquecer el proceso de aprendizaje del estudiantado. Dichas asignaturas se enumeran a continuación:

- (102305) **FUNDAMENTOS DE DERECHO ADMINISTRATIVO** *(Grado en Derecho, Grupos I y II)*
- (102307) **INTRODUCCIÓN AL DERECHO PENAL** *(Grado en Derecho, Grupos II y III)*
- (102309) **GARANTÍAS JURÍDICO-ADMINISTRATIVAS** *(Grado en Derecho, Grupo III)*
- (102311) **TEORÍA JURÍDICA DEL DELITO** *(Grado en Derecho, Grupo II)*
- (102313) **DERECHOS FUNDAMENTALES Y ORGANIZACIÓN TERRITORIAL DEL ESTADO** *(Grado en Derecho, Grupos I y II)*
- (102314) **CONTRATOS PÚBLICOS, URBANISMO Y ORDENACIÓN DEL TERRITORIO** *(Grado en Derecho, Grupos II y III)*
- (102321) **DERECHO FINANCIERO Y TRIBUTARIO. PARTE GENERAL** *(Grado en Derecho, Grupos I, II y III)*
- (102326) **DERECHO FINANCIERO Y TRIBUTARIO. PARTE ESPECIAL** *(Grado en Derecho, Grupos I, II y III)*
- (102342) **BIENES PÚBLICOS Y MEDIO AMBIENTE** *(Grado en Derecho, asignatura optativa)*
- (100401) **INTRODUCCIÓN AL ESTADO CONSTITUCIONAL** *(Grado en Ciencia Política y Administración pública)*
- (100417) **CONTROL DE LA LEGALIDAD DE LA ADMINISTRACIÓN** *(Grado en Ciencia Política y Administración Pública)*
- (100430) **DERECHO DEL MEDIO AMBIENTE** *(Grado en Ciencia Política y Administración Pública)*
- (100433) **GESTIÓN ADMINISTRATIVA** *(Grado en Ciencia Política y Administración Pública)*
- (100443) **BIENES PÚBLICOS Y CONTRATACIÓN ADMINISTRATIVA**

(Grado en Ciencia Política y Administración Pública)

- (100901) **FUNDAMENTOS DEL ESTADO CONSTITUCIONAL** *(Grado en Ciencia Política y Administración pública)*
- (104530) **DERECHO DE LA PREVENCIÓN DE RIESGOS LABORALES I** *(Grado en Relaciones Laborales)*

4. OBJETIVOS ESTABLECIDOS

La acción principal en la que se ha enmarcado el desarrollo de este proyecto, como es sabido, se corresponde con la Innovación en modalidad de Aprendizaje-Servicio integrado en titulaciones oficiales, tal y como fue reflejado en su momento en la solicitud del mismo. En efecto, el PID2022/058 aspiraba a reformular las técnicas metodológicas del profesorado universitario, mediante la maximización de la puesta en práctica de los contenidos analizados en las diferentes asignaturas y planes de estudios, aplicados a la resolución de problemas sociales concretos y al impulso del conocimiento de las tecnologías disruptivas y el fenómeno tecnológico por parte del estudiantado, cuestiones todas ellas esenciales no solo para potenciar la inserción laboral y profesional del estudiantado, sino también para fortalecer el desarrollo de actuaciones de responsabilidad social por parte de la comunidad universitaria de la Universidad de Salamanca. La alta participación y el enorme grado de sensibilización del alumnado demuestran que la elección de la temática objeto de estudio fue muy acertada y ha contribuido sobremanera a mejorar el prestigio del Estudio salmantino al situarla como un actor decisivo en la consecución de una transformación digital humanista.

Con el firme propósito de impulsar la puesta en marcha de nuevas herramientas metodológicas que contribuyan de manera significativa a fomentar la participación del estudiantado y maximizar la adquisición de conocimientos mediante el planteamiento de problemas sociales de profundo calado que demandan respuestas innovadoras por parte de la comunidad universitaria, mostrar las oportunidades de empleabilidad y emprendimiento que permite la transformación digital de nuestras sociedades, así como los profundos desafíos que esta vertiginosa (r)evolución digital plantea desde el prisma de las Ciencias jurídicas; el equipo encargado del desarrollo del proyecto de innovación docente ha trabajado en la consecución de los siguientes objetivos:

I. Sumergir al estudiantado en los desafíos económicos y sociales que plantea el despliegue del metaverso, con el firme propósito de fortalecer tanto su capacidad para analizar las implicaciones jurídicas que posee esta última manifestación del fenómeno tecnológico, como espolear sus competencias digitales, lo que permitirá diversificar la inserción laboral y el emprendimiento del alumnado, de conformidad con el ODS3, el ODS4 y el ODS8.

II. Introducir al estudiantado en el análisis de los principales desafíos e interrogantes que plantea la (r)evolución digital, especialmente los entornos virtuales altamente inmersivos, con la finalidad de garantizar el pleno disfrute

de los derechos y libertades fundamentales de la ciudanía, el normal funcionamiento de las instituciones, la salvaguarda de la seguridad jurídica o la pervivencia del Estado social y democrático de Derecho.

III. Fortalecer la colaboración entre el Estudio salmantino y otras Instituciones (Agencia Española de Protección de Datos, Supervisor Europeo de Protección de Datos, Secretaría de Estado de Digitalización e Inteligencia Artificial, etc.) las cuales disponen de un papel capital en la transformación digital que está impulsando el Estado español, lo que las convierte en actores esenciales en la exposición de las nuevas fuentes de empleabilidad que propician los procesos de digitalización y datificación de la sociedad.

IV. Apostar por la gamificación de la docencia mediante el impulso de nuevas herramientas metodológicas, más atractivas e interactivas para el estudiantado, tales como: YouTube, TED, Kahoot!, Animoto, Socrative, Plickers, Quizziz, etc.

V. Potenciar el empleo responsable de las redes sociales y los recursos digitales como herramienta para enriquecer los procesos de aprendizaje en el ámbito educativo superior, mediante la organización de actividades formativas que fomenten la participación del estudiantado tales como Twitter Chat, Twitter Spaces, etc., cuya eficacia y éxito se ha comprobado en el impulso de proyectos de innovación docente de aprendizaje-Servicio en cursos académicos anteriores.

VI. Potenciar el interés y la atracción del estudiantado por las asignaturas de Derecho Administrativo y Derecho Financiero Tributario, mediante la implementación de una visión práctica y crítica de los estudios jurídicos, y profundizando en el análisis del futuro sombrío del sector legal, ámbito en el que la automatización amenaza con hacer desaparecer antes de 2050 entre el 30% y el 50% de la fuerza laboral.

VII. Concienciar y sensibilizar al profesorado en formación y a los jóvenes investigadores acerca de la necesidad de fomentar herramientas y metodologías docentes innovadoras, como presupuesto fundamental para mejorar la calidad de las enseñanzas impartidas en la Universidad de Salamanca.

VIII. Maximizar el intercambio de experiencias de innovación docente mediante la incorporación de docentes de otras instituciones de educación superior, con el firme propósito de avanzar en la renovación y mejora continua de las metodologías y capacidades docentes del profesorado, así como en el establecimiento de sinergias duraderas en el tiempo con otros centros educativos.

IX. Potenciar la empleabilidad del alumnado de los grados implicados en el proyecto de innovación docente, de la mano del impulso de la educación para la digitalización, lo que permitirá acercarles a las diferentes alternativas

laborales que plantea el renovado protagonismo de las Ciencias Jurídicas (abogacía digital, delegados de protección de datos, expertos en privacidad y ciberseguridad, etc.).

X. Responder a una de las recomendaciones más acuciantes planteada por los organismos externos de evaluación de la calidad de los programas formativos, es decir, mejorar el grado de empleabilidad y la inserción laboral de titulaciones tales como el Grado en Ciencia Política y Administración Pública o el Grado en Derecho, mediante el planteamiento de nuevas oportunidades de futuro y nichos de empleo.

5. GRADO DE INNOVACIÓN ALCANZADO

A. El grado de compromiso y la interdisciplinaridad del equipo docente

Una de las principales notas características del presente proyecto de innovación docente, la cual constituye sin duda una de sus principales fortalezas, es la incorporación, dentro del equipo docente de profesorado perteneciente a diferentes ramas del mundo jurídico como son el Derecho Administrativo, el Derecho Financiero y Tributario, el Derecho Constitucional, el Derecho Penal y el Derecho Laboral, áreas de conocimiento diferenciadas pero muy próximas entre sí. Esta cuestión, la cual a priori se presentaba como un importante desafío, ha resultado ser crucial para conseguir no solamente una visión holística del poderoso alcance que ejerce la tecnología en las diferentes ramas del ordenamiento jurídico, sino también para diseñar nuevas líneas de investigación en la materia de cara al futuro inmediato.

El citado proyecto de innovación ha permitido afianzar la colaboración y cooperación del grupo de trabajo, permitiendo al equipo docente involucrarse, a través de su actuación cotidiana en las aulas, en la búsqueda de soluciones tangibles para dos desafíos de los desafíos más acuciantes a los que se enfrenta la sociedad: (i) minimizar las externalidades y efectos nocivos derivados de los profundos procesos de datificación y digitalización de la sociedad; y (ii) garantizar la seguridad jurídica de todos los operadores implicados en los entornos digitales.

De esta forma se complementa y enriquece la trayectoria de un elenco de docentes interesados en espolear el interés del estudiantado y el fomento de la adopción de metodologías docentes más cercanas que permitan incrementar la participación del mismo.

Ciertamente, el proyecto de innovación docente que ahora se justifica ha servido para seguir profundizando en la senda de iniciativas anteriores, en las que el grupo de trabajo centro sus esfuerzos en el estudio de importantes reformas normativas, el análisis y difusión de los nuevos derechos digitales, el impulso de la administración electrónica, el emprendimiento juvenil o la implementación de la perspectiva de género, analizando el impacto que estas cuestiones poseían sobre los derechos y la posición jurídica de los ciudadanos.

B. El enfoque práctico y la temática de la iniciativa. Un proyecto para situar a la Universidad de Salamanca a la cabeza de una transformación digital humanista

Asimismo, el PID2022/058 introducir en el aula una realidad (la tecnológica) tangible pero sumamente desconocido para los futuros profesionales del mañana, no solamente en forma de enriquecedores debates jurídico-administrativos en el aula, sino también mediante la participación del estudiantado en diferentes iniciativas de formación continuada impulsadas por el profesorado, lo cual ha permitido a docentes y discentes no solamente conocer de primera mano, a través del testimonio de profesionales de primer nivel, los desafíos éticos y jurídicos que plantea el vertiginoso avance digital (y especialmente los sistemas algorítmicos); sino también, y lo más importante, el papel protagonista que el Derecho ejerce en estos procesos de digitalización y las nuevas oportunidades laborales que comporta la especialización en este concreto campo.

Así mismo, el importante grado de innovación de la iniciativa desarrollada y la transcendencia del estudio de esta novedosa línea de investigación ha sido reconocida por las más altas instancias institucionales del Reino de España, lo que se ha traducido en la incorporación del Prof. Dr. Daniel Terrón Santos y del Prof. José Luis Domínguez Álvarez al Grupo de Reflexión destinado a profundizar en la dimensión ética de la Inteligencia Artificial impulsado por el Senado de España.

C. La participación del personal investigador en formación y el protagonismo de la innovación docente desde el inicio de la carrera académica

Igualmente novedoso y llamativo resulta la incorporación y el importante grado de participación que el coordinador del proyecto de innovación docente objeto de justificación ha concedido a los jóvenes investigadores y docentes que integraban el plantel docente de la iniciativa, los cuales han contribuido a enriquecer sobremanera el elenco de actividades planteadas al estudiantado, interiorizando desde las primeras fases de la carrera académica la importancia de la innovación docente y la búsqueda de nuevas herramientas metodológicas para captar la atención del estudiantado y potenciar su participación en el aula.

D. La apuesta por las redes sociales y la gamificación de la docencia como atractivo

Finalmente, además de plantear una temática innovadora y un grupo de trabajo multidisciplinar, el PID2022/058 se ha caracterizado de igual forma por la adopción de técnicas y herramientas metodológicas innovadoras orientadas a maximizar la interacción del estudiantado y la adquisición de los conocimientos propuestos desde una perspectiva práctica.

Para ello, no solamente se ha potenciado el empleo de las nuevas tecnologías en el aula, lo que se ha concretado en el uso de apps como YouTube, TED, Kahoot, Animoto, Socrative, Plickers o Quizziz, sino también en el impulso del uso responsable de las redes sociales, especialmente Twitter, como fuente inagotable de información

y como espacio de debate e intercambio de ideas y reflexiones.

6. PLAN DE TRABAJO IMPLEMENTADO

En el marco del PID2022/058 se han realizado diferentes actividades desde distintas perspectivas y áreas de conocimiento, abordadas en una serie de asignaturas que han dado cobertura a las iniciativas planteadas a lo largo de este curso 2022/2023. Las actividades concretas se especificaron a través de un plan de trabajo transversal que fue asumido satisfactoriamente por cada uno de los integrantes del equipo de trabajo, y que será especificado en las próximas líneas.

A. Tipo de contenidos a desarrollar

Como se ha señalado con anterioridad, la finalidad del PID2022/058 no es otra que la sumergir al estudiantado en el cambio de paradigma que están experimentando las Ciencias Jurídicas, fruto del prolífico avance que están protagonizando las tecnologías disruptivas (Metaverso, Inteligencia Artificial, Internet of Things, Blockchain, etc.) con el firme propósito de implementar y diversificar la inserción laboral y el emprendimiento del estudiantado. De esta forma, el equipo docente ha trabajado en la consecución de un doble objetivo, por un lado, maximizar la empleabilidad del estudiantado mediante el análisis de la transformación de las Ciencias jurídicas al calor de la transición digital y, por otro, potenciar la participación de la Universidad en la resolución de retos sociales globales y tangibles, mediante la mejora de la colaboración interinstitucional, lo que puede traducirse en el establecimiento de mecanismos de colaboración duraderos en el tiempo que faciliten la inserción laboral del estudiantado.

Para ello, en primer lugar, el profesorado realizó una exposición del proyecto al estudiantado, enumerando por escrito y con numeroso material de consulta disponible en Studium (https://studium.usal.es), tanto los objetivos, como la finalidad y las pautas de desarrollo del Proyecto de Innovación Docente, con el propósito de potenciar la participación del alumnado. Como decimos, se facilitaron materiales con las nociones y recursos necesarios para garantizar la participación efectiva de los estudiantes y sacar el máximo rendimiento a la iniciativa.

A continuación, se expusieron los principales desafíos e interrogantes que plantea la (r)evolución digital en general, y el metaverso en particular, con la finalidad de garantizar el pleno disfrute de los derechos y libertades fundamentales de la ciudanía, el normal funcionamiento de las Administraciones públicas, la salvaguarda de la seguridad jurídica o la pervivencia del Estado social y democrático de Derecho, para que después el alumnado pudiera continuar explorando de forma autónoma la cuestión a través de los diversos materiales aportados, apoyo indispensable para su posterior participación activa en el desarrollo de esta iniciativa.

B. Tipo de trabajo

El trabajo llevado a cabo por los estudiantes ha revestido carácter individual puesto que, como se ha detallado anteriormente, los estudiantes debían identificar, a raíz de las diferentes intervenciones de las personalidades invitadas a participar en la iniciativa, y reflexionar mediante la elaboración de un abstract una problemática particular vinculada a los procesos de digitalización de la sociedad. Aportaciones que fueron compartidas por el estudiantado en un apartado específico del Campus Virtual Studium y posteriormente fueron examinadas, evaluadas y calificadas de forma individualizada por parte del profesorado que ha participado en la iniciativa.

C. Tipo de participación

La participación de los alumnos ha sido obligatoria en toda la actividad, puesto que el proyecto de innovación docente formaba parte de las exigencias propias de las asignaturas enumeradas en el apartado 2. De este modo, el trabajo de recopilación y aprendizaje teórico, si bien limitado y previo al desarrollo propio del proyecto, sirvió de base para la realización de las tareas prácticas encomendadas y para cumplimentar con éxito los objetivos detallados en el punto 3 de esta memoria.

D. Peso del trabajo en la evaluación de la asignatura

El trabajo desarrollado por el estudiante y exigido en el marco del Proyecto de Innovación Docente que nos ocupa ha supuesto el 10% de la calificación final de la asignatura, de tal manera que se ha tenido muy presente la implicación de cada uno de los estudiantes en las tareas, así como su motivación y compromiso de participación activa en la calificación final de las asignaturas que integraban la propuesta de innovación docente.

7. CRONOGRAMA DE EJECUCIÓN

Como se ha señalado con anterioridad, el presente proyecto de innovación docente tenía como objetivo, por un lado, potenciar la puesta en marcha de nuevas herramientas metodológicas que contribuyan de manera significativa a fomentar la participación del estudiantado y maximizar su proceso de aprendizaje, mediante el planteamiento de problemas sociales de profundo calado que demandan respuestas innovadoras por parte de la comunidad universitaria; y, por otro, mostrar las oportunidades y desafíos que la digitalización y datificación de la sociedad plantea desde el prisma de la inserción laboral de los egresados de Ciencias Jurídicas. Al mismo tiempo se contemplaba la adquisición de competencias del alumnado para fomentar la educación para la digitalización en el sector legal, cuestión fundamental no contemplada hasta la fecha en los planes de estudio vigentes a pesar de su transcendía. Todo ello se ha pretendido conseguir a través del impulso de las siguientes actuaciones:

I. **Organización y reparto de tareas.** Reunión del grupo de profesores participantes en el proyecto de innovación docente, diseño de materiales y distribución de intervenciones y tareas para la correcta coordinación y desarrollo de la iniciativa [noviembre de 2022]

II. **Elaboración de materiales originales.** El personal investigador en formación, bajo la supervisión del coordinador, llevó a cabo el diseño y elaboración de materiales originales e innovadores (contribuciones científicas, presentaciones, infografías, imágenes, cartelería, etc.), así como de la recopilación de fuentes bibliográficas y recursos normativos, elementos en los que se sustentará con posterioridad el desarrollo del proyecto de innovación docente [diciembre de 2022-enero de 2023]

III. **Exposición del proyecto al estudiantado.** Los integrantes del grupo de trabajo expusieron en sus respectivas asignaturas los objetivos, la finalidad y las pautas de desarrollo del proyecto de innovación docente, potenciando la participación activa del alumnado. Para ello, se procedió a la creación de un espacio dedicado exclusivamente al PID dentro del Campus Virtual Studium de cada una de las asignaturas que forman parte de la iniciativa, a través del que se facilitaron materiales con las nociones y recursos necesarios para garantizar la participación efectiva del estudiantado y sacar el máximo rendimiento a la iniciativa [febrero de 2023]

IV. **Exposición simplificada de los principales desafíos e interrogantes que plantea la (r)evolución digital, especialmente el universo del metaverso**. El propósito no es otro que el de garantizar el pleno disfrute de los derechos y libertades fundamentales de la ciudanía, el normal funcionamiento de las Administraciones públicas, la salvaguarda de la seguridad jurídica o la pervivencia del Estado social y democrático de Derecho, por parte del profesorado participante en el equipo de trabajo desde las diferentes perspectivas que proporcionan las diferentes áreas de conocimiento [marzo de 2023]

V. **Implicación del estudiantado.** El profesorado elaboró una serie de pautas con el propósito de que cada estudiante procediera a identificar una problemática vinculada al avance digital y articular una respuesta o solución tangible que contribuya a garantizar el ejercicio pleno de los derechos de la ciudadanía. Se valoró positivamente el uso de la información puesta a su disposición en los materiales facilitados previamente por el profesorado [mayo de 2023]

VI. **Evaluación de la participación del estudiantado en la iniciativa.** Una vez concluidas las diferentes actividades que conforman el proyecto de innovación docente, el equipo docente procedió a examinar de forma individualizada tanto el grado de participación del alumnado en las diferentes actuaciones, como las aportaciones tangibles de los mismos, al objeto de consignar la calificación individualizada de cada alumno/a, ya que se prevé que la implicación del alumnado represente el 10% de la

calificación global de aquellas asignaturas que integran la propuesta de proyecto de innovación docente [junio de 2023]

VII. Valoración del proyecto de innovación docente, elaboración de propuestas de mejora y justificación de la iniciativa [junio de 2023]

8. RECURSOS EMPLEADOS

La irrupción de la COVID-19 supuso la generalización de los medios digitales, convirtiéndolos en herramientas indispensables para el desarrollo de las actividades docentes. En este sentido, el Campus Virtual Studium de la Universidad de Salamanca y la aplicación de videoconferencias Zoom se han convertido en el vehículo idóneo para la realización de buena parte de las actividades que se han impulsado en el marco del PID2022/058.

El profesorado implicado a empleado de igual forma diferentes instrumentos para esquematizar y presentar los contenidos esenciales de la iniciativa, bien a través de la elaboración de presentaciones tradicionales (Power Point, Prezi, etc.) o bien mediante la elaboración de infografías y mapas conceptuales para condensar las cuestiones objeto de estudio (Canva, Infogram, etc.).

De igual forma, el equipo docente ha apostado por la gamificación de las actividades que se han sucedido durante los meses en los que se ha puesto en marcha el proyecto de innovación docente, con el firme propósito de incrementar la atención del estudiantado y maximizar su participación e implicación en la propuesta innovadora. Para ello se han empleado instrumentos tales como Kahoot!, Quizizz, etc.

Adicionalmente, se ha fomentado el uso responsable de las redes sociales, como instrumento para buscar información diversa y amplia sobre el objeto de estudio e interactuar con actores destacados del ámbito de la protección de datos, la seguridad de la información o la digitalización de la economía, entre otros muchos ámbitos.

9. RESULTADOS OBTENIDOS

Mediante el desarrollo del proyecto de innovación docente objeto de justificación se ha conseguido que el estudiantado:

- Conozca suficientemente las ventajas y potencialidades, así como los principales interrogantes y desafíos derivados del avance del metaverso, herramienta que está propiciando una vertiginosa transformación de las estructuras sociales y económicas y que tiene ya una incidencia directa en la empleabilidad de los egresados de las Ciencias Jurídicas.
- Participe en el diseño de políticas públicas innovadoras e instrumentos normativos específicos que contribuyan a alcanzar un desarrollo tecnológico antropocéntrico, ético, sostenible, igualitario respetuoso con los derechos y valores fundamentales que integran la concepción de ciudadanía europea.
- Analice los desafíos y oportunidades de inserción laboral y emprendimiento

que presenta la automatización del sector legal, para lo que se prevé la colaboración con Administraciones públicas, Autoridades de control en materia de protección de datos (Agencia Española de Protección de Datos, Supervisor Europeo de Protección de Datos, etc.) y empresas del sector tecnológico.

- Adquiera competencias digitales mediante el impulso de metodologías docentes novedosas, sustentadas en el empleo responsable de las redes sociales, para lo que se prevé la creación de foros y Twitter Chats, iniciativas que tuvieron una acogida extraordinaria por parte del estudiantado en proyectos de innovación docente precedentes (especialmente en el ID2019/051, ID2020/035 y el ID2021/049).
- Visualice de forma directa la aplicabilidad práctica de los contenidos teóricos que componen el programa de cada una de las asignaturas que componen los planes de estudio del Grado en Derecho, Grado en Ciencia Política y Administración Pública y Grado en Criminología.

10. MEMORIA ECONÓMICA

El PID2022/058, «Metaverso y derecho: implicaciones éticas y jurídicas más allá de los horizontes de la privacidad» no ha contado con ningún tipo de financiación por parte de la Universidad de Salamanca. Las actividades desarrolladas por el equipo docente no han sido objeto de ningún tipo de remuneración y las conferencias impartidas por profesionales externos al Estudio salmantino en el marco del proyecto de innovación docente han sido financiados directamente por el coordinador (Prof. Dr. Daniel Terrón Santos) y el adjunto a la coordinación (Prof. José Luis Domínguez Álvarez).

11. EVIDENCIAS DEL PROYECTO DE INNOVACIÓN DOCENTE

A continuación, se enumeran los documentos que se adjuntan a la presente memoria de justificación, los cuales se corresponden con algunos de los materiales empleados por el equipo docente para dar forma a la iniciativa:

A. PRIMEROS PASOS [DOC1]

B. DOCUMENTO DE PARTIDA [DOC2]

VICERRECTORADO DE DOCENCIA E INNOVACIÓN EDUCATIVA

VNiVERSiDAD D SALAMANCA

ANEXOS [PID2022/058]

«Metaverso y derecho: implicaciones éticas y jurídicas más allá de los horizontes de la privacidad»

METAVERSO(S), PRIVACIDAD Y SEGURIDAD: ESPECTATIVAS Y ESPEJISMOS[1]

JOSÉ LUIS DOMÍNGUEZ ÁLVAREZ[2]
Personal Investigador en Formación (FPU)
Área de Derecho Administrativo
Universidad de Salamanca

«Es momento de hablar de ética y privacidad en el metaverso»
CATHY HACKL

I. ACERCAMIENTO AL METAVERSO: MÁS ALLÁ DE TEORÍAS FUTURISTAS

El vertiginoso avance digital ha encontrado su última manifestación en el metaverso[3], el cual constituye el nuevo objeto de conquista de las grandes corporaciones tecnológicas que aspiran a diseñar un mundo virtual altamente inmersivo que dibuja multitud de nuevos horizontes y posibilidades para el conjunto de la población.

La aparición de este nuevo fenómeno caracterizado por la combinación de elementos físicos y digitales permitirá a los usuarios interactuar y realizar transacciones en mundos

[1] El autor quisiera agradecer las recomendaciones y enseñanzas facilitadas por el extraordinario elenco de profesionales que componen la División de Innovación Tecnológica de la Agencia Española de Protección de Datos durante la elaboración de este trabajo, el cual se enmarca en la realización de una estancia de investigación en la citada autoridad de control independiente.

[2] Personal Investigador en Formación del Área de Derecho Administrativo de la Universidad de Salamanca. FPU17/01088, Ministerio de Educación, Cultura y Deporte y miembro del Grupo de Investigación Reconocido «Next Generation – Derecho Administrativo EU» (NEGUEDA).

[3] El metaverso no es un concepto novedoso. Para encontrar su formulación primigenia conviene remontarse hasta 1992, momento temporal en el que Neal Stephenson lleva a cabo la publicación de su novela de ciencia ficción *Snow Crash*, donde humanos y avatares interactúan en un entorno puramente virtual.

totalmente digitales, lo que constituye una importante fuente para la innovación, la creatividad o el despliegue de la economía digital[4], entre otras muchas cuestiones[5]. De igual forma, el metaverso lleva aparejado consigo el despliegue de multitud de nuevas tecnologías y productos (gafas virtuales[6], guantes hápticos[7], etc.) y la puesta en marcha de intensos procesos de recopilación, almacenamiento y utilización de datos personales de la ciudadanía, lo que a todas luces representa un nuevo desafío regulatorio y contribuirá a tensionar aún más el binomio desarrollo tecnológico-privacidad.

A este respecto, centrando nuestra atención en la esfera de la protección de datos de carácter personal son múltiples los interrogantes que plantea el despliegue de este fenómeno: ¿cumplirán estos nuevos productos inteligentes con las exigencias establecidas en la ambiciosa regulación en materia de protección de datos personales? ¿qué tipología de tratamientos de datos personales comportará este nuevo universo digital? ¿cuál será el grado de importancia y protagonismo que se confiera a la privacidad en el diseño de estos nuevos productos y servicios digitales?

Sin perjuicio de acometer iniciativas reguladoras específicas pro futuro, orientadas a embridar los claroscuros que envuelven el metaverso, y del esperado desarrollo del Paquete Digital Europeo[8], conviene recordar que la actual regulación en materia de

---

[4] Se estima que, en 2025, el metaverso global podría estar valorado en más de $280 billones de dólares.

[5] En palabras de NISA ÁVILA, "el Metaverso es una revolución social, industrial, tecnológica y sobre todo legal. El estado y sus herramientas protectoras deben evolucionar hacia una realidad que se está imponiendo y va a surgir con una fuerza que puede hacer *tambalear el Estado de derecho actual* (…) El derecho es un vertebrador social y como tal debe proteger a sus ciudadanos en cualquier ámbito o situación e impedir la dilución del Estado por una falta de adaptación de la norma a tiempos donde la tecnificación será prácticamente completa". *Vid.* NISA ÁVILA, J.A., "El Metaverso: conceptualización jurídica, retos legales y deficiencias normativas", disponible en: https://bit.ly/3OfUBkP (última consulta el 15 de junio de 2022).

[6] A este respecto recuérdese que, en 1968, Ivan Shuterland y David Evans diseñaron las primeras gafas de realidad virtual con adaptación al movimiento del usuario. Tiempo después, en 1987 Jaron Lanier y Tom Zimmerman desarrollaron el primer guante de datos creando el primer hardware y software asociado al campo de la realidad virtual háptica, o campo de datos hápticos.

[7] La aparición exponencial de dispositivos conectados que podemos usar para controlar aspectos relativos al bienestar y la salud, ha dado lugar al concepto de Internet de los Cuerpos (Internet of Bodies, IoB) o cuerpo conectado. El uso de estos dispositivos para monitorizar distintos parámetros de nuestro cuerpo tiene como resultado el tratamiento de datos biométricos y de salud con indudables ventajas, pero también implica nuevos riesgos para la privacidad y, en determinadas circunstancias, pueden llegar a comprometer la integridad física de la persona usuaria. Se puede definir conceptualmente el Internet de los Cuerpos como el uso de dispositivos conectados a Internet que monitorizan y/o actúan sobre todas o algunas de nuestras constantes vitales y otros datos biométricos, así como otros indicadores de salud como actividad física, calidad del sueño, actividad deportiva o sedentarismo. Todo esto son datos personales que van a ser analizados, explotados, almacenados, y en definitiva procesados de muy diversas formas, por diferentes personas responsables y encargadas del tratamiento. *Vid.* AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *IoT (II): Del Internet de las Cosas al Internet de los Cuerpos*, Madrid, 2021. Disponible en: https://bit.ly/3ba8YZU (última consulta el 15 de junio de 2022).

[8] Momento en el que nos encontramos nuevamente en tiempo de tribulación, en el que se está gestando no solamente el tercer acuerdo transatlántico para la transferencia de datos personales de los ciudadanos europeos entre Estados Unidos y la Unión Europea, conocido *como Trans-atlantic data privacy framework*;

protección de datos de carácter personal, presidida por el poderoso Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos —RGPD—) constituye un importante dique de contención frente a los anhelos de los gigantes tecnológicos de servirse de nuevos datos de los usuarios.

Sentada esta premisa, y partiendo de los distintos pronunciamientos de las autoridades de control europeas en la materia[9], el presente trabajo aspira a clarificar los principales

sino también los distintos hitos normativos que darán forma al esperado Paquete Digital de la Unión Europea. Junto a este hito, destacan otro conjunto de instrumentos jurídicos con los que se pretende garantizar la soberanía digital del proyecto de integración europeo e instaurar un auténtico mercado único digital, como ocurre en el supuesto concreto de la Ley de gobernanza de datos, la Ley de servicios digitales, el Reglamento sobre mercados digitales y la Estrategia de Ciberseguridad de la Unión Europea. Más allá de este conglomerado de iniciativas y transformaciones normativas se prevé, de igual forma, el despliegue de un importante volumen de inversiones e instrumentos presupuestarios necesarios para dotar de efectividad esta transición digital, incluidos los programas de cohesión, el instrumento de apoyo técnico y el Programa Europa Digital. Así mismo, cabe destacar el acuerdo de los colegisladores de que un mínimo del 20% del montante total de inversiones derivadas del Mecanismo de Recuperación y Resiliencia debe apoyar la transición digital con la finalidad de contribuir a sustentar este programa de reformas avanzando con ello en la consecución de los objetivos del Decenio Digital de Europa. *Vid.* COMISIÓN EUROPEA, *Brújula Digital 2030: el enfoque de Europa para el Decenio Digital,* Bruselas, 2021, pág. 2 [COM(2021) 118 final].

[9] A este respecto, entre otros, conviene recordar el Dictamen 8/2014 sobre la evolución reciente del Internet de las Cosas (IOT en sus siglas en inglés), donde el anterior Grupo de Trabajo del artículo 29 exponía que los principales problemas de intimidad y protección de datos derivados del uso de estos dispositivos estaban estrechamente imbricados con la falta de control y la asimetría de la información, la calidad del consentimiento del usuario, las conclusiones extraídas de los datos y readaptación del tratamiento original, la revelación invasiva de pautas de comportamiento y perfiles, las limitaciones de la posibilidad de permanecer en el anonimato cuando se hace uso de estos servicios o los riesgos para la seguridad de la información. *Vid.* GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos*, adoptado el 16 de septiembre de 2014, págs. 7-11 (WP 223).

Tiempo después, el Supervisor Europeo de Protección de Datos publicaba un informe sobre gafas inteligentes y protección de datos en el que se ponían de relieve los peligros que dichos dispositivos pueden llegar a ocasionar en lo relativo a la privacidad y protección de datos personales de los usuarios, así como de terceros: (i) falta de control de datos por parte de los usuarios y especialmente por parte de los no usuarios; (ii) imposibilidad de consentir y ser informado adecuadamente, principalmente para los no usuarios; (iii) inferencias derivadas de datos y reutilización; (iv) análisis intrusivo del comportamiento y elaboración de perfiles; (iv) limitaciones y falta de anonimato debido a la alta identificabilidad de la información que se procesa (imágenes faciales, videos, grabaciones de sonido o incluso la posibilidad de que los propios dispositivos identifiquen a las personas que están a su alcance mediante el reconocimiento facial y de voz y las señales de Wi-Fi y Bluetooth); (v) procesamiento de categorías especiales de datos, que requiere salvaguardias especiales, etc. *Vid.* EUROPEAN DATA PROTECTION SUPERVISOR, *Technology report 1: Smart glasses and data protection*, Bruselas, 2019, pág. 7. Disponible en: https://bit.ly/2AYHdOV (última consulta el 15 de junio de 2022).

Destacables resultan también, los comunicados emitidos por las autoridades de control en materia de protección de datos de Irlanda e Italia, emitidos a propósito de la puesta en marcha de Facebook View (glasses), nuevo producto que mediante el uso de controles activados por voz (dato biométrico), permite al usuario de las gafas grabar videos cortos y tomar fotos para publicar en las redes sociales. Las famosas Ray-Ban Stories comenzaron a comercializarse en España el pasado 17 de marzo de 2022. Junto a su lanzamiento, el gigante tecnológico Meta ha creado una campaña de comunicación en varios países de la

problemas que entraña el despliegue del metaverso desde el prisma de la intimidad y la protección de datos de carácter personal (licitud del tratamiento, falta de control y asimetría de la información, calidad del consentimiento del usuario, ausencia de privacidad desde el diseño y por defecto, etc.), poniendo de relieve la plena operatividad del sistema europeo de tutela jurídica de los derechos de la privacidad y la conveniencia de revigorizar el enfoque de riesgo[10] que subyace y vehicula el mismo, como presupuesto indispensable para garantizar la dignidad y seguridad de la persona en este nuevo universo digital altamente inmersivo.

II. IMPLICACIONES DEL DESPLIEGUE DEL METAVERSO PARA LOS DERECHOS DE LA PRIVACIDAD DE LA CIUDADANÍA

Como se ha apuntado con anterioridad, el metaverso ya no constituye una utopía[11], sino una realidad tangible objeto de implementación gracias al avance exponencial de aquellas

---

Unión Europea para explicar el funcionamiento de estas gafas inteligentes, al tiempo que hace un llamamiento a sus usuarios para que hagan un empleo razonable de las mismas, especificando, por ejemplo, en qué situaciones conviene no hacer uso de las capacidades que ofrecen las gafas. En otras palabras, desde la corporación tecnológica se deja a la buena voluntad de los usuarios la preservación de la privacidad, cuestión escabrosa que en el medio plazo puede dar lugar a la incoación de un nuevo procedimiento sancionador contra Meta por vulnerar —una vez más— la actual regulación europea en materia de protección de datos de carácter personal.

[10] La gestión del riesgo está formada por un conjunto de acciones ordenadas y sistematizadas con el propósito de controlar las posibles (probabilidad) consecuencias (impactos) que una actividad puede tener sobre un conjunto de bienes o elementos (activos) que han de ser protegidos. La gestión del riesgo precisa de un análisis, es decir, una reflexión crítica y objetiva de un tratamiento, requiere, por tanto, tomar decisiones que se han de plasmar en hechos concretos (controles) que minimicen el impacto sobre los activos hasta unos niveles tolerables. *Vid.* AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales,* Madrid, 2021, pág. 12.
Recuérdese a este respecto que, las normas ISO 31000:2018 e ISO 31010:2019, definen el concepto de "riesgo" como el "efecto de la incertidumbre sobre la consecución de objetivos" entendiendo como tal efecto cualquier desviación positiva o negativa sobre lo previsto inicialmente, teniendo en cuenta que los objetivos pueden ser de distinto tipo según el ámbito de actividad de una organización.
Por su parte, conviene precisar que el RGPD demanda la identificación, evaluación y mitigación, realizadas de una forma objetiva, del riesgo para los derechos y libertades de las personas en los tratamientos de datos personales (Considerandos 76 y 77, respectivamente). La mitigación ha de realizarse mediante la adopción de medidas técnicas y organizativas que garanticen y, además, permitan demostrar la protección de dichos derechos (art. 24 RGPD). Estas deberán determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento. Además, dichas medidas se revisarán y actualizarán cuando sea necesario . En definitiva, el RGPD exige un proceso de gestión del riesgo para los derechos y libertades de los interesados, que necesariamente debe estar documentado en virtud del principio de responsabilidad proactiva o "accountability" (art. 5.2 RGPD).

[11] El metaverso involucra al usuario en múltiples dimensiones, como la social, económica, política o emocional, hasta virtualizar todos los aspectos de desarrollo del individuo, y extiende los datos recogidos a la información no verbal y biométrica. La coyuntura colectiva y técnica actual ha creado el contexto ideal para su desarrollo y expansión, traduciendo las experiencias humanas a un tratamiento de datos digitales mediante simulaciones. Sin embargo, el tratamiento de estos datos personales es completamente real. *Vid.* AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Metaverso y privacidad", disponible en: https://bit.ly/3OiNMiG (última consulta el 15 de junio de 2022).

tecnologías que han permitido el despliegue de la vida virtual[12]. A este respecto, conviene señalar que la crisis sociosanitaria propiciada por la COVID-19 ha acelerado sobremanera el despliegue de servicios digitales[13], los cuales han logrado una vertiginosa penetración en todos los segmentos de la población, y en particular entre las personas más jóvenes[14].

Todas estas tecnologías se caracterizan por facilitar una interacción altamente inmersiva en espacios virtuales, que conceden al usuario una experiencia social, una identidad digital y una propiedad de activos con un mercado de intercambio. Las aplicaciones son infinitas, tantas como actividades humanas: mercados de productos digitales, descentralización de las finanzas, eliminación de intermediarios, juegos, educación, trabajo, interacción social, diseño y simulación, salud, compra de terrenos digitales, etc.

Desde el prisma de los derechos de la privacidad, la llegada del metaverso no solamente trae consigo un incremento de los procesos de recopilación, tratamiento y almacenamiento de datos personales, sino también la irrupción de nuevas metodologías de recopilación de este importante activo. En efecto, el uso del metaverso puede resultar muy intrusivo, ya que el conjunto de datos que se tratan aumenta de forma exponencial. Cualquier entorno virtual está plenamente datificado desde su diseño y permite tratar un

---

[12] Entre este conjunto de fenómenos digitales sobresalen: las tecnologías de realidad virtual (VR), aumentada (AR) y mixta (MR), o en su conjunto realidad extendida (XR); las monedas virtuales, criptomonedas y tokens; las técnicas de identidad digital; las técnicas de entidad digital o avatares, y su interacción realista que proyectan los movimientos de los usuarios y las expresiones faciales; los NFT o activos digitales (acciones, artículos de arte, juegos, entradas para eventos digitales, propiedades, terrenos…); el Internet de las cosas, wearables (gafas, cascos, guantes hápticos, joysticks, smartwatches, sensores, etc.) y los interfaces neuronales (Interfaces cerebro-computador, BCI), como fuentes de información para la interacción físico-virtual, que permiten el tratamiento de características biométricas; la Inteligencia Artificial (IA), esencial para responder al comportamiento en el mundo real, habilitar una interacción inteligente entre los usuarios y avatares, y facilitar la toma de decisiones y el perfilado; así como las infraestructuras de redes de datos distribuidas y descentralizadas como el Blockchain, el 5G, el cloud o el Edge computing.

[13] En efecto, durante los meses de restricción de la movilidad, se hizo patente la capacidad y resiliencia de las redes de telecomunicaciones para cubrir una situación extrema de súper-conectividad, con incrementos respecto a 2019 de hasta el 50% en voz fija, del 30% en voz móvil, del 20% en datos en red fija, y de un 50% en tráfico de datos móviles. También se incrementó significativamente el teletrabajo, y se impulsó la digitalización de la educación, lo que supuso de facto un cambio radical de metodologías y contenidos. De igual forma, el desarrollo de tipos de vacunas totalmente nuevos (por ejemplo, Moderna, BioNTech, etc.) ha puesto de relieve para el gran público los beneficios de una innovación disruptiva que ha permitido desarrollar vacunas en menos de un año, con eficiencia y siguiendo un método que nunca se había aplicado hasta ahora, así como la importancia de dominar estas tecnologías. *Vid.* TERRÓN SANTOS, D. y DOMÍNGUEZ ÁLVAREZ, J.L., *i-Administración pública, sistemas algorítmicos y protección de datos,* Iustel, Madrid, 2022, pág. 36.

[14] Son muchas las compañías que han apostado por el impulso de proyectos e iniciativas emprendedoras en el metaverso: PWC dispone de servicios de reunión virtual y ha adquirido terrenos virtuales, Adidas ha diseñado NFTs, Warner Music planea conciertos virtuales, el banco HSBC ha adquirido terrenos digitales para tener oficinas virtuales, Epic Games y Lego se han asociado para crear un metaverso para menores, MasterCard ha solicitado varias patentes relacionadas con NFTs y el metaverso, la Nación de Barbados se dispone a abrir una embajada diplomática virtual, etc.

espectro más amplio de información relativa a actividades humanas[15]. Todas las tecnologías que conforman el entorno del metaverso (redes sociales, IA, IoT, interfaces neuronales, etc.) tienen sus propios riesgos para la privacidad que deben ser gestionados. Pero, además, la aplicación conjunta de todas estas tecnologías puede provocar efectos individuales y sociales capaces de generar riesgos para los derechos y libertades a una escala difícil de estimar a priori[16].

Un aspecto importante a tener en cuenta es el desarrollo de metaversos sobre tecnologías que pretendan sustituir los mecanismos de regulación y gobernanza del mundo real por reglas ejecutadas automáticamente, como ya ha ocurrido en ciertas criptomonedas sobre Blockchain. Es decir, la posibilidad de desplazar al humano en el proceso de aplicación de la norma y del Derecho, y sustituirlo por algoritmos que tomen las decisiones en un entorno virtual. Por esta razón, las "leyes del metaverso" y la "gobernanza algorítmica" se tendrán que contrastar no solo con el RGPD, sino también con las nuevas y poderosas propuestas de regulación que componen el esperado Paquete Digital Europeo, como son la Digital Services Act, la Data Act, la Digital Markets Act, la Data Governance Act, o la propuesta de Reglamento por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Artificial Intelligence Act).

Otro aspecto a destacar es el tratamiento exponencial de datos biométricos. En este sentido, conviene reseñar que los datos biométricos[17] ya están disponibles a través de

---

[15] Así, sin ir más lejos, en el metaverso, podrán rastrearse los movimientos corporales, las ondas cerebrales y las respuestas fisiológicas, entre otras muchas cuestiones. En particular, puede implicar el tratamiento de nuevas categorías de datos con mayor granularidad y precisión. Sirva de ejemplo la diversidad de datos biométricos recogidos a través de los wearables o los interfaces neuronales, aunque lo más interesante es la información que se busca extraer de esos datos biométricos. Las gafas VR extraen información de las variaciones del iris, y los mandos que hacen de interfaz con el metaverso desvelan los cambios posturales, lo que permite analizar la respuesta emocional. Por su parte, los tiempos y la forma de reacción permiten estudiar biomecánicamente al individuo, y así sucesivamente. Esto, unido a los interfaces neuronales, permiten conocer y perfilar al individuo a niveles no conocidos previamente en las redes sociales. Con todo ello, se podría desvelar información de forma no deseada y que sería incluso explotable por medios automáticos. Y por supuesto, se podrían emplear con gran precisión novedosas técnicas de neuromarketing.

[16] A la luz del Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales y de la jurisprudencia del Tribunal Europeo de Derechos Humanos sobre el art. 8 del Convenio, conviene subrayar que cualquier interferencia con el derecho a la protección de datos solo podrá autorizarse si es conforme a la ley y si es necesaria, en una sociedad democrática, para proteger un interés público importante. *Cfr.* Tribunal de Justicia de las Comunidades Europeas, Sentencia de 20 de mayo de 2003 en los asuntos acumulados C-465/00, C-138/01 y C-139/01 (Rechnungshof contra Österreichischer Rundfunk y otros), Tribunal Europeo de Derechos Humanos, Sentencia de 4 de diciembre de 2008, nº 30562/04 y 30566/04 (S. y Marper contra Reino Unido) y Sentencia de 19 de julio de 2011, nº 30089/04, 14449/06, 24968/07, 13870/08, 36363/08, 23499/09, 43852/09 y 64027/09 (Goggins y otros contra Reino Unido).

[17] *Vid.* ROMEO CASABONA, C., "Datos biométricos (comentario al art. 4.14 RGPD)", *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales,* Dir. A. Troncoso Reigada, Civitas, Cizur Menor, págs. 709-712.

cascos de realidad virtual, que rastrean el entorno, los movimientos físicos y las dimensiones de un usuario cuando usa un dispositivo XR. A través de auriculares y gafas que permiten a las personas acceder al metaverso, las empresas pueden rastrear el movimiento de los ojos, en qué entornos virtuales entra una persona, qué movimientos corporales hace, cuánto tiempo permanecen en un entorno y su respuesta fisiológica a una experiencia o estímulo.

De esta forma, el acceso a estos nuevos ecosistemas digitales lleva aparejado necesariamente el diseño y uso de diferentes dispositivos de realidad virtual (VR)+, así como el despliegue de la incipiente tecnología de "eye tracking", la cual puede utilizarse para: (i) lograr una mayor inmersión y accesibilidad para personas con algún tipo de deficiencia; y (ii) conseguir un nivel de recopilación de datos personales nunca visto y con una certeza casi absoluta.

A este respecto, conviene recordar que, con carácter general, los datos biométricos[18] constituyen una categoría especial de datos personales[19]. Así, de conformidad con el art. 9.1 RGPD, queda prohibido el tratamiento de aquellos datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a

[18] Es decir, aquellos datos personales "obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" (art. 4.14 RGPD).

[19] Con el propósito de esclarecer este acalorado debate, conviene reseñar el Informe 36/2020 de la Agencia Española de Protección de Datos, en el que se esboza el siguiente planteamiento: "[n]o obstante, hay que adelantar que el RGPD no parece considerar a todo tratamiento de datos biométricos como tratamiento de categorías especiales de datos, ya que el artículo 9.1 se refiere a los «datos biométricos dirigidos a identificar de manera unívoca a una persona física», por lo que, de una interpretación conjunta de ambos preceptos parece dar a entender que los datos biométricos solo constituirían una categoría especial de datos en el caso de que se sometan a un tratamiento técnico específico dirigido a identificar de manera unívoca a una persona física [como ocurre en el supuesto concreto del metaverso]".

Con igual criterio, el Protocolo de enmienda al Convenio para la Protección de Individuos con respecto al procesamiento de datos personales, aprobada por el Comité de Ministros en su 128 periodo de sesiones en Elsinor el 18 de mayo de 2018 (Convenio 108+) incluye únicamente como categorías especiales de datos, en su artículo 6.1 a los datos biométricos dirigidos a la identificación unívoca de una persona ("biometric data uniquely identifying a person"), sin incluir la referencia a la autenticación.

Al objeto de aclarar las dudas interpretativas que surgen respecto a la consideración de los datos biométricos como categorías especiales de datos puede acudirse a la distinción entre identificación biométrica y verificación/autenticación biométrica que establecía el Grupo del Artículo 29 en su Dictamen 3/2012 sobre la evolución de las tecnologías biométrica: (a) Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios); y (b) verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno-a-uno).

identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida o la orientación sexuales de una persona física.

Lo anterior no será de aplicación cuando concurra alguna de las siguientes circunstancias (art. 9.2 RGPD): (i) el interesado haya manifestado su consentimiento explícito; (ii) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento; (iii) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; (iv) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro; (v) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos; (vi) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial; (vii) el tratamiento es necesario por razones de un interés público esencial, etc.

Conviene precisar, por tanto, cuál será la base de legitimación empleada por las grandes corporaciones tecnológicas para esquivar la prohibición general de proceder al tratamiento de datos biométricos[20]. Esta cuestión es especialmente sensible, como pone de relieve el procedimiento sancionador PS/00120/2021instruido recientemente por la Agencia Española de Protección de Datos frente al uso preventivo de datos biométricos por parte de una gran cadena de supermercados.

Ahora bien, más allá de las pretensiones de sustitución de los mecanismos de regulación y gobernanza del mundo real, y el incremento exponencial del tratamiento de datos biométricos por parte de los grandes gigantes tecnológicos, el metaverso entraña otra serie de riesgos y desafíos derivados de la monitorización y procesamiento de las preferencias y los comportamientos de los usuarios, los cuales pueden individualizarse y remitirse al usuario en cuestión en forma de campañas de publicidad personalizadas. Este fenómeno conocido como segmentación publicitaria o microtargeting puede ser especialmente peligroso para la pervivencia de nuestras sociedades tal y como las concebimos

[20] Para ello, el responsable del tratamiento ha de determinar si el mismo y sus mecanismos, las categorías de datos que deben recogerse y tratarse, así como la transferencia de la información contenida en la base de datos, son necesarios e indispensables. Las medidas de seguridad adoptadas deben ser adecuadas y eficaces. El responsable del tratamiento ha de considerar los derechos que deben concederse a las personas a que se refieren los datos personales, y garantizar que a la aplicación se incorpore un mecanismo apropiado para ejercer tales derechos. *Vid.* GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Dictamen 3/2012 sobre la evolución de las tecnologías biométricas*, adoptado el 27 de abril de 2012, pág. 9 (WP193).

actualmente. Sirva de ejemplo el supuesto concreto de Cambridge Analytica[21], entidad empresarial que llegó a acaudalar datos de más de 230 millones de votantes en los Estados Unidos con el propósito de elaborar perfiles sociodemográficos empleados para pronosticar e incidir en el comportamiento de los votantes[22]. Junto a estas amenazas se vislumbran igualmente otra serie de riesgos, como pueden ser la aparición de nuevas e intensas fórmulas de vigilancia masiva de la sociedad[23], la acentuación del fraude en el entorno digital o el incremento exponencial de los supuestos de suplantación de identidad[24].

III. EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS FRENTE A LOS CLAROSCUROS DEL METAVERSO

Como es sabido por todos, en la actualidad, el régimen jurídico encargado de la tutela efectiva del derecho fundamental a la protección de datos de carácter personal comprende el Reglamento 679/2016 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), y se complementa con las disposiciones contenidas en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), además de toda aquella normativa de carácter sectorial publicada antes y después de la entrada en vigor del Reglamento europeo[25].

Esta poderosa regulación, proporciona una extraordinaria flexibilidad para poder garantizar y demostrar la adecuación de un tratamiento de datos a la norma[26]. Sin

---

[21] Como consecuencia del escándalo internacional con respecto a las estrategias de procesamiento de datos que desarrollaba esta empresa, Cambridge procedió al cierre táctico de la organización.

[22] *Vid.* GONZÁLEZ DE LA GARZA, L.M., "La crisis de la democracia representativa. Nuevas relaciones políticas entre democracia, populismo virtual, poderes privados y tecnocracia en la era de la propaganda electoral cognitiva virtual, el microtargeting y el Big Data", *Revista De Derecho Político*, vol. 1, núm. 103, 2018, págs. 283-284.

[23] Nos encontramos a las puertas de una suerte de corporativismo vigilante, la renovada versión de la primigenia "actividad informativa estatal de acopio de datos". *Cfr.* RIVERO ORTEGA, R., *El Estado vigilante: consideraciones jurídicas sobre la función inspectora de la Administración*, Tecnos, Madrid, 1999.

[24] Durante los últimos 20 años, las aplicaciones de carácter social han sido los principales motores de la evolución de los entornos digitales. Los usuarios tienden a compartir cada vez más aspectos de su vida y, además, cada vez en más servicios y sitios web. En la actualidad, es frecuente transmitir en directo la vida, las conexiones, los pensamientos, los conocimientos, las relaciones, las opiniones, etc. Por otro lado, los usuarios usan cada vez más dispositivos para conectarse a la red, lo que también complementa la información sobre la identidad digital del individuo. *Cfr.* FUNDACIÓN TELEFÓNICA, *Identidad Digital: El nuevo usuario en el mundo digital,* editorial Ariel, Madrid, 2013, pág. 9.

[25] *Vid.* PIÑAR MAÑAS, J.L., "Reglamento Europeo de Protección de Datos: retos y oportunidades para la abogacía", *Abogados: Revista del Consejo General de la Abogacía*, núm. 98, 2016, págs. 26-29.

[26] *Vid.* AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Listado de cumplimiento normativo*, Madrid, 2018. Disponible en: https://bit.ly/3pUtp1K (última consulta el 15 de junio de 2022).

embargo, hay un conjunto mínimo de condiciones *sine qua non* que deben cumplirse para garantizar que el tratamiento de datos personales empleado para desarrollar soluciones tecnológicas innovadoras[27], es conforme a la vigente regulación europea. El metaverso no es una excepción, habida cuenta de que la protección de datos es un pilar fundamental, tanto para las empresas, como para los desarrolladores tecnológicos y los propios usuarios a la hora de interactuar en este nuevo entorno digital altamente inmersivo[28].

Por esta razón, los gigantes tecnológicos que comienzan a orientar su actuación al despliegue del metaverso no escapan del ámbito de actuación de la normativa diseñada con el propósito de garantizar la tutela jurídica de la protección de datos personales y deberán disponer, como mínimo, de la capacidad de demostrar el estricto cumplimiento de las siguientes exigencias contempladas en el texto articulado del RGPD antes de iniciar su actividad.

1. Principios de privacidad que deben orientar el tratamiento de datos

El tenor literal de la actual regulación europea de los derechos de la privacidad, es claro al señalar que todo tratamiento llevado a cabo por el responsable o encargado del tratamiento deberá realizarse de manera lícita[29], legal y transparente. A tal fin, el art. 5 RGPD preceptúa que los datos deberán ser recogidos con fines determinados, explícitos y legítimos, debiendo ser además adecuados, pertinentes y limitados acorde a las finalidades detalladas[30]; siendo exactos, confidenciales, y definiendo los correspondientes plazos de conservación (art. 5 RGPD). Aplicar escrupulosamente los

---

[27] *Vid.* CASEY, A.J. Y NIBLETT, A., "Focus feature: Artificial Intelligence, Big Data, and the future of law", en *University of Toronto, Law Journal*, *vol. 66*, núm. 4, 2016, págs. 423-442.

[28] Consciente de esta realidad, el legislador europeo ha articulado una enérgica respuesta punitiva para combatir la inobservancia de las previsiones contempladas en la actual normativa de protección de datos. Sin ir más lejos, el art. 83 RGPD contempla la posibilidad de que toda empresa, como responsable o encargado de tratamiento pueda llegar a ser sancionada con multas de hasta el 4% de la facturación anual o de 20 millones de euros dependiendo de la infracción según la naturaleza, gravedad, duración de la infracción, intencionalidad y medidas adoptadas, entre otros factores.

[29] Para comprender el principio de tratamiento lícito, debemos hacer referencia a las condiciones de las limitaciones lícitas del derecho a la protección de los datos, a la luz del artículo 52, apartado 1, de la Carta de Derechos Fundamentales de la Unión Europea, así como a los requisitos de las injerencias justificadas, de conformidad con el artículo 8, apartado 2, del Convenio Europeo de Derechos Humanos. De este modo, el tratamiento de datos personales será lícito únicamente si: se realiza de conformidad con la ley; sirve a un fin legítimo; y es necesario en una sociedad democrática para lograr el fin legítimo.

[30] Es decir, los tratamientos de datos deberán tener unos fines determinados, explícitos y legítimos, y no deberán tratarse ulteriormente con otros fines, a excepción de determinadas finalidades declaradas compatibles, como son su archivo en interés público, la investigación científica e histórica o finalidades estadísticas. En torno a esta última cuestión, resulta especialmente clarificador GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Dictamen 3/2013 sobre la limitación a una finalidad específica,* adoptado el 2 de abril de 2013, 31 págs. (WP 203).

principios relativos al tratamiento en el metaverso se convierte, por tanto, en una cuestión de imperiosa necesidad.

Igualmente relevante resulta la aplicación del principio de responsabilidad proactiva[31] (arts. 24 al 43 RGPD) que establece la necesidad de incorporar una serie de garantías adicionales, más allá de un mínimo, documentadas y orientadas a gestionar el riesgo para los derechos y libertades de los individuos. En particular, la necesidad de apostar por el establecimiento de medidas de privacidad desde el diseño y por defecto (art. 25 RGPD), la obligación de mantener un registro de actividades de tratamiento (art. 30 RGPD), o la necesidad de efectuar una evaluación de impacto sobre la protección de datos con carácter previo al inicio del tratamiento cuando se traten datos personales utilizando nuevas tecnologías que, por su naturaleza, alcance, contexto o fines, entrañen un alto riesgo para los derechos y libertades de las personas (art. 35 RGPD), entre otras muchas cuestiones.

2. Licitud del tratamiento de datos

La existencia de una base normativa que garantice la legitimación del tratamiento de datos personales (arts. 6 al 11 RGPD) es otra de las exigencias indiscutibles que debe guiar cualquier proceso de desarrollo tecnológico conducente al impulso del metaverso. En este sentido, el establecimiento de una base jurídica legitimadora es el primer paso para determinar el cumplimiento de cualquier solución tecnológica con el RGPD. Si no se encuentra una base legitimadora (art. 6 RGPD) no se debe realizar el tratamiento de datos de carácter personal para no incurrir en una vulneración de los derechos y libertades fundamentales de la ciudadanía.

Previsiblemente, las bases jurídicas en la que se escudarán las grandes corporaciones tecnológicas dispuestas a conquistar el metaverso para justificar las diferentes operaciones de tratamiento de datos será:

---

[31] Este principio implica que el responsable del tratamiento tiene que garantizar la licitud, la lealtad y la transparencia en todo el proceso del tratamiento de datos con relación al interesado. Pero su responsabilidad no termina aquí, toda vez que el legislador le impone a dicho responsable la obligación de poder acreditar que efectivamente dicho tratamiento ha reunido las características especificadas en el apartado 5.1 RGPD. *Vid.* PUYOL MONTERO, J., "Los principios del derecho a la protección de datos", *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad*, Dir. J.L. Piñar Mañas, editorial Reus, Madrid, 2016, pág. 140. Esta cuestión, la cual constituye, junto al enfoque de riesgo, la gran piedra angular del nuevo modelo europeo de la tutela jurídica de los derechos de la privacidad ha sido abordada por los principales expertos en la materia. Entre otros, *vid.* RALLO LOMBARTE, A. "El nuevo derecho de protección de datos", *Revista Española de Derecho Constitucional,* núm. 11, 2019, pág. 49; MARTÍNEZ MARTÍNEZ, R., "El principio de responsabilidad proactiva y la protección de datos desde el diseño y por defecto", *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales*, Eds. R. García Mahamut y B. Tomás Mallén, Tirant Lo Blanch, Valencia, 2019, pág. 317, etc.

a) El interés legítimo[32] de las respectivas entidades empresariales. Sin embargo, en este punto, conviene recordar que la base de legitimación del interés legítimo no es el bálsamo de fierabrás empleado por el intrépido hidalgo cervantino, toda vez que adolece de una serie de limitaciones conceptuales[33], en la medida en que dichos intereses (no basta con la simple conveniencia o la maximización del rédito económico corporativo) están supeditados a los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un menor de edad.

b) El consentimiento de los interesados, que, como establece el art. 4.11 RGPD, es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen[34].

c) Que el tratamiento sea necesario para la ejecución de un contrato en el que el interesado es parte, o para la aplicación de medidas precontractuales a petición de este. Podría ser el caso de desarrolladores que contraten a sujetos para hacer uso de sus datos personales en la etapa de entrenamiento del sistema. También podría ser que el responsable del tratamiento, y que proporciona un servicio a terceros interesados que incluye la solución de IA, utilizara los datos de estos en el marco del contrato del servicio[35].

3. Establecimiento de mecanismos de gobernanza del metaverso que garanticen el ejercicio de los derechos subjetivos de los interesados

[32] El carácter abierto de este fundamento jurídico plantea muchas cuestiones importantes relativas a su aplicación y alcance exactos. Sin embargo, "esto no significa necesariamente que esta opción deba considerarse como aquella que puede utilizarse con moderación únicamente para cubrir las lagunas en situaciones raras o imprevistas como «un último recurso», o como una última posibilidad si no se pueden utilizar otros fundamentos. Tampoco deberá percibirse como una opción preferente ni deberá extenderse su uso de manera indebida porque se considere menos restrictiva que los demás fundamentos". *Vid.* GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE*, adoptado el 9 de abril de 2014, pág 11 (WP 217).

[33] Esta controvertida figura ha sido magistralmente analizada por GIL GONZÁLEZ, E., *El interés legítimo en el tratamiento de datos personales,* Wolters-Kluwer, Madrid, 2022, 408 págs.

[34] Asimismo, deberá tenerse en cuenta especialmente, tal y como se indica en el Informe 36/2020 de la Agencia Española de Protección de Datos, que el consentimiento debe ser libre, señalando el Considerando 42 del RGPD que "[e]l consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno".

[35] No podrían emplearse las restantes bases jurídicas contempladas en el art. 6 RGPD, es decir, escudarse en la protección de intereses vitales, la existencia de razones de interés público o ejercicio de poderes públicos o el cumplimiento de obligaciones legales.

Taxativamente, debe cumplirse la obligación de informar a los sujetos de los datos y fomentar la transparencia de los distintos tratamientos[36] (arts. 12 al 14 RGPD). La información que cada responsable ha de proporcionar a los interesados se establece en los arts. 13 y 14 RGPD, y el contenido concreto se tendrá que adaptar a las particularidades del entorno virtual en cuestión y las herramientas digitales empleadas para la realización de los diferentes tratamientos de datos personales. No obstante, conviene precisar que el art. 11 LOPDGDD establece la posibilidad de que el responsable ofrezca esta información mediante una aproximación por capas o niveles: una primera capa, de carácter general, con información básica del tratamiento[37]; y una segunda capa que completa la información de la primera con mayor nivel de detalle y que sea accesible desde esta de forma fácil e inmediata, incluso por medios electrónicos.

Paralelamente, es pertinente dar cumplimiento a la obligación de proporcionar a los sujetos de los datos mecanismos para el ejercicio de sus derechos subjetivos[38]. Los

---

[36] Según el Considerando 78 RGPD , el principio de transparencia es una medida de privacidad por defecto para permitir, entre otros, que los interesados puedan supervisar el tratamiento al que están sometidos. El principio de transparencia se desarrolla en los Considerandos 39 y 58 RGPD. En estos Considerandos se interpreta la obligación de información a los interesados de un modo que va más allá de lo dispuesto en la letra de los arts. 13 y 14 RGPD. En particular, los Considerandos comentan la obligación de que "toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender", "sea concisa", "se utilice un lenguaje sencillo y claro", que "en su caso, se visualice", que "podría facilitarse en forma electrónica", que se proporcione "información añadida para garantizar un tratamiento leal y transparente" y que los interesados "deben tener conocimiento de los riesgos, las normas, las salvaguardias" del tratamiento.
En el caso de tratamientos basados en IA, la transparencia puede ser considerada un aspecto crítico. Debe permitir a los interesados ser conscientes del impacto que el empleo de dichas soluciones puede llevar asociado. De ahí que la transparencia esté dirigida tanto a los interesados como a los operadores del tratamiento. En particular, la transparencia está ligada con una información veraz sobre la eficiencia, las capacidades y las limitaciones reales de los sistemas de IA, que evite la creación de falsas expectativas, en los usuarios y los interesados, que puedan ocasionar una mala interpretación de las inferencias que se realizan en el marco del tratamiento. *Vid.* AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Guía para la adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción,* Madrid, 2020, pág. 33.
La transparencia no se reduce a un instante puntual, sino que debe ser entendida como un principio en torno al que orbita de forma dinámica el tratamiento realizado y que afecta a todos y cada uno de los elementos y participantes que intervienen en la solución.

[37] Así, en la primera capa deberá consignarse la siguiente información referente a: (i) la identidad del responsable del tratamiento o de su representante; (ii) la finalidad del tratamiento; (iii) la posibilidad de ejercer los derechos 15 al 22 RGPD; (iv) el tratamiento incluye la elaboración de perfiles o decisiones automatizadas; (v) si los datos personales objeto del tratamiento no han sido obtenidos directamente del afectado, la información básica incluirá también: las categorías de datos objeto de tratamiento y las fuentes de las que procedieran los datos, etc. Por su parte, en la segunda capa, debe figurar la estante información contenida en los arts. 13 y 14 RGPD.

[38] *Vid.* ÁLVAREZ CARO, M., "El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas", *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad*, Dir. J.L. Piñar Mañas, editorial Reus, Madrid, 2016, págs. 227-240. En torno a esta cuestión, igualmente destacable ADSUARA VARELA, B., "Derechos de rectificación, supresión (olvido) y portabilidad de los datos", *Tratado de protección de datos. Actualizado con la Ley*

responsables que hagan uso de soluciones de inteligencia artificial para tratar datos personales, elaborar perfiles o tomar decisiones automatizadas, han de ser conscientes de que los interesados tienen derechos en el ámbito de la protección de datos que deben ser atendidos (arts. 15 al 23 RGPD).

Por lo tanto, durante la fase de concepción del tratamiento, los responsables han de ser conscientes de que tienen que establecer mecanismos y procedimientos adecuados para poder atender las solicitudes que reciban, y que dichos mecanismos deberán estar adecuadamente dimensionados para la escala del tratamiento que están efectuando.

4. Privacidad desde el diseño y por defecto

El responsable del tratamiento deberá aplicar, tanto a la hora de determinar los medios de tratamiento como en el momento del propio tratamiento, es decir, «desde el diseño[39]», medidas técnicas y organizativas apropiadas, e integrar las garantías necesarias en el tratamiento, a fin de cumplir eficazmente las obligaciones legales y proteger los derechos de las personas afectadas (art. 25.1 RGPD).

Asimismo, promoverán la aplicación de las medidas técnicas y organizativas apropiadas para garantizar que, «por defecto[40]», solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad (art. 25.2 RGPD).

5. Seguridad de la información

Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y Garantía de los Derechos Digitales, Coord. A. Rallo Lombarte, Tirant lo Blanch, Valencia, 2019, págs. 313-352.

[39] La idea de "protección de datos desde el diseño" existe desde hace más de 20 años y se ha trabajado intensamente en ella bajo la terminología de "privacidad desde el diseño" (*Privacy by Design,* PbD). Este concepto fue desarrollado por la Comisionada de Protección de Datos de Ontario, Ann Cavoukian, en la década de los 90; presentado en la XXXI Conferencia Internacional de Comisionados de Protección de Datos y Privacidad del año 2009 bajo el título *"Privacy by Design: The Definitive Workshop"* y aceptado internacionalmente en la XXXII Conferencia Internacional de Comisionados de Protección de Datos y Privacidad, celebrada en Jerusalén en el año 2010, con la aprobación de la "Resolución sobre la Privacidad por Diseño". Implica utilizar un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva para establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso). *Vid.* AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Guía de Privacidad desde el Diseño*, Madrid, 2019, pp. 5-6. Disponible en: https://bit.ly/3t4e2Wx

[40] De conformidad con el l documento "*Guidelines 4/2019 on Article 25 Data Protection by Design and by Default"*, el Comité Europeo de Protección de Datos manifiesta en el apartado 2.2 "Protección de datos por defecto" que la Protección de Datos por Defecto (PDpD) hace referencia a las elecciones realizadas con respecto a los valores de configuración u opciones de tratamiento fijadas en los sistemas y procedimientos que implementan el tratamiento y que determinan la cantidad de los datos personales recopilados, el alcance de su procesamiento, el periodo de su conservación y su accesibilidad. *Vid.* AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Guía de protección de Datos por Defecto,* Madrid, 2020, p. 5. Disponible en: https://bit.ly/3F3ukRO

El responsable del tratamiento de los datos personales deberá garantizar la seguridad de la información de los usuarios que se aventuren a introducirse en el metaverso. Por ello, con la finalidad de que el derecho a la seguridad digital se aplique de forma efectiva, el tratamiento de los datos de los usuarios se debe realizar en base a los principios de confidencialidad, integridad y disponibilidad. Esta premisa se refleja en el art. 32 RGPD, el cual impone a los responsables de los tratamientos de datos personales la obligación de determinar y establecer las medidas de seguridad técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo[41] en función del estado de la técnica, los costes de aplicación y, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas[42]; y que *«en su caso incluya, la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento»*[43]:

---

[41] En torno a esta cuestión se ha pronunciado recientemente la Sentencia 188/2022 dictada por la Sala tercera del Tribunal Supremo, mediante la que se resuelve el recurso de casación interpuesto por Commcenter, S.A., empresa distribuidora oficial de Movistar, y se confirma la sanción impuesta por la Agencia Española de Protección de Datos por infracción del artículo 9.1 de la ya derogada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Dicho pronunciamiento señala que "[l]a obligación de adoptar las medidas necesarias para garantizar la seguridad de los datos personales no puede considerarse una obligación de resultado, que implique que producida una filtración de datos personales a un tercero exista responsabilidad con independencia de las medidas adoptadas y de la actividad desplegada por el responsable del fichero o del tratamiento". A tal efecto recuerda que en el caso de las "obligaciones de resultado" existe un compromiso consistente en el cumplimiento de un determinado objetivo, asegurando el logro o resultado propuesto, en este caso garantizar la seguridad de los datos personales y la inexistencia de filtraciones o quiebras de seguridad. En las "obligaciones de medio", en cambio, el compromiso que se adquiere es el de adoptar los medios técnicos y organizativos, así como desplegar una actividad diligente en su implantación y utilización que tienda a conseguir el resultado esperado con medios que razonablemente puedan calificarse de idóneos y suficientes para su consecución, por ello se las denomina obligaciones "de diligencia" o "de comportamiento" (FD3).

[42] A fin de mantener la seguridad de los tratamientos se exige al responsable evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos. En dicha evaluación del riesgo deben tenerse en cuenta los riesgos que atenten contra los derechos y libertades de los interesados, especialmente sus derechos y libertades fundamentales.

Con el objetivo de seleccionar las medidas para gestionar el riesgo para los derechos y libertades, pueden utilizarse estándares de seguridad ya existentes en el mercado como la norma ISO 27000. Por su parte, las Administraciones públicas deberán utilizar el Esquema Nacional de Seguridad para seleccionar las medidas que deban implantarse para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos. *Vid.* AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales,* Madrid, 2021, p. 15.

[43] En lo que se refiere a la seguridad de las comunicaciones, ya el Considerando 39 RGPD afirmaba que el tratamiento que se haga de datos personales debe hacerse de un modo *«que garantice una seguridad y confidencialidad adecuadas»* de tales datos, lo que incluye cualquier tipo de actuaciones dirigidas a impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento. En este mismo sentido el Considerando 83, al tratar la evaluación de riesgos en relación con la seguridad de los datos durante su tratamiento, afirma que las medidas que el responsable o el encargado aplique para mitigar dichos riesgos deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad. Y se refiere, a modo de ejemplo, al cifrado de la información como una práctica efectiva a tal fin.

A. Confidencialidad. Se basa en la protección de los datos de los usuarios en los entornos virtuales, con el objetivo de preservar su privacidad digital. Los responsables de tratamiento o proveedores de servicios han de garantizar que no se revelarán los datos confidenciales del usuario y que no se cederán a terceros sin su consentimiento explícito.

B. Integridad. Se refiere a la protección de los datos frente a cualquier modificación, alteración o acceso ilegítimo por parte de terceros. El objetivo es asegurar que la información que circule en el metaverso sea veraz. Uno de los nuevos derechos digitales que incluye la LOPDGDD y que tiene que ver con la integridad de la información es el derecho al olvido[44], que consiste en el derecho del usuario a solicitar la eliminación de aquellos datos presentes en buscadores o redes sociales que sean inexactos, falsos o estén desactualizados.

C. Disponibilidad. Tiene que ver con el derecho de los usuarios a que sus datos personales estén disponibles en todo momento para ejercer sus derechos subjetivos de acceso, rectificación, supresión, limitación, portabilidad y oposición (ARSULIPO).

Con el propósito de establecer incentivos para los prestadores de servicios digitales en aras de garantizar el estricto respeto de estos elementos vehiculares del derecho a la seguridad digital, la propia regulación en materia de protección de datos tipifica el quebranto de tales principios axiomáticos como una infracción de carácter grave, como se desprende del tenor literal del art. 73.f) RGPD, según el cual, se consideran graves y prescribirán a los dos años las infracciones que supongan *«[l]a falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el*

[44] El derecho al olvido, un derecho cuya denominación ha sido puesta en entredicho en multitud de ocasiones por no ajustarse a la realidad o a su significado propiamente dicho, trae causa de la Sentencia del Tribunal de Justicia de la Unión Europea, de 13 de mayo de 2014, en el caso Mario Costeja/AEPD v. Google (C-131/12), concluyendo que existe un derecho a la desindexación de enlaces en motores de búsqueda, en determinadas circunstancias, con independencia de que la publicación de la información en la fuente de origen sea lícita, lo que se conoce como una de las grandes conquistas de las autoridades de control en la historia reciente frente al omnímodo poder de los gigantes tecnológicos. En torno a esta cuestión, fruto de su importancia capital, existe una abundante bibliografía: DE TERWANGNE, C., "Privacidad en Internet y el derecho a ser olvidado/derecho al olvido", *IDP. Revista de Internet, Derecho y Política,* núm. 13, 2012, págs. 53-66; SIMÓN CASTELLANO, P., El régimen constitucional del derecho al olvido digital, Tirant lo Blanch, Valencia, 2012, 254 págs.; ÁLVAREZ CARO, M., *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital,* editorial Reus, Madrid, 2015, 144 págs.; PLATERO ALCÓN, A., "El derecho al olvido en Internet. El fenómeno de los motores de búsqueda", *Opinión Jurídica*, vol. 15, núm. 29, 2016, págs. 243-260, etc.

artículo 32.1 del Reglamento (UE) 2016/679». En este punto, conviene recordar que el art. 83.4 RGPD impone que la infracción de tales disposiciones se sancionarán con multas administrativas de 10.000.000 euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

6. Evaluación de Impacto sobre la Privacidad

El art. 35 RGPD establece que, cuando un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales (EIPD). El Reglamento determina algunos de los casos en que se presumirá que existe ese alto riesgo, supuestos entre los que se encuentran la evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se basen en un tratamiento automatizado de datos, como ocurre ante la elaboración de perfiles, el tratamiento a gran escala de categorías especiales de datos o datos personales relativos a condenas e infracciones penales, entre otras cuestiones[45].

La EIPD es un proceso que se integra en el propio proceso de gestión de riesgos para los derechos y libertades. Dentro de ese proceso de gestión, un aspecto importante de la EIPD es su carácter a priori, es decir, la obligación de ejecutarla antes del inicio de las actividades de tratamiento[46].

El RGPD incide en este carácter previo con relación a la ejecución efectiva del tratamiento. Explícitamente, no exige que se haya de realizar con carácter previo a otras etapas del ciclo de vida del tratamiento, como podrían ser su diseño o implementación. De esta forma, el RGPD se limita al ejercicio de sus competencias, es decir, no entra a valorar otras consideraciones que vayan más allá de la protección de datos de carácter personal. Los derechos y libertades de los ciudadanos se verán afectados cuando el

[45] El RGPD prevé que las autoridades nacionales de protección de datos publiquen listas de otros tratamientos de alto riesgo. También contempla un contenido mínimo de las Evaluaciones de Impacto.

[46] Atendiendo a las "Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679" del Comité Europeo de Protección de Datos, la ejecución de una EIPD no es un mero requisito de cumplimiento formal, sino que, es "un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales evaluándolos y determinando las medidas para abordarlos", proceso que se aplica al ciclo completo de vida del tratamiento y no solamente a un momento concreto del mismo.

tratamiento se ejecute de forma efectiva, por lo tanto, es antes de que se vean comprometidos dichos derechos y libertades cuando debe realizarse la EIPD.

Sin embargo, y aunque el RGPD no entra en la valoración, sería altamente recomendable que la entidad lleve a cabo la EIPD antes de iniciar el proceso de diseño e implementación efectiva[47]. Toda fase del ciclo de vida de desarrollo de un tratamiento previo a la puesta en explotación del mismo supone realizar inversiones para llevar a cabo desarrollos, adquisiciones, cambios organizativos, contrataciones, etc. En este sentido, las Directrices WP248 se expresan literalmente en los siguientes términos: *"[l]a EIPD debe percibirse como un instrumento de ayuda en la toma de decisiones relativas al tratamiento"*.

De donde se deduce que la EIPD es recomendable realizarla en las fases de concepción y diseño del tratamiento. Existen dos razones que aconsejan esta aproximación. La primera es la de proteger la inversión realizada por el responsable en el tratamiento, pero esta razón no entra dentro de las competencias de protección de datos. La segunda es para cumplir con los principios de protección de datos desde el diseño[48].

IV. LA IMPORTANCIA DE LA ÉTICA DIGITAL PARA SALVAGUARDAR LOS DERECHOS Y LIBERTADES FUNDAMENTALES DE LA CIUDADANÍA EN LOS ENTORNOS VIRTUALES ALTAMENTE INMERSIVOS

Cuando hablamos de ética digital nos referimos al código social necesario para solucionar los problemas que el uso de las tecnologías disruptivas está ocasionando en múltiples esferas, tales como el derecho de propiedad intelectual, los ciberataques a la seguridad, los límites a la libertad de expresión, la regulación de las grandes corporaciones, la desconexión digital, la conducta en redes sociales y la privacidad de nuestros datos personales[49].

---

[47] Con el propósito de facilitar que los responsables del tratamiento dispongan de instrucciones precisas para poder desarrollar una EIPD con las máximas garantías, recientemente la Agencia Española de Protección de Datos ha presentado una lista de verificación para identificar y determinar de una forma rápida si el proceso y la documentación que están empleando para llevar a cabo una Evaluación de Impacto en la Protección de Datos contiene los elementos exigidos por el actual marco normativo europeo. *Vid.* AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Lista de verificación para determinar la adecuación formal de una EIPD y la presentación de consulta previa*, Madrid, 2022. Disponible en: https://bit.ly/3aX2NIn (última consulta el 15 de junio de 2022).

[48] El RGPD establece y tipifica infracciones en el caso de ausencia o falta de adecuación del desarrollo de la EIPD cuando sea preciso llevarla a cabo. Concretamente, el RGPD establece en el artículo 83.4 que las infracciones a los artículos 35 "Evaluación de Impacto relativa a la Protección de Datos" y 36 "Consulta Previa" se sancionarán con multas administrativas de 10.000.000€ como máximo o, tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

[49] El uso de tecnologías emergentes puede suponer un riesgo latente para los derechos y libertades de las personas en su concreta aplicación a, digamos, datos especialmente sensibles como los datos de salud. Por su propia naturaleza, "estos datos van más allá de los propios individuos, sino también a su grupo familiar,

Por ello, es preciso estar vigilantes y realizar un seguimiento tanto de la legitimidad ética de los tratamientos como de los efectos inesperados de estos[50]. Asimismo, debe considerarse el posible impacto colateral[51] de dichos tratamientos en un entorno social, más allá de las limitaciones concebidas inicialmente de propósito, de duración en el tiempo y de extensión.

Resulta, pues, necesaria la toma de decisiones de ética digital anticipando aquellos escenarios que puedan generar riesgos[52] para la privacidad y los derechos y libertades fundamentales restantes, prestando especial atención al potencial que poseen estas tecnologías emergentes, al combinarlas con actuaciones de tratamiento masivo de datos personales y técnicas de Big Data, para permitir la reidentificación de los individuos e invadir la esfera personal de la ciudadanía[53].

---

incluso de colectivos más amplios relacionados social, cultural o étnicamente. Por las técnicas necesarias para su procesamiento solo unos pocos y grandes operadores están en condiciones de su tratamiento, lo cual puede generar una concentración de conocimiento y, por tanto, poder, que acentuará el desequilibrio no solo entre estos grandes operadores y los interesados, sino quizás también entre aquellos y la sociedad. Es importante considerar a los interesados como personas, sujetos de derechos, y no solo como usuarios o consumidores. Las tendencias actuales para favorecer el mercado único digital, pueden conducir a aumentar los riesgos de los tratamientos masivos para las personas, precisamente por el carácter impredecible y disruptivo que tienen las tecnologías emergentes, lo cual hace que las protecciones legales pueden llegar a ser insuficientes si han de enfrentarse a nuevas situaciones y supuestos, para los cuales no estaban diseñadas (…) Por eso es importante, también, introducir un enfoque ético, centrado en los tratamientos basados en tecnologías emergentes, que sitúe la dignidad humana en el centro de la ecuación". *Vid.* ALBERTO GONZÁLEZ, P., "Responsabilidad proactiva en los tratamientos masivos de datos", *Dilemata,* núm. 24, 2017, págs. 127-128.

[50] Un aspecto crítico de los sistemas de IA es el de la posible existencia de sesgos. Un sesgo ("bias" en inglés) es una desviación inadecuada en el proceso de inferencia. Los sesgos son particularmente graves cuando, por ejemplo, derivan en discriminaciones de un grupo en favor de otro. Esta problemática ya fue señalada por FRIEDMAN y NISSENBAUM: «systematically and unfairly discriminate against certain individuals or groups of individuals in favor of others. A system discriminates unfairly if it denies an opportunity or a good or if it assigns an undesirable outcome to an individual or group of individuals on grounds that are unreasonable or inappropriate». *Vid.* FRIEDMAN, B. y NISSENBAUM, H., "Bias in computer systems", *ACM Transactions on Information Systems*, vol. 14, núm. 3, 1996, págs. 330-347.

[51] *Vid.* O´NEIL, C., *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy,* Broadway Books, Portland, 2016, 259 págs.

[52] La anteriormente citada norma ISO-3100 "Gestión del Riesgo. Principios y Directrices" expone en el apartado 5.5 relativo al "Tratamiento del Riesgo" las condiciones generales para la gestión del riesgo en cualquier tipo de ámbito: "La selección de la opción más apropiada de tratamiento del riesgo implica obtener una compensación de los costes y los esfuerzos de implementación en función de las ventajas que se obtengan, teniendo en cuenta los requisitos legales, reglamentarios y de otro tipo, tales como la responsabilidad social y la protección del entorno natural. Las decisiones también se deberían tomar teniendo en cuenta los riesgos cuyo tratamiento no es justificable en el plano económico, por ejemplo, riesgos severos (consecuencias altamente negativas) pero raros (baja probabilidad)".

[53] En este sentido, como recuerda COTINO HUESO, desde la perspectiva ética no son pocas las consideraciones y cuestiones que disponen de un carácter esencial, a saber: "las relativas al control humano a la autonomía artificial, la interactuación incluso emocional de seres humanos y robots, la responsabilidad, el rediseño institucional (gobernanza, regulación, diseño, desarrollo, inspección, monitoreo, pruebas y certificación), la zona gris entre el impulso o la sutil manipulación (*nudging*) hasta la manipulación, la explicabilidad y transparencia de la IA, los límites a los sistemas de puntuación social (*social scoring*), el perfilado humano sin consentimiento, la vigilancia masiva o los sistemas de IA encubiertos amén del uso de sistemas letales de armas autónomas, etc.". *Vid.* COTINO HUESO, L., "Ética en el diseño para el

Para ello, como ha insistido en señalar en diversos foros la Agencia Española de Protección de Datos se considera una práctica recomendable fomentar la formación en ética y privacidad de los distintos agentes implicados en los procesos de desarrollo tecnológico, en especial cuando nos encontramos ante el diseño e implementación de sistemas algorítmicos, así como impulsar la alfabetización digital con carácter transversal. En particular, los nuevos desarrolladores tecnológicos deberían tener especialmente en cuenta las siguientes ideas-fuerza[54]:

a) Impulsar la mayor transparencia posible para que los usuarios y usuarias conozcan qué datos se están recabando, cuándo se registran y para qué se emplean. Para alcanzar un nivel significativo de transparencia, los interesados deberán disponer del derecho de acceso a sus datos personales de un modo sencillo y fácil de utilizar.

b) Promover la igualdad de género, la protección de la infancia, de las víctimas y de las personas en situación de vulnerabilidad.

c) Garantizar que las tecnologías eviten perpetuar los sesgos o aumentar las desigualdades existentes, evitando la discriminación algorítmica por razón de raza, procedencia, creencia, religión, sexo, género[55] o cualquier otra razón.

d) Realizar la mínima intrusión en la vida e intimidad de las personas, garantizando un tratamiento proporcional y necesario que preserve las libertades individuales.

e) Implementar mecanismos de verificación, validación y acreditación que garanticen un tratamiento leal y que fomenten la rendición de cuentas.

Ciertamente, conviene recordar que la ética digital persigue proteger valores tales como la dignidad, la libertad, la democracia, la igualdad, la autonomía del individuo y la justicia frente al gobierno de un razonamiento mecánico, lo que la convierte en otro de los

---

desarrollo de una inteligencia artificial, robótica y big data confiables y su utilidad desde el Derecho", *Revista Catalana de Derecho Público*, núm. 58, 2019, pág. 31.

[54] *Vid.* AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: *Guía para la…*, pág. 2.

[55] Acerca de esta novedosa cuestión tuvimos la oportunidad de perfilar algunas ideas y reflexiones con ocasión de un estudio anterior, *vid.* DOMÍNGUEZ ÁLVAREZ, J.L., "Sistemas algorítmicos, protección de datos y nuevas formas de desigualdad. La necesidad de afrontar los sesgos ante el avance digital", en *Estudios interdisciplinares de género,* (Dir.) M. del Pozo Pérez, Thomson Reuters-Aranzadi, Cizur Menor, 2021, pp. 211-229. No obstante, conviene reseñar que la preocupación por combatir el establecimiento de nuevas formas de desigualdad al calor del avance digital constituye una línea prioritaria de actuación de los poderes públicos e instituciones más avezadas. Por todos, *vid.* MINISTERIO DE IGUALDAD, *Mujeres y digitalización. De las brechas a los algoritmos*, Madrid, 2020, págs. 31 y ss. Por su parte, el Senado de España, en estrecha colaboración con el Estudio Salmantino, durante el mes de mayo de 2021, procedió a la creación del "Grupo de reflexión destinado a profundizar en la dimensión ética de la Inteligencia Artificial", del que los autores de esta obra tienen el privilegio de formar parte.

elementos capitales a la hora de avanzar en el establecimiento de un desarrollo tecnológico antropocéntrico, ético, sostenible, igualitario y respetuoso con los derechos y valores fundamentales que integran la concepción de ciudadanía europea[56]. En otras palabras, sin las debidas cauciones en materia de ética y privacidad difícilmente se podrá lograr el ansiado humanismo tecnológico y el despegue de la economía digital se verá seriamente mermado, ante esta tesitura, no parece extraño que la normativa de protección de datos de carácter personal esté llamada a jugar un papel esencial ante los desconocidos horizontes que plantea la innovación tecnológica, convirtiéndose en última instancia en el *dique de contención* encargado de preservar la dignidad de la persona ante un caudal incesante de nuevas amenazas y riesgos envueltos en forma de novedosas aplicaciones, sistemas algorítmicos[57] y metaverso(s).

Ahora bien, esta renovada actualidad del concepto de privacidad[58] ha de venir acompañada de una pausada reflexión que permita concebir la misma como un valor y no como una mercancía que puede ser objeto de monetización, toda vez que la responsabilidad digital está estrechamente vinculada con el respeto por los derechos humanos. Así, respetar la privacidad, la intimidad y la confidencialidad de los datos personales, promover la toma de decisiones libre e informadamente, la equidad, la transparencia y la rendición de cuentas son condiciones necesarias para evitar las prácticas discriminatorias, los usos no deseados y también encubiertos del desarrollo tecnológico[59].

---

[56] *Cfr.* COMISIÓN EUROPEA, *Configurar el futuro digital de Europa,* Bruselas, 2020 [COM(2020) 67 final].

[57] Entendidos como "un conjunto metódico de pasos que pueden emplearse para hacer cálculos, resolver problemas y alcanzar decisiones. Un algoritmo no es un cálculo concreto, sino el método que se sigue cuando se hace el cálculo". *Vid.* HARARI, Y.N.: *Homo Deus. Breve historia del mañana,* Debate, Barcelona, 2017, *pág.* 100.

[58] Por regla general el uso de IA respecto de personas supone un tratamiento de datos y, por tanto, sometido a la normativa general. Bajo la responsabilidad proactiva y demostrada del RGPD, a mayor impacto de los tratamientos, mayores han de ser sus garantías compensatorias; *casi por defecto* será exigible un estudio de impacto. Y más garantías proceden cuando se trata de decisiones automatizadas del artículo 22 RGPD, así como y los deberes de transparencia e información, (arts. 13.2.f y 14.2.g). *Vid.* COTINO HUESO, L., "Derecho y garantías ante el uso público y privado de inteligencia artificial, robótica y big data", *El Derecho de las TIC en Iberoamérica*, (Dir.) M. Bauzá, La Ley-Thompson-Reuters, Montevideo, 2019, pp. 917-952.

[59] Acerca de esta cuestión, el European Data Protection Supervisor (EDPS) afirma que "en el entorno digital actual, no basta con respetar la ley, sino que es preciso tener en cuenta la dimensión ética del tratamiento de datos. El marco regulador de la Unión Europea ya permite la adopción de decisiones y salvaguardas flexibles y específicas en el momento de tratar información personal (…)Pero subyacen cuestiones más profundas por lo que se refiere a las repercusiones que las tendencias en una sociedad datadirigida pueden tener sobre la dignidad, la libertad individual y el funcionamiento de la democracia". *Vid.* EUROPEAN DATA PROTECTION SUPERVISOR, *Dictamen 4/2015, Hacia una nueva ética digital: datos, dignidad y tecnología,* Bruselas, 2015, pág. 4.

Como desarrollo de tal declaración, el Diario Oficial de la Unión Europea acogía el 28 de enero de 2016, la publicación de la Decisión del Supervisor Europeo de Protección de Datos, de fecha 3 de diciembre de

Por todo ello, consideramos que la normativa de protección de datos constituye, por un lado, límite y presupuesto, al mismo tiempo, para el avance del metaverso; y por otro, el último bastión del ordenamiento jurídico para garantizar la dignidad de la persona ante los envites de este nuevo ecosistema digital.

2015, por la que se establece un grupo consultivo externo sobre las dimensiones éticas de la protección de datos. Entre las atribuciones de este Grupo Consultivo sobre Ética destacan: (i) analizar las dimensiones éticas de la protección de datos; (ii) presentar recomendaciones al EDPS, previa solicitud; (iii) presentar propuestas de investigación, promoviendo la cooperación interdisciplinaria; (iv) elaborar al menos dos informes públicos; (v) implicar a otros expertos en su labor de manera permanente o ad hoc, en su caso, en particular en los casos en que estos expertos puedan aportar conocimientos y experiencias adicionales que no estén representados en el Grupo consultivo, entre los que se incluye la experiencia en los ámbitos de la medicina, la salud, las finanzas, la energía, la gobernanza política, la policía o la seguridad; y (vi) presentar hipótesis a un público crítico y evaluar los resultados de las reflexiones del Grupo consultivo en relación con la experiencia de otros profesionales.