Revista de Derecho Civil
http://nreg.es/ojs/index.php/RDC
ISSN 2341-2216
vol. XII, núm. 1 (enero-marzo, 2025)
Ensayos, pp. 279-329

LA PATRIMONIALIZACIÓN DE DATOS ANTE LA CONTAMINACIÓN DIGITAL. UNA PERSPECTIVA CIVIL ANTE UN RETO A NUESTRO SISTEMA[1]

José Manuel de Torres Perea

Profesor Titular de Derecho Civil
Universidad de Málaga

TITLE: *The assetization of data in the face of digital pollution: a civil law perspective on a challenge to our system.*

RESUMEN: En los últimos años está teniendo lugar en Europa un debate doctrinal sobre la patrimonialización de los datos digitales, debate que a día de hoy sigue abierto y que presenta posiciones enfrentadas, las cuales se han visto reflejadas en el reciente desarrollo legislativo europeo.

En este artículo planteamos enfocar esta cuestión desde una perspectiva amplia y conectarlo con los fines que se han de procurar en la nueva economía digital. Por tanto, no se trata simplemente de optar por un determinado modelo de titularidad dominical, sino de analizar cómo el Derecho Civil puede coadyuvar en la formación del nuevo modelo social que regirá las relaciones humanas en la sociedad de la información, pues nos encontramos en un momento histórico crucial en el que hay que decidir sobre la distribución de la nueva riqueza creada por la vigente revolución digital. Para ello en este estudio empezamos por poner de relieve los riesgos que para toda la sociedad se derivan de un tratamiento de datos que está dando lugar a una creciente contaminación digital. Aunque esta contaminación parece hoy normalizada, puede poner en jaque al sistema democrático, y muy especialmente a los derechos a la libertad de expresión y de sufragio, por lo que estos riesgos deben poder ser neutralizados. En este trabajo estudiamos diversas vías encaminadas a ello, entre ellas, la delimitación de la titularidad de los datos para después proceder a la distribución de la riqueza digital entre empresas que los procesan y usuarios que los crean con su comportamiento digital, para lo cual si bien contamos con una base jurídica que lo sostiene, sin embargo encontramos importantes dificultades prácticas que suponen un auténtico reto mayor.

ABSTRACT: *In recent years, a doctrinal debate has been taking place in Europe on the commoditization of digital data. This debate is still open today and presents opposing positions. In fact, these positions have been reflected in recent European legislative developments.*

In this article we propose to approach this issue from a broad perspective and connect it with the purposes to be pursued in the new digital economy. Therefore, it is not simply a matter of opting for a certain model of ownership, but of analyzing how Civil Law can contribute to the formation of the new social model that is destined to govern human relations in the information society. We are at a crucial historical moment in which it is necessary to decide on the distribution of the new wealth created by the current digital revolution. To this end, in this study we begin by highlighting the risks for society as a whole arising from data processing. This is giving rise to a growing digital pollution, a pollution which, although it seems normalized today, can nevertheless threaten the democratic system. It must therefore be possible to neutralize these risks. In this paper we study various ways to achieve this, including the possibility of redistributing digital wealth, involving the citizen as an active participant in the creation of data, for which,

[1] Este artículo es resultado del Proyecto InnoGuard: Hybrid and Generative Intelligence for Trustworthy Autonomous Cyber-Physical Systems. Horizon Europe Framework Programme MCSA Doctoral Network Marie Sklodowska-Curie Actions.

although we have a legal basis that supports it, we nevertheless find significant practical difficulties to make it effective.

PALABRAS CLAVE: datos, datos digitales, activo económico, mercantilización, revolución digital, revolución de IA, contaminación digital, daños morales, acciones de clase, libertad de expresión

KEY WORDS: *data, digital data, economic asset, commoditization, digital revolution, AI revolution, digital pollution, moral damages, class actions, freedom of expression.*

1. INTRODUCCIÓN. UNA APROXIMACIÓN INICIAL A LOS PROBLEMAS DERIVADOS DEL TRATAMIENTO DE DATOS

La digitalización ha supuesto avances significativos, la sociedad ha experimentado importantes cambios en las últimas tres décadas que han modificado los cimientos de las relaciones humanas y sus sistemas políticos.

La mercantilización de los datos ha provocado el surgimiento de todo tipo de compañías que buscan clientes a los que vender datos elaborados en forma de estadísticas, perfiles abstractos, etcétera[2], que les permitan tanto prever el comportamiento humano como influir en él. Esto ha generado un nivel creciente de contaminación digital[3], es decir

[2] A título de ejemplo Dawex, empresa líder en intercambio de datos, en cuya página web leemos: «Para crear valor a escala con el intercambio de datos, las organizaciones necesitan confiar en tecnologías de intercambio de datos de última generación que aborden varias problemáticas a la vez como la seguridad, el cumplimiento, la confianza y la interoperabilidad, con una solución integrada y coherente. La tecnología Dawex integra miles de funcionalidades dedicadas al Intercambio de Datos. Explore la Arquitectura de Referencia de Intercambio de Datos implementada por Dawex, que permite a todos los participantes del ecosistema de datos realizar transacciones de datos de confianza…» (https://www.dawex.com/en/).

[3] Entendemos por contaminación digital la causada por el procesamiento masivo de datos, que supone una hipervigilancia omnipresente y la pérdida del anonimato del ser humano. Se ha dicho que los datos

inundación de todo tipo de información procesada por algoritmos dirigida hace individuos concretos mediante la técnica del contraste con perfiles sintéticos[4], contaminación de proporciones gigantescas que lo invade todo y que puede poner en jaque el pleno ejercicio de importantes derechos fundamentales. Las técnicas de creación de perfiles abstractos y microsegmentación son usadas, en ocasiones, para enviar de forma personalizada todo tipo de *fake news*, verdades «enfatizadas» dirigidas en el momento oportuno y de teorías de la conspiración para que las reciban las personas idóneas de cara a manipular su concepción de la realidad y sus decisiones, entre ellas las electorales. Esto cuestiona importantes derechos fundamentales como el de la libertad de expresión, pues la relativización de la realidad lleva a que este derecho quede vacío, y el de sufragio, pues la manipulación convierte al elector en un títere. Téngase en cuenta que una forma de vaciar el derecho de sufragio es la manipulación del cuerpo electoral mediante desinformación y mentiras, lo cual si bien ocurre desde que las democracias representativas están instituidas, pues no en pocas ocasiones la línea editorial de un diario ha provocado la adulteración de las noticias, ahora ha alcanzado unas proporciones desconocidas, debido a la sofisticación de los algoritmos, la apariencia de veracidad que generan las noticias y la capacidad de manipulación ideológica microsegmentada, entre otras muchas estrategias de manipulación.

Los remedios para luchar contra estos abusos han de venir desde un análisis jurídico-privatista del proceso que los genera y muy especialmente del fenómeno de recolección y análisis de datos que da lugar a la construcción de modelos, es decir, perfiles abstractos, que luego se implementan. Todo ello requiere partir del estudio de los datos digitales desde la perspectiva civil, empezando por determinar si es posible un derecho de propiedad sobre los datos y a quién corresponde su titularidad, la respuesta a estas preguntas nos puede ayudar a construir un sistema de remedios que proteja a la sociedad de uno de los principales problemas que la desafía.

serían el nuevo petróleo, este silogismo nos permitiría encontrar un paralelismo entre la contaminación ambiental creada por los hidrocarburos y la contaminación digital creada por el procesamiento generalizado de datos. Como consecuencia de este fenómeno se ha producido una «contaminación de libertades» en las democracias modernas, desde esta perspectiva puede considerarse el derecho a un entorno digital no contaminado paralelo al derecho a un medio ambiente saludable.

[4] En este trabajo se entiende por perfil sintético, abstracto o comportamental a un conjunto de datos y características que describen «conductas grupales tipificadas» en función del comportamiento, hábitos, preferencias u otras características inferidas, y que no incluyen identificadores directos como el nombre o la dirección, pues quedan desconectados de las personas cuya conducta digital ha servido para crearlos. Estos perfiles no quedan sujetos al RGDP por no contener datos personales, si bien están ideados para poder identificar personas individuales que reúnan las características recogidas en los mismos, mediante la técnica de contraste. Por ejemplo, un perfil de personas aficionadas a deportes extremos o con hábitos de compra de productos de lujo, que una vez construido permite identificar a los sujetos que reúnan las características que conforman la «conducta grupal tipificada» correspondiente.

Por tanto, en primer lugar queremos detenernos en los riesgos que está creando la creciente contaminación digital, para en un segundo momento analizar posibles remedios para intentar neutralizarla, dentro de los cuales incluimos la hipótesis de la redistribución de la riqueza digital a favor del usuario que contribuye a crearla, para lo cual será necesario dar acomodo en nuestro Código Civil a la patrimonialización de los datos. Hipótesis que desde la perspectiva teórica puede encontrar suficiente respaldo jurídico, pero que desde la perspectiva práctica plantea importantes problemas de partida.

1.1. *Primer problema: desafío a los derechos fundamentales y al sistema democrático*

La influencia de la digitalización en la sociedad se realiza a diario en distintos ámbitos. Uno de ellos, no menor, al moldear la propia mente humana. Como señaló Ramón y Cajal el cerebro juvenil posee una plasticidad exquisita, en cuya virtud puede, a impulsos de un energético querer, mejorar extraordinariamente su organización creando asociaciones nuevas, depurando y afinando el juicio. Por ello afirma que el trabajo sustituye al talento[5]. De igual forma, el sometimiento de la mente a todo tipo de exposición digital desde muy corta edad influye en su formación y posterior comportamiento, dada su plasticidad. Estas nuevas mentes que han sido moldeadas por todo tipo de dispositivos desde su infancia, recibiendo impulsos electrónicos incesantes, no suelen desarrollar el hábito de la lectura fuera de determinados dispositivos y aplicaciones electrónicas, caracterizadas por contener textos de lectura rápida[6]. Esta falta de lectores ávidos por sondear y contrastar argumentos expuestos mediante un formato tradicional, que exige tiempo y dedicación, ha creado un problema estructural. La esfera pública ya no encuentra referentes intelectuales de talla sobre los que construir una opinión, sencillamente porque ha renunciado a prestar su tiempo al enjuiciamiento de argumentos ajenos expuestos en obras de ensayo. Sin lectores receptores de argumentos, no puede haber intelectuales que guíen. Es en parte por ello que se considera que la filosofía occidental no tiene futuro, porque además ha renunciado a las grandes preguntas, a la totalidad, y ha huido hacia la especialización.

[5] RAMÓN Y CAJAL, Santiago, *Reglas y consejos sobre investigación científica. Los tónicos de la voluntad,* Ed. Austral, 1898, Séptima impresión 2020, p. 48.

[6] CARR, Nicholas, *The Shallows: What the Internet is doing to our Brains*, Ed. W.W. Norton & Company, Nueva York, 2010, sostiene que internet está «dañando» la manera de pensar, de aprender y de ser del ser humano. Precisamente afirma que al ser el cerebro humano plástico, cambia al adaptarse a las circunstancias, tecnologías y formas de aprendizaje.

En esta línea destaca el manifiesto de Liubliana sobre lectura profunda, en el cual se denuncia como la lectura profunda es la herramienta más poderosa que tiene el ser humano para desarrollar el pensamiento analítico y crítico y se apela a que se reconozca la importancia permanente de dicha lectura profunda en la era digital, vid. https://readingmanifesto.org/?lang=es

Como ha señalado Jürgen Habermas la esfera pública liberal vive hoy supuestos culturales y sociales inverosímiles. El periodismo independiente, que tenía la capacidad de dirigir a la ciudadanía hacia determinadas materias para crear opinión política y que vivía de la mano de una población lectora interesada en la política, con buen nivel educativo, acostumbrada al conflictivo proceso de formación de opinión y dispuesta a dedicar su tiempo para formarse una opinión pública de calidad, ya no es operativo. Señalaba Habermas, ya en 1962, que la opinión pública está en decadencia y pierde su función política, entendida como «sumisión de los estados de cosas hechos públicos al control de un público crítico». Téngase en cuenta que para Habermas era primordial la necesidad de un público compuesto por personas privadas que razonan y se apropian de la opinión pública, convirtiéndola en una esfera de crítica del poder público, a partir de una «opinión pública literaria», dotada de organización y plataformas de discusión, que da lugar a la opinión pública política[7]. Más recientemente, en 2018, Habermas, ha vuelto a tratar esta cuestión para afirmar que ha sido internet el instrumento que ha terminado por difuminar esta esfera pública, y la ha llevado a la mercantilización mediante la explotación económica del perfil privado del usuario. Explotación calificada por Jürgen Habermas como auténtico «robo de datos» de clientes sin su conocimiento a fin de poder manipularlos en ocasiones con «fines políticos inconfesables». Por ello considera a la revolución digital[8] como la primera revolución de medios en la historia de la humanidad que sirve ante todo a fines económicos y no culturales[9]. De hecho, se ha probado que este «robo»[10] interesado de datos permite usarlos mediante técnicas de

[7] HABERMAS, Jürgen, *Historia crítica de la opinión pública, La transformación estructural de la vida pública,* (*Strukturwandel der Öffentlichkeit),* Ed. Gustavo Gili (GG) Mass Media, trad. Antoni Domènech, 1982, 2ª edición, Barcelona/Buenos Aires/México, pp. 88-171.

[8] Un importante resultado de esta revolución digital es lo que ZUBOFF, Shoshana denomina «capitalismo de vigilancia», es decir, un capitalismo que hace uso de una nueva materia prima, la experiencia humana. *La era del capitalismo de la vigilancia. La lucha por un futuro humano frente a las nuevas fronteras de poder*, trad. Albino Santos Mosquera, Ed. Paidós Ibérica, Barcelona, París 2020, p. 21. Zuboff considera que está en juego la misma naturaleza humana, pues este nuevo capitalismo tiene un efecto modificador de toda la arquitectura global, tal como el capitalismo industrial transformó el mundo natural del siglo XX. Por tanto, asimila a los humanos más a abejas de una colmena controlada por una arquitectural digital omnipresente, que a ganado manipulable. Se trata de otro duro paso en el camino del Antropoceno, un paso que se sabe cómo comienza, pero del que se desconoce las derivadas a las que puede llevar al género humano.

Por su parte, LASSALLE RUIZ, José María, en *Civilización artificial*, ed. Arpa, Barcelona 2024, p. 44 afirma que la revolución digital ha muerto después de siete décadas y ha sido reemplazada por la revolución de la IA.

[9] HABERMAS. Jürgen, «Moralischer Universalismus in Zeiten politischer Regression. Jürgen Habermas im Gesprächt über die Gegenwart und sein Lebenswerkt», en *Leviathan*, 48, 1, 2020, pp. 7-28.

También HERMOSO, Borja, «Entrevista a Jürgen Habermas», *El País Semanal,* 10 de mayo de 2018. https://elpais.com/elpais/2018/04/25/eps/1524679056_056165.html

[10] DOMÍNGUEZ YAMASAKI, María Isabel, «El tratamiento de datos personales como prestación contractual. Gratuidad de contenidos y servicios digitales a elección del usuario», *Revista de Derecho Privado,* N. 4, julio-agosto 2020, pp. 93-120, pp. 114-118, pone de relieve como la desinformación viene

microsegmentación para manipular la opinión pública y la propia publicidad electoral adaptándola conforme al perfil del receptor, e incluso incluyendo *fake news*, lo cual ha puesto en jaque al propio sistema democrático hoy vigente en occidente.

Sin medios independientes que puedan llegar a la esfera pública, sin lectores de intelectuales de referencia, hemos entrado en un escenario desconocido en el que reina un nuevo nihilismo que ha llevado a la ciudadanía a una pérdida de creencia en los propios hechos. El relato se impone sobre los hechos a través de todo tipo de desinformación y *fake news*, cuando no teorías de la conspiración. Es lo que ha llamado Byung-Chul Han la «crisis de la verdad», se pierde la verdad como idea reguladora de la sociedad, lo que en última instancia lleva a la crisis de la democracia, pues se socava la distinción entre verdad y mentira y se pierde la fe en los propios hechos. De esta forma, la libertad de expresión se convierte en una farsa, pues al carecerse de referencias que conecten con la realidad pierde su contenido[11], además la inundación de información que ha traído la revolución digital crea la dificultad de poder discriminar adecuadamente y distinguir entre información relevante y nimia, por lo que la fiabilidad de dicha información queda en tela de juicio[12]. Llegamos a la conclusión de que en la sociedad de la información estamos bien informados pero desorientados, pues la información ya no tiene capacidad orientativa.

De hecho, el capitalismo de vigilancia ha creado una arquitectura global de modificación de la conducta que amenaza con transfigurar la naturaleza humana y puede someter a la gran mayoría de los individuos a la tiranía de unos pocos. Para ello, se hace uso de herramientas de analítica de datos avanzada y sistemas de inteligencia artificial con la finalidad de perfilar al individuo y realizar inferencias acerca de su pasado, presente y futuro. Inferencias que no respetan ni sus pensamientos, ni sus sentimientos. Mediante la creación de perfiles abstractos, formados con una ingente información debidamente segmentada, se crean patrones que permiten su contraste con cualquier individuo, incluso aquel que no ha dado consentimiento alguno para el procesamiento de sus datos, a fin de poder inferir en su comportamiento y detectar la información individualizada idónea para influir en su conducta futura.

de la mano del empleo abusivo de los términos «gratis» o «gratuitos» que tradicionalmente han aparecido en los muros de *cookies*.

[11] HAN, Byung-Chul, *La digitalización y la crisis de la democracia. Infocracia,* Ed. Taurus, trad. Joaquín Chamorro Mielke, 2022, pp. 71-75.

[12] FINK, Leonard, «Big Data and Artificial Intelligence», *Zeitschrift für Geistiges Eigentum – Intellectual Property Journal*, Volume 9, 2019, fascículo 3 Band 9, pp. 288-298, señala que hoy en día toda información, incluso la menos relevante, puede tener un potencial económico en el entorno de la digitalización.

1.2. Segundo problema: Desequilibrio provocado por un reparto desigual de la riqueza digital

La generación de riqueza en la era digital se basa en la interacción entre datos y los algoritmos que los procesan, lo que ha transformado profundamente la noción misma de capital y los criterios que determinan el valor económico actual. Esta transformación está alterando los equilibrios tradicionales, generando un desajuste éticamente neutro que amenaza con desestabilizar la cohesión social. El trabajo, especialmente el realizado por las clases medias, pierde relevancia y capacidad adquisitiva en un contexto donde la inteligencia artificial avanza, volviéndolo cada vez más prescindible.[13]. De hecho, conforme señala Lassalle, Los datos, concebidos como bienes intangibles, están reemplazando al trabajo humano tanto como referente de valor como principal generador de riqueza. A esto se suma su crecimiento exponencial: Lassalle estima que el volumen global de datos se ha duplicado aproximadamente cada año y medio.[14]

En palabras de Juan Cristóbal Cobo Romaní, «vivimos en una suerte de feudalismo digital en el que unos pocos administran los datos y una gran población los entrega sin recibir una compensación real»[15]. Administrar datos significa administrar información digitalizada con un potencial como activo económico de unas dimensiones extraordinarias en el conjunto de la economía. Esta discriminación social ha de ser rectificada para hacer viable el sistema social y democrático vigentes, pues de lo contrario las consecuencias pueden ser irreparables, lo cual nos lleva a la necesidad de plantear una redistribución de la riqueza digital entre usuarios que la generan con su conducta y empresas que procesan los datos con algoritmos e IA.

1.3. Tercer problema: Hacer compatible la IA con una ética humana

En materia de IA encontramos dos problemas relevantes que merecen nuestra atención. En primer lugar el procesamiento de datos se potencia mediante sistemas de IA, que contienen miles de datos, capaces de elaborar perfiles sintéticos, que pueden ser objeto de contraste en personas concretas. Mientras más datos tenga un sistema de IA, más precisos serán los perfiles que podrá realizar y mayor fiabilidad tendrá en sus predicciones y resultados, por lo que están programados para fagocitar todo tipo de datos, que luego los algoritmos discriminarán. Es evidente la necesidad de regular estos sistemas de IA para que sigan patrones respetuosos con la condición humana y los

[13] Recojo en este párrafo las reflexiones de LASSALLE RUIZ, *Civilización,* cit., p. 74.
[14] LASSALLE RUIZ, José María, *Ciberleviatán. El colapso de la democracia liberal frente a la revolución digital*, Ed. Arpa, Madrid, 2019, pp. 34 y 37.
[15] COBO ROMANÍ, Juan Cristóbal, *Acepto las condiciones – Usos y abusos de las tecnologías digitales,* Fundación Santillana, Madrid, 2019, p. 5.

derechos fundamentales. Se afirma que hay que apostar por una «humanidad compartida» que pueda encauzar la IA dentro de unos parámetros compatibles con la evolución humana[16].

En segundo lugar, se afirma que tras la creación de chatGPT nos encontramos inmersos en la revolución de la IA, pues se ha producido un punto de inflexión, esto es la singularidad de que la IA ha pasado a ser protagonista de las vidas de los ciudadanos. De hecho, la IA está realizando tareas que hasta hace poco se pensaba que solo podría hacer una inteligencia humana, lo cual está provocando que esté reemplazando a número creciente de trabajadores en un periodo de tiempo récord[17]. De hecho en tareas de trabajo rutinario se ha calculado que solo se necesitará en un futuro cercano entre un 10 o 15% de las plantillas hoy existentes. Lo cual implica que el mercado laboral se ve amenazado por la IA que simultáneamente está concentrando toda la riqueza digital en manos de unos pocos[18]. Por meras razones de subsistencia social es urgente plantear un reparto de la riqueza digital más equitativo y «humano» que supere el utilitarismo egoísta de las grandes plataformas, y en este punto el Derecho tiene una importante tarea por hacer, pues han de formularse unos criterios factibles que permitan una solución legal que no sea impracticable; así como establecer mecanismos legales para hacer compatible el desarrollo de la IA con la pervivencia de los modelos sociales hasta hoy vigentes.

[16] HARARI, Yuval Noah en *Nexus: A brief history of information networks from the Stone Age to AI,* Ed. Vintage publishing, London, 2024, pp. 15 y ss. realiza un estudio detallado de la información como «flujo que nos ha moldeado a nosotros y a nuestro mundo», ha señalado como en el momento presente abunda la desinformación, la cual coadyuva a profundizar la crisis existencial en que se encuentra el género humano. De hecho se considera que nos dirigimos hacia una nueva red de información en la era de IA, que puede llegar a ser destructiva para el ser humano, y que requiere replantear las relaciones entre información, verdad y poder, pues no en vano los distintos sistemas políticos han hecho uso de la información durante milenios para alcanzar sus objetivos.

[17] Se afirma que en la actual revolución digital no se prevé una sustitución del trabajo realizado por la clase media, sino su reemplazo por un trabajo más eficiente realizado por máquinas, siendo así que ese trabajo cada vez sea menos valorado, y que por ello el poder adquisitivo de la clase media disminuya paulatinamente en la misma medida que aumentan los populismos reflejo del descontento general. LASSALLE RUIZ, *Civilización,* cit., p. 45, pone el énfasis en la desigualdad que crea la transformación digital y la necesidad de controlarla y regularla para evitarla.

[18] FENOLLOSA, Carlos, *La singularidad*, ed. Arpa, 2024, Barcelona, pp. 9 y ss.

2. UNA REVOLUCIÓN DIGITAL CIMENTADA EN LA RECOPILACIÓN MASIVA DE DATOS GENERADOS POR LOS USUARIOS

2.1. *Técnicas de recopilación de datos*

Una vez presentados los problemas que plantea el procesamiento indiscriminado de datos, procede estudiar cómo se desarrolla éste. Para ello, en primer lugar debemos tener en cuenta que la información ha sido siempre un bien valioso, ahora lo que ha cambiado es el acceso digital a la misma. De hecho, el desarrollo y expansión de internet en las últimas décadas ha ido en paralelo a su comportamiento digital. Captación que se realiza por medios aparentemente inocuos y gratuitos, como son los muros de *cookies*, pero que en realidad conllevan importantes contraprestaciones, pues suponen verdaderas transacciones de datos, que muchas veces pasan desapercibidas para la ciudadanía y a las que Habermas califica como «apropiaciones inconsentidas». Esta captación masiva de datos se realiza para procesarlos y, mediante el uso de técnicas de microsegmentación, convertirlos en productos finales con valor económico[19].

El punto de partida ha de ser un análisis de la situación vigente en la sociedad de la información, pues hoy en día encontramos en internet un sinfín de herramientas, que suelen pasar inadvertidas, pero que están encaminadas a recopilar toda clase de datos generados por los usuarios. En primer lugar, destaca la técnica de *Browser fingerprinting*[20] dirigida a identificar perfiles de usuarios en base a rasgos y características únicas que solo ellos poseen. Utiliza la información obtenida a través de peticiones http del navegador. La cabecera de esa información contiene tipos de ficheros soportados, codificación de caracteres, idioma, tipo de navegador, etc., lo que permite informar al servidor de posibles limitaciones del usuario. Aunque esta información no identifica al usuario con alto grado de certeza, sí que permite crear perfiles de usuarios con dichas características para recopilar información[21].

Otra opción que sigue el *figerprinting* es inyectar scripts en determinados sitios webs para obtener más información sobre el dispositivo y el navegador. Las características recolectadas por los scripts se pueden combinar mediante una función *hash*, que es un algoritmo que toma una entrada -características recolectadas- y devuelve una cadena de

[19] La capacidad de recolección aumenta conforme a cuatro factores: (1) mayor tiempo de uso de dispositivos tecnológicos, (2) mayor número de usuarios de los dispositivos (3) mayor variedad de dispositivos tecnológicos y (4) mayor capacidad de interpretación de datos y sobre todo de metadatos.

[20] Para una explicación más detallada, se pueden consultar el siguiente enlace: -Geekflare-(https://geekflare.com/browser-fingerprinting/).

[21] Depende del navegador que se use el usuario estará más o menos expuesto al rastreo de la huella digital de su *fingerprint*. Por ejemplo, el usuario que acceda a internet a través de Chrome estará menos protegido que el que entra a través del navegador Brave.

longitud fija y generalmente una representación numérica única para cada entrada diferente. Cada *hash* representa un elemento y es unidireccional, una vez se realiza el *hash* es imposible conocer las características iniciales. El *hash* permite hacer un seguimiento del usuario por toda la web, siendo más eficaz que el seguimiento mediante *cookies*. El cliente solo puede optar por deshabilitar JavaScript para evitar este tipo de seguimiento.

Igualmente, dentro de las estrategias *fingerprinting*, debemos referir el Html5. Para entender su funcionamiento pensemos en dos sitios webs que utilizan el elemento canvas de html5, que fuerzan al navegador a generar una imagen o un texto en segundo plano, aunque esos dos navegadores ejecutándose en equipos diferentes generaran textos o imágenes diferentes. Como cada navegador genera una imagen o texto distinto se puede identificar en qué navegador, es decir en qué equipo informático, Mac, Windows, Linux, etc. se encuentra el usuario. Por tanto, con esta información se puede detectar si se accede desde un ordenador Mac, lo cual podría ser útil, por ejemplo, para identificar un mayor poder adquisitivo que si se accede desde un navegador Linux, a fin de ofrecer tarifas adaptadas al poder adquisitivo detectado. Detección que solo puede evitarse si se accede desde páginas de incógnito. Es importante subrayar que el elemento Html5 canvas dibuja gráficos ocultos que el usuario no ve[22].

Si reflexionamos sobre lo explicado hasta aquí podemos deducir que existe todo un sistema de herramientas «ocultas» o al menos desapercibidas para un usuario no experto, que han sido configuradas para registrar todo tipo de datos generados por el usuario para procesarlos mediante técnicas de microsegmentación. Esta segmentación de la información del usuario debidamente procesada por algoritmos permite muy diversos usos, no siempre confesables, y se convierte en un activo económico de primer orden. Todo este proceso se realiza sin que ni siquiera se haya solicitado algún tipo de aceptación en ningún momento. Es un proceso automático y programado que pone de manifiesto la debilidad del usuario de internet y la deficiencia de la normativa vigente que lo deja indefenso ante la extracción desmedida de los datos que genera, la cual se produce de forma totalmente ajena a su voluntad. Desde la perspectiva civil, esta forma «quasi-clandestina» de operar programada por algoritmos puede resultar poco honesta y fuera de las exigencias de la buena fe, y puede atentar contra los principios de licitud, lealtad y transparencia recogidos en el art. 5.1.1 del Reglamento de Protección de Datos.

[22] Además debemos referirnos al WebGL Fingerprinting, similar al canvas fingerprinting, pero basado en la renderización de gráficos 3D para extraer características únicas del hardware gráfico y los drivers; y al Audio Fingerprinting, técnica que analiza la forma en que el dispositivo reproduce un sonido, detectando diferencias sutiles en el hardware de audio y los controladores.

Por otro lado, nos encontramos con herramientas que si bien sí requieren de un previo consentimiento del usuario, lo enmascaran bajo fórmulas aparentemente inocuas, de forma que aparecen como simples pasos para el acceso gratuito a determinados contenidos o servicios digitales. Nos referimos a las conocidas *cookies*, las cuales sirven para almacenar y recuperar datos conforme a lo que ya dispuso el artículo 22.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI). Una *cookie* es un archivo alfanumérico que es colocado en el ordenador del usuario, ya sea por el proveedor del servicio web, o por el proveedor de publicidad, que tiene como finalidad registrar la información de la actividad desarrollada por el usuario. De esta forma se logra acceso a las preferencias y hábitos del usuario de cara a la posterior personalización de la publicidad, mecanismo que en ocasiones se ve potenciado con el uso de herramientas de inteligencia artificial y de esta forma aplicar algoritmos que puedan llegar, incluso, a predecir el comportamiento del usuario[23].

Denominar a estas herramientas por el equivalente inglés al término «galleta» tuvo su razón en una analogía, pues ambas dejan «migas», o huellas que permiten seguirlas. Esta huella digital que el usuario genera al aceptar *cookies* puede ser una valiosa fuente de información sobre hábitos, tendencias y preferencias, que pueden permitir a un algoritmo debidamente programado utilizarlo para incluirlo en un determinado grupo aplicando técnicas de microsegmentación. De esta manera, mediante una auténtica minería de datos, se genera una información que puede ser muy valiosa para muy distintos objetivos. Lo paradójico es que en muchas ocasiones este proceso pasa inadvertido para el usuario, pues lo único que percibe es que la aceptación de la *cookie* ha sido necesaria para acceder al contenido o servicio digital ofrecido de manera gratuita (aparentemente), por lo que no es consciente de haber realizado una contraprestación por su parte, lo cual es evidentemente falso, pues puede que haya dispuesto de parte de su intimidad y haya permitido que sus datos se procesen para convertirlos en productos económicamente valiosos. En realidad al aceptar las *cookies* el usuario consiente su instalación en su dispositivo, las cuales van a permitir el acceso a sus datos a un número inimaginable de terceros, así por ejemplo en un diario digital el consentimiento de los «es» supone dar acceso de promedio a entre 800 y 900 terceros[24].

[23] TRUJILLO CABRERA, Carlos, «Los nuevos *cookies walls*: "Consent or pay". A propósito de la Sentencia del Tribunal de Justicia de la Unión Europea de 4 de julio de 2023», *Revista de Derecho Civil,* vol. XI, Nú.2 (abril-junio 2024), Estudios, p. 81.
[24] Ibid., p. 104.

En especial merecen nuestra atención las «webs beacons», también llamadas balizas web[25]. Se trata de imágenes pequeñas o trasparentes de un píxel por un píxel que se incluyen en sitios webs y que permiten monitorizar la actividad de los usuarios. Las balizas web han de ser aceptadas por *cookies*. Por ejemplo, una baliza web en un correo electrónico sirve para permitir conocer si el correo fue recibido, si fue abierto, la dirección IP del dispositivo del destinatario que puede ser usada para la geolocalización, el tipo de cliente del correo, el sistema operativo y la hora y fecha de apertura, entre otros datos. Estas balizas pueden incluirse en webs de compras para sectorializar a los clientes, etc.[26].

Estas herramientas digitales programadas para recopilar datos generan un producto que aumenta de valor conforme más información segmentada pueda generar. Esta extracción masiva de datos posteriormente procesados puede ser útil de cara a conseguir muy diversos fines, desde una publicidad a la carta, hasta influir en el voto ciudadano en un proceso electoral. Así en las elecciones al Congreso de los EE.UU. de 2018, se encontraron rastreadores de terceros en el 87% de los sitios afiliados a la candidatura. El problema es que la regulación de protección de datos sigue siendo ineficaz, incluso en Europa, lo cual se puso de manifiesto en las elecciones presidenciales francesas de 2017 en las que ninguna candidatura cumplió completamente los requerimientos legales en relación con el consentimiento y uso de *cookies*[27]. Por tanto, mediante el uso de estas técnicas se puede manipular faltando a la honestidad, obrando de mala fe, por lo que puede dar lugar a una manipulación de la opinión pública, pues el ciudadano se ve colapsado por todo tipo de información individualizada, *fake news*, teorías de la conspiración, etc., por lo que puede llegar a ponerse en jaque el propio

[25] Las balizas web, también conocidas como «web beacons» o «etiquetas de píxel», son pequeños archivos de imagen incrustados en páginas web o correos electrónicos que permiten rastrear la actividad del usuario. Es importante señalar que son invisibles para el usuario, en todo caso estas balizas son instrumentos para recopilar datos sobre cómo interactúan los usuarios con un correo electrónico o un sitio web. Esto significa que cuando un usuario visita una página web o abre un correo electrónico que contiene una baliza web, lo que ocurre es que ésta envía una solicitud a un servidor externo que recoge información que puede resultar valiosa para el análisis de marketing, como la dirección IP del usuario, el tipo de navegador, y detalles sobre la interacción, como si se abrió el correo o se hizo clic en un enlace. Además esta información puede servir para técnicas de personalización de contenido, o incluso para el seguimiento de conversiones. En resumen, permiten rastrear las actividades de los usuarios sin su conocimiento lo cual plantea problemas de privacidad que aparentemente pueden resolverse pidiendo el consentimiento al usuario. Pueden consultarse: (https://techlib.net/techedu/web-beacon/).

[26] Así, por ejemplo, la empresa Meta de Facebook ofrece a empresas privadas este tipo de seguimiento de sus sitios web, de forma que pueden controlar la eficacia de sus anuncios, acciones de sus clientes, como visitar una página o usar el carrito, determinar cuántos clientes realizaron una acción después de ver una determinada publicidad, etc., https://www.facebook.com/business/tools/meta-pixel

[27] https://ourdataourselves.tacticaltech.org/posts/third-party-tracking-es/

sistema democrático, es decir, tanto el derecho a la libertad de expresión como el propio derecho a un sufragio electoral libre[28].

2.2. *Distintas bases de legitimación para el tratamiento de datos*

Debe hacerse una distinción entre las herramientas de rastreo que quedan vinculadas a un previo consentimiento y las que no, pues en virtud del art. 6 del Reglamento General de Protección de Datos todo tratamiento de datos debe estar amparado por una base de legitimación, siendo una de ellas el consentimiento del usuario, recogido en el art. 4.11 del Reglamento General de Protección de Datos, según el cual el consentimiento supone «toda manifestación de voluntad libre, específica, informada e inequívoca para la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen», por lo que se incluye la aceptación tácita[29]. Igualmente el art. 6.1 RGPD exige que el consentimiento sea específico, por lo que un consentimiento general carecerá de validez. El consentimiento ha de ser informado conforme al art. 6 y teniendo en cuenta los arts. 13 y 14 RGPD, por lo que las *cookies* han de informar de forma clara y visible sobre las consecuencias de su uso al solicitar el consentimiento[30].

A su vez, el art. 7.4 del RGPD evalúa la existencia de un «consentimiento libre» atendiendo a si la ejecución del contrato se supedita al tratamiento de datos personales que no sean necesarios para la ejecución del contrato, recogiendo el Considerando 43 en el que se presume que media un consentimiento no libre cuando se trata de un requisito imprescindible para la ejecución de la prestación. Señala Trujillo Cabrera que para que el consentimiento pueda ser considerado libre es necesario que no medie vicio

[28] El Consejo Europeo de junio de 2018 encomendó a la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad y a la Comisión Europea la tarea de presentar un Plan de Acción para una respuesta coordinada contra la desinformación. Este Plan de Acción fue presentado y aprobado en el Consejo Europeo del 13 y 14 de diciembre de 2018. Consecuentemente, en marzo de 2019 se creó un Sistema de Alerta Rápida para alertar instantáneamente sobre campañas de desinformación a través de una infraestructura tecnológica específica e intercambiar información entre los Estados miembros y la Unión.

[29] Este consentimiento solo habilitaría para el tratamiento de datos personales ordinarios, pero no para los «especiales», es decir, datos relativos a la salud, la vida sexual o las opiniones políticas ni las restantes categorías recogidas en el art. 9.1 RGPD, que requerirían de un consentimiento explícito y una solicitud motivada, según el art. 9.2 RGPD. Vid. CASTILLO PARRILLA, José Antonio y MORAIS CARVALHO, Jorge, «*Pay or ok*. Pagar con datos personales tras la Directiva 2019/770: una visión comparada entre España y Portugal», en *Revista electrónica de Dereito*, junho 2024, nº 2, Vol.34, p. 120.
Sin embargo, El Grupo de Trabajo del Artículo 29, que se convirtió en el Comité Europeo de Protección de Datos (CEPD), ha realizado un dictamen sobre el consentimiento (Dictamen 15/2011) en cuya p. 29 señala que «Las soluciones consistentes en entender que existe una autorización tácita si no se manifiesta explícitamente lo contario, no cumplirán el requisito de ser explícitas».

[30] TRUJILLO CABRERA, «Los nuevos *cookie walls*», cit., p. 96.

del consentimiento, ni amenaza de consecuencias perjudiciales de entidad en caso de que se rechace prestar el consentimiento[31]. Recientemente el TJUE ha tenido oportunidad de manifestarse al respecto, en el asunto C 252/21 Facebook v Bundeskartellamt de 4 de julio de 2023 (FJ 147-148), al señalar que en el caso de que el operador de red social en línea tenga una posición dominante, dicha circunstancia deberá ser sopesada a la hora de valorar el libre consentimiento del usuario, por el riesgo que causa dicha situación en tanto pueda impedir una libre elección y por el enorme desequilibrio que causa entre operador y usuario. Finalmente, cabe señalar que el TJUE aclara que el consentimiento se considerará válido si en caso de negarse el usuario a prestar su consentimiento, se le ofrece, a cambio de una remuneración adecuada, la posibilidad de acceder al servicio sin tratamiento de sus datos (FJ.150).

Por otro lado, el art. 6 del RGPD recoge otras vías de legitimación distintas al consentimiento, pero jerárquicamente equivalentes, estableciendo una lista de supuestos muy amplia: desde su necesidad para la ejecución de un contrato en el que el interesado sea parte hasta que lo exija el cumplimiento de una misión realizada en interés público.

El art. 6 RGPD viene a concretar los principios recogidos en el artículo precedente, pues en tanto que medie un tratamiento de datos de carácter personal debe realizarse de manera lícita, leal y transparente, respetando los principios de limitación de la finalidad y minimización de datos. La sentencia de 4 de julio de 2023 del TJUE (que se detalla más adelante) nos puede servir para comprender los otros supuestos legitimadores del art. 6 RGPD. En esta sentencia se analizó el condicionado general que Facebook (Meta) incluía en los contratos que realizaba con sus usuarios y que les permitía el tratamiento de actividades realizadas tanto dentro como fuera de dicha red social, (off Facebook). El Tribunal descartó por razones obvias que pudiera servir como base de legitimación la prevista en art.6.1.c) obligación legal, d) protección de intereses vitales o e) misión realizada en interés público o ejercicio de poderes públicos. Respecto a la base de legitimación fundada en ser necesario para la «ejecución del contrato» (art.6.1.b) conforme había alegado Meta, la sentencia señala que se requiere que sea objetivamente necesario para dicha ejecución, necesidad que quedaba excluida de mediar otra alternativa menos invasora. Por tanto, de poderse prestar el servicio con otra opción, como por ejemplo, la publicidad no personalizada, esta base de legitimación decaería. Respecto al «interés legítimo» del responsable del tratamiento o terceros

[31] TRUJILLO CABRERA, «Los nuevos *cookie walls*: "Consent or pay"», cit., p. 97-98. Igualmente debemos referirnos a las Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2018/679, adoptadas el 4 de mayo de 2020 del Comité Europeo de Protección de Datos. Vid. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf

(art.6.1.f), la sentencia considera que dicho interés solo podrá ser considerado como base de legitimación si no prevalece un derecho, interés o libertad fundamental del usuario exigida por la protección de sus datos. En concreto, se estimó que el rastreo de actividades en línea y fuera de línea o el seguimiento en distintos sitios web pueden no quedar justificados, pues hay que ponderar caso por caso para determinar los datos que el usuario puede o no esperar razonablemente que sean tratados sin su consentimiento, por lo que, concluye el tribunal, que en este punto prevalecen los intereses del usuario sobre los del operador, aunque se ofrezca un servicio gratuito financiado por medio de esta actividad.

Además, debemos tener en cuenta que si un perfil abstracto contiene datos obtenidos sin consentimiento, en tanto que es un perfil abstracto queda fuera del ámbito de aplicación del RGPD, solo en el caso de aplicación de dicho perfil abstracto a una persona física se planteará la posibilidad de su sometimiento al art. 22 RGPD[32].

2.3. *Concepto y clases de datos*

Los datos generados por empresas, Administración y ciudadanos están creciendo a nivel exponencial constituyendo el fuel de la llamada «sociedad de la información» y de la economía de los datos. Para definir el concepto «dato» podemos acudir a la Norma ISO/IEC 2382 -I, que lo define como la «representación reinterpretable de información de una manera formalizada, adecuada para la información o el procesamiento»[33]. Es decir, se trata de unos valores que reflejan situaciones o hechos que se producen y que permiten recrear o conocer una realidad, una representación simbólica, ya sea numérica, alfabética, algorítmica, espacial, etc.) que describe hechos empíricos y puede surgir de distintas fuentes: una imagen de una cámara de tráfico, una fotografía, un mensaje en redes sociales, la temperatura de una habitación etc.[34] En resumen, el «dato» sería una información codificada y legible por una máquina[35].

[32] Lo señalan CASTILLO PARRILLA, José Antonio y FERNANDEZ BASSO, Carlos, «Perfiles abstractos y propiedad intelectual», en *III Congreso Internacional de Derecho Digital*, CPO Universidad de Sevilla, 27 de junio de 2024.

[33] ISO/IEC 2382 -I: A reinterpretable representation of *information* in a formalized manner suitable for communication, interpretation, or processing. https://www.iso.org/obp/ui/es/#iso:std:iso-iec:2382:-1:ed-3:v1:en

[34] VIZCAINO DELGADO, Diego, ROMERO PANIAGUA, María, LLORENTE PINTO, Alejandro, Dir.: Emilio ONTIVEROS BAEZA, Coord. Verónica PÉREZ SABATER, *Economía de datos. Riqueza 4.0,* Ed. Fundación Telefónica, Madrid, 2018, p. 23.

[35] ZECH, Herbert, «Data as Tradeable Commodity – Implications for Contract Law», septiembre 2017, Josef Drexl, (ed.) *Proceedings of the 18th EIPIN Congress: The New Data Economy between Data Ownership, Privacy and Safeguarding Competition*, Edward Elgar Publishing, publicado el 2 de noviembre de 2017. pp. 319-321. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063153

Debe distinguirse entre los datos no personales, datos que tratan «información asociada al usuario» o datos personales, que se caracterizan por poder identificar al individuo que los ha generado y que, por tanto, merecen una protección especial y gozan de un estatuto jurídico diferenciado.

El Tribunal Constitucional ha configurado la protección de los datos personales como un derecho fundamental autónomo en el marco del artículo 18.4 de la Constitución. De hecho, en las sentencias 94/1998, de 4 de mayo[36], y 292/2000, de 30 de noviembre[37], ha afirmado que dicho derecho consiste en «un poder de disposición y control sobre los datos personales que faculta a la persona para decidir cuáles de estos datos proporciona a un tercero, sea el Estado o un particular, o cuáles puede recabar este tercero». Este derecho también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. El artículo 3 de la LOPDgdd[38] contempla el acceso a los datos personales del fallecido que se solicitará ante el responsable o encargado del tratamiento. En este caso los legitimados coinciden con los previstos en el artículo 96, si bien las facultades que pueden ejercer lo serán de acceso, rectificación o supresión, salvo prohibición del fallecido, que no podrá afectar al acceso de los herederos a los datos de carácter patrimonial del causante.

Sin embargo, cuando analizamos el aspecto patrimonial de los datos nos damos cuenta de que ha de realizarse desde una perspectiva muy distinta a la personal. Los datos puntuales de una sola persona considerados por sí solos cuentan poco desde la perspectiva patrimonial. Para que lleguen a tener valor y se conviertan en activo económico debe realizarse un análisis de datos. De hecho, la innovación tecnológica avanza a gran velocidad en la obtención, procesamiento y análisis de datos fortaleciendo las posibilidades expansivas de la economía de datos.

3. EL ACCESO A CONTENIDOS Y SERVICIOS DIGITALES MEDIANTE EL MODELO *PAY OR OK*, ¿OPCIÓN LEGÍTIMA O PRÁCTICA CONTRARIA A DERECHO?

Debemos distinguir entre *cookies* técnicas, como, por ejemplo, de memoria caché, y funcionales, que son las que permiten el rastreo. En este último caso la aceptación de *cookies* para acceder a contenidos o servicios digitales supone una transacción onerosa

[36] STC núm. 94/1998 de 4 de mayo, RTC 1998\94.
[37] STC (pleno) núm. 292/200 de 30 de noviembre, RTC 2000\292.
[38] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

implícita pues conlleva como contraprestación la cesión de datos generados por el usuario[39].

Hoy en día la población está hiperconectada con todo tipo de aplicaciones, generando una recopilación masiva de datos, por lo que la dimensión económica de los datos exige un tratamiento jurídico diferenciado de su tratamiento personalista. Esto provoca múltiples preguntas, como a quién pertenecen esos datos, cómo pueden valorarse económicamente y si el usuario que los ha generado podría participar en parte del lucro que generen. En primer lugar, vamos a analizar el concepto de dato como activo económico

3.1. *El dato como bien digital, su faceta económica*

3.1.1. El debate sobre la función económica de los datos

Conforme a José Antonio Castillo Parrilla, los bienes digitales se pueden definir como entidades metajurídicas (no creadas por el Derecho) de carácter estático (frente a los servicios dinámicos) cuya relevancia jurídica viene determinada por su valor económico. Igualmente, propone un concepto funcional de bienes digitales como categoría jurídico-patrimonial adecuada para la distribución de la riqueza digital[40]. En el derecho español partimos de un acervo común que nos permite considerar esta cuestión desde una posición ventajosa en tanto que el Código Civil recoge en la categoría de bienes los inmateriales, dentro de los cuales pueden encontrar acomodo los datos digitales. En otros ordenamientos, como el alemán, esta posibilidad queda descartada debido al carácter restrictivo de su regulación en el BGB que solo observa los elementos corpóreos. En todo caso, los bienes digitales se caracterizan por tener unas cualidades comunes, pues son no rivales, infinitamente extensibles y espaciales[41]. A su vez, se pueden

[39] Vid. CÁMARA LAPUENTE, Sergio, «El régimen de la falta de conformidad en el contrato de suministro de contenidos digitales según la propuesta de Directiva de 9 de diciembre de 2015», *InDret, Revista para el Análisis del Derecho,* n.3.16, julio, 2016. https://indret.com/wp-content/uploads/2018/05/1242.pdf p. 22.

[40] CASTILLO PARRILLA, José Antonio, «Derecho al patrimonio digital. Bienes digitales y datos como bienes», *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, Dir. Antonio Troncoso Reigada, Ed. Civital Thomson-Reuter, Cizur Menor, 2021, pp. 4344-4347 y 4352. Este autor pone de manifiesto la dificultad causada por el hecho de que los bienes digitales *strictu sensu* no son objeto de venta sino de licencia de uso, lo cual en la STJUE de 3 de julio de 2012 se resolvió en el sentido de aplicar la regla de agotamiento por entender que la licencia de uso implicaba la transferencia del derecho de propiedad de la copia del programa de ordenador. Concluye que el problema es aceptar los bienes digitales como categoría jurídica.

[41] Danny QUAH, Danny, «Digital Goods and the New Economy», *Journal Research Gate Online*, publicado el 1 de abril de 2003. Consultado el 23 de julio de 2023.
https://www.researchgate.net/publication/4808107_Digital_Goods_and_the_New_Economy

clasificar en tres categorías distintas: bienes digitales en sentido estricto, contenidos digitales y datos[42].

Lo cierto es que en la Directiva 770/2019[43] ya no se hace referencia a la información de las personas como un valor comparable al dinero, ni se observa el acceso a los datos como objeto de contraprestaciones diferentes al dinero, tal como sí hacía el Considerando 13 de la versión que le precedió de 2015. De hecho, tras la Opinión del Supervisor Europeo de Protección de Datos de 14 de marzo de 2017[44] que desaconsejaba toda referencia a los datos como contraprestación o mercancía, en el Considerando 24 de la vigente Directiva 2019/770 se recoge ahora que los datos no pueden considerarse como una mercancía[45]. No obstante, como señala Castillo, esto se ajusta mal al texto del art. 3 de la propia Directiva 2019/770 en el que se hace expresa referencia a los contratos en los que el consumidor entrega datos personales a cambio de contenidos digitales, lo cual claramente se corresponde con el concepto de «contraprestación». En todo caso, si un dato es objeto de un intercambio oneroso debería ser considerado como mercancía[46]. Por otro lado, debe distinguirse entre los distintos derechos fundamentales, pues no todos merecen el mismo trato jurídico. Si bien el derecho fundamental a la vida no puede ser objeto de transacción económica, está comúnmente aceptado en las democracias occidentales que el ciudadano sí pueda disponer patrimonialmente de otros derechos fundamentales, especialmente del derecho al honor, intimidad personal y familiar y propia imagen. En el caso que nos ocupa, la cesión de datos personales, el derecho protegido está muy relacionado con el referido derecho al honor, intimidad personal y

CASTILLO PARRILLA y MORAIS CARVALHO, «*Pay or ok*. Pagar con datos personales», cit., p. 115. Señalan que el carácter de no rivalidad viene dado por el hecho de que en tanto bienes informacionales, su disfrute por un sujeto no condiciona ni limita el uso por otros; infinitamente extensibles, en tanto que su reproducción es ilimitada y a coste cero; y espaciales, por poderse encontrar en distintos lugares simultáneamente.

[42] CASTILLO PARRILLA, José Antonio, *Propuesta de construcción jurídica de los bienes digitales informáticos,* Tesis doctoral, Università di Bologna, 2018, quien concluye que los bienes digitales en sentido estricto son aquellos que solo pueden ser bienes en el entorno digital, es decir, fundamentalmente programas de ordenador, páginas web y sistemas y modelos de IA. Por otro lado, los contenidos digitales serían las obras de ingenio en soporte digital y los datos finalmente serían bienes informacionales, que no podrían ser calificados como obras de ingenio.

[43] Directiva (UE) 2019/770 del Parlamento europeo y del Consejo de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos digitales y servicios digitales.

[44] Supervisor europeo de protección de datos, Opinión 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 14 de marzo de 2017.

[45] Igualmente el Comité Europeo de Protección de Datos, Opinión 8/2024 p. 30 señala que los datos personales no pueden ser considerados como bienes comerciables.

[46] Igualmente, en el art. 119 TRLGDCU, transposición española de la Directiva 2019/770 se hace referencia a los «datos como contraprestación». Vid CÁMARA LAPUENTE, Sergio, «Un primer balance de las novedades del RDL 7/2021, de 27 de abril, para la defensa de los consumidores en el suministro de contenidos y servicios digitales. La transposición de las Directivas 2019/770 y 2019/771), *Diario La Ley,* nº 9881, 29 de junio de 2021, pp. 1-32.

familiar y propia imagen, por lo que *prima facie*, no encontramos una razón para atribuirle un trato jurídico distinto, salvo que se trate de datos personales que merezcan un nivel de protección superior[47].

A mayor abundamiento, debemos tener presentes los llamados «fines de mercadotecnia directa» y la «elaboración de perfiles de usuario» en el RGPD como utilidades económicas de los datos, consecuencia de su previa cesión por los usuarios que reflejan la realidad existente, pues, siguiendo a Galileo, *eppur si muove*[48]. A mayor abundamiento en el Considerando 150 la sentencia de 4 de julio de 2023 del TJUE trata sobre la libertad de consentimiento del usuario de una red social al tratamiento de sus datos, entendiendo que el consentimiento valía como base de legitimación y afirma que el hecho de conceder al usuario dos opciones –*pay or ok*- no es contrario a la libertad de consentimiento de acuerdo con el artículo 4.11 RGPD[49].

Esta sentencia se dicta a consecuencia de la cuestión prejudicial planteada por el Oberlandesgericht Düsseldorf, tribunal que se planteó dudas sobre la base para el tratamiento de datos en el cado enjuiciado. En concreto, la resolución de la Bundeskartellamt, es decir, la autoridad federal alemana de defensa de la competencia, que había sido impugnada ante el Tribunal Superior Regional de Düsseldorf, había prohibido a Meta Platforms Inc[50] determinados tratamientos de datos. Consideraba que debían prohibirse la inclusión en las condiciones generales de la referida plataforma (Meta Platforms Inc) de cláusulas que condicionasen el uso de la red social Facebook, por parte de usuarios residentes en Alemania, al tratamiento mediante el uso de *cookies* de sus datos concernientes a actividades realizadas tanto dentro como fuera de dicha red social, que finalmente se relacionan con una cuenta de Facebook, - es decir, datos off Facebook. Igualmente se prohibía el tratamiento de estos datos en base a condiciones generales anteriores que carecieran del consentimiento del usuario. En resumen, el

[47] CASTILLO PARRILLA y MORAIS CARVALHO, «*Pay or ok*. Pagar con datos personales», cit., p. 110, proponen como categorías de datos personales que deberían quedar excluidas de la comercialización: los datos genéticos, los datos biométricos y los datos relativos a la salud. En esta línea avanza la iniciativa de la construcción de un Espacio Europeo de Datos Sanitarios.
Vid. Alberto HIDALGO CEREZO, *Propiedad y patrimonio en el medio digital*, ed. Aranzadi, Pamplona, 2021.

[48] CASTILLO PARRILLA, «Derecho al patrimonio digital», cit., pp. 4355, 4358 y 4364.

[49] Sentencia de 4 de julio de 2023 del TJUE (ECLI:EU:C:2023:537. https://curia.europa.eu/juris/document/document.jsf;jsessionid=F3DD0CA874FF40844471F2F6AC22FD50?text=&docid=275125&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=97875.
CASTILLO PARRILLA y MORAIS CARVALHO centran su estudio de esta materia en: «*Pay or ok*. Pagar con datos personales», cit., p. 103. Hay que señalar que recientemente el Comité Europeo de Protección de datos (CEPD) ha dado su opinión al respecto (8/2024), «on valid consent in the context of consent or pay models implemented by large online platforms», 17 de abril de 2024.

[50] Meta, (Meta Platforms Inc) es una plataforma norteamericana propietaria y operadora de Facebook, WhatsApp, Instragram, y Threads, que en la UE opera como Meta Platforms Ireland.

Bundeskartellamt exigía que en las condiciones generales se reflejara claramente que sin el consentimiento del usuario no sería posible recoger dichos datos, ni ponerlos en relación con cuentas de Facebook, añadiendo y quizá esto sea lo más relevante – que el consentimiento no sería válido si se planteara como un auténtico requisito para poder acceder a la red social.

En la sentencia de 4 de julio si bien el TJUE afirmó que los usuarios debían disponer de «la libertad para negarse individualmente a prestar su consentimiento a operaciones particulares de tratamiento de datos que no sean necesarias para la ejecución del contrato, sin verse por ello obligados a renunciar íntegramente a la utilización del servicio ofrecido por el operador de la red social en línea»; por otro lado añadió en el FJ 150 que de ello se derivaba que «debía ofrecerse a dichos usuarios, en su caso a cambio de una remuneración adecuada, una alternativamente equivalente no acompañada de tales operaciones de tratamiento de datos». Por tanto el TJUE ha consagrado la fórmula *pay or ok*, señalando la doctrina como dicha fórmula se ha extendido de forma uniforme desde dicha fecha en todo tipo de páginas web, Facebook, periódicos digitales etc[51], y de hecho la Guía sobre el uso de *cookies* de la Agencia española de Protección de Datos señala que esta fórmula es idónea debiéndose ofrecer «una alternativa, no necesariamente gratuita, de acceso al servicio sin necesidad de aceptar el uso de *cookies*[52].

Ahora bien, Trujillo Cabrera plantea si esta alternativa *pay or ok* supone la prestación de un verdadero consentimiento libre. Por un lado, niega que de la sentencia del TJUE pueda deducirse una aceptación genérica de la fórmula *pay or ok*, pues se considera que es necesario un escrutinio caso por caso, que impide soluciones genéricas. Por otro, se refiere la sentencia del Tribunal Constitucional de 24 de febrero de 2020 que puso en duda que concurriese un consentimiento válido al uso de condiciones generales en contratación online cuando se realizan en una posición dominante y se redactan en un lenguaje de difícil comprensión para el usuario medio. En esta línea Trujillo recoge la opinión 8/2024 del Comité Europeo de Protección de Datos[53]*,* según la cual ofrecer exclusivamente una alternativa de pago a un servicio que incluya el tratamiento con fines de publicidad comportamental no es una solución óptima. Por el contrario, considera que debería poder ofrecerse a los usuarios una alternativa equivalente que no implicara ningún tipo de pago, como por ejemplo una versión del servicio con publicidad carente

[51] TRUJILLO CABRERA, «Los nuevos *cookies walls*», cit., pp. 77-78. Autor que, no obstante, presenta objeciones a esta fórmula, tal como veremos al tratar consentimiento como base de legitimación.
[52] https://www.aepd.es/guias/guia-”cookies”s.pdf
[53] Comité Europeo de Protección de Datos Opinión 8/2024 *on the Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms,* Bélgica, 2024.

de tratamiento de datos personales[54]. Por ello Trujillo concluye que la práctica *pay or ok* vulnera sistemáticamente los derechos fundamentales de los usuarios, criticando tanto la STJUE del caso C-252/21 como la Guía sobre el uso de *cookies* de la AEPD por la «rendija» que han abierto y por la que parece consagrarse esta fórmula.

Por otro lado, en la Guía 05/2020 del Comité europeo de Protección de datos, se afirma que los llamados «muros de *cookies* dan lugar a consentimientos no libres». No obstante, la doctrina propone interpretarlo conforme al criterio hermenéutico de la realidad social recogido, en el art. 3 del Código Civil, pues aunque estas guías suponen opiniones relevantes, no son vinculantes, no se trata de una interpretación auténtica y en todo caso han de evitarse interpretaciones que perjudiquen la realidad de la economía de datos[55]. Esta misma observación podemos hacerla a las posiciones que niegan validez al consentimiento prestado mediante la fórmula *pay or ok,* la cual en todo caso ha quedado refrendada por el TJUE[56].

3.1.2. Valoración de los datos como objeto de intercambio

La valoración o apreciación de los datos objeto de intercambio es otro reto pendiente al que el legislador debe dar respuesta. Como señala Weber, no es una tarea fácil y depende tanto del tamaño como de la calidad de la red en la que se encuentren los datos[57]. Igualmente, la consideración de un solo dato bruto (*raw date*) por sí solo, *prima facie*, no tiene significancia económica relevante, si bien potencialmente pueda tener un valor económico que crecerá al agruparse con otros datos. Es precisamente el procesamiento de conjuntos de datos lo que crea un valor económico añadido, a mayor tamaño del grupo de datos procesados, mayor valor tendrán los datos que contiene[58]. Señala Spanga que este comportamiento es justo el contrario al que caracteriza en general a los activos económicos[59]. Por tanto, es necesario la aplicación de una

[54] TRUJILLO CABRERA, «Los nuevos *cookie walls*», cit., pp. 102-103.
[55] CASTILLO PARRILLA y MORAIS CARVALHO, «*Pay or ok*…», cit., pp. 125-126.
[56] GARCÍA PÉREZ, Rosa María, «Datos como contraprestación: ¿El principio del fin del modelo "consiente o paga" en el acceso a los servicios digitales», *Actualidad Civil* nº 6, junio 2024, editorial La Ley. (pp. 1-29), p. 16, señala que en cada caso habría que analizar si el pago es proporcionado a la prestación recibida, pues de no existir correspondencia entre la remuneración y la contraprestación, resultando desproporcionada la cuantía del pago, considera que estaríamos ante una coacción que viciaría el consentimiento
[57] WEBER, Robert H., «Improvement of Data Economy Through Compulsory Licenses? ed. Lohsse, S.; Schulze, R., Staudenmayer, D. *Trading Data in the Digital Economy: Legal Concepts and Tools – Münster Colloquia on EU Law and the Digital Economy, Hart & Nomos Verlagsges,* 2017, Baden Baden, p. 158.
[58] GIL GONZÁLEZ, Elena*, El interés legítimo en el tratamiento de datos personales*, Ed. Wolters Kluwer, Madrid, 2022, p. 29.
[59] SGANGA, Caterina, *Dei Beni in generale,* libro de la colección *Il Codice Civile Commentario: art. 820-821*, Dir.: Francesco Donato Brusnelli, Giuffrè Editore, Milan, 2015, p. 61.

tecnología para convertir los datos brutos y la información masiva en una información útil que resulte una mercancía o producto final. El valor económico de los datos vendría determinado por su utilidad, tanto si puede monetizarse como si no; y su valoración económica vendría determinada por las leyes de la oferta y la demanda[60], si bien la enorme casuística existente puede dificultar enormemente su estimación monetaria. En todo caso, el valor del conjunto de datos vendría determinado por la confianza que generen, conforme a la calidad de los datos, los algoritmos que los procesan y la seguridad de los entornos donde se almacenan[61].

Concluimos que permanece sin resolver el problema de cómo valorar los datos. La ruptura de la paradoja de la escasez plantea un problema que parece irresoluble. Si bien es cierto que los bienes mientras más escasos son, más valiosos son, con la revolución digital este paradigma ha cambiado. La lógica de los bienes físicos no es trasladable a los datos como bienes digitales. El dato tiene una capacidad de multiplicación de la que carecían los bienes pre-digitales, por lo que no es dependiente de la escasez. Mientras más datos estén disponibles en un sistema a ser procesado por IA, más valor podrá generar ese sistema de IA, más específico serán los perfiles abstractos que genere y por tanto, más valor tendrán dichos datos. Tampoco es posible encorsetar los datos con barreras como el copyright, que tan eficaces han sido en materia de propiedad intelectual, simplemente no se puede restringir el fluir de los datos poniendo puertas en el campo. La regla según la cual a mayor escasez, mayor precio quiebra cuando la aplicamos a los datos y esto impide aplicar las reglas generales de valoración económica de los bienes físicos a los datos como bienes digitales. A lo cual hay que añadir que habría que calcular cuán necesario es un determinado dato para obtener el «resultado final» teniendo en cuenta las características del algoritmo empleado. Por todo ello, la valoración del precio de mercado de los datos se presenta tan difícil, y la negociación de su «aprovechamiento económico» tan inasequible[62].

Es decir, solo en un primer momento, cuando se negocia la aplicación de la fórmula *pay or ok* entre el usuario y el prestador del servicio, es posible valorar económicamente el

[60] CASTILLO PARRILLA y MORAIS CARVALHO, «*Pay or ok*. Pagar con datos personales…», *cit.*, p. 114.

[61] CASTILLO PARRILLA, José Antonio, «Privacidad de grupo: Un reto para el derecho de protección de datos a la luz de la evolución de la inteligencia artificial», *Derecho Privado y Constitución*, 43, 2023, (pp. 53-88), p. 61. En este punto sigue a Jack M. BALKIN, «The three laws of robotics in the age of big data», *Ohio State Law Journal*, 78, 2017, p. 1220.
Señalan GÜNTHER, Wendy Arianne, MEHRIZI, Mohammad H. Rezazade, HUYSMAN, Marleen y FELDBERD, Frans, que las dos características sociotécnicas de los macrodatos que influyen en la obtención de valor son la portabilidad y la interconectividad. «Debating big data. A literatura review on realizing value from big data», *Journal of Strategic Information Systems*, 26, 2017, p. 192.

[62] CASTILLO PARRILLA, José Antonio, Seminario online sobre mercantilización de datos, Universidad de Granada, 23 de septiembre de 2024.

alcance de la cesión de los datos. Posteriormente, dicha valoración queda restringida por las dificultades prácticas que encontramos. Sin embargo, defendemos desde nuestra posición, como veremos posteriormente, la necesidad de encontrar una fórmula para poder valorar los datos y hacer coparticipe al usuario en la cotitularidad de los mismos. Si bien, a día de hoy dicha fórmula aún no es reconocible, no hemos hecho sino entrar en la era de la revolución digital, por lo que no es momento de precipitarse, sino de esperar a encontrar cimientos sólidos sobre los que construir una formulación jurídica sólida.

4. DISTRIBUCIÓN DE LA RIQUEZA GENERADA: LA TITULARIDAD DE LOS DATOS, LA DIFERENCIA ENTRE OPTAR POR UNA ECONOMÍA DE LA VELOCIDAD O UNA ECONOMÍA DE ESCALA

En el ciberespacio el mercado de datos se contempla como instrumento para el intercambio de todo tipo de datos, no solo los derivados, sino también los brutos y, por supuesto, los productos finales elaborados a partir de los datos[63]. Esto ha llevado a parte de la doctrina a defender que los datos se contemplen como bienes objeto de intercambio, siempre desde una perspectiva moderna del concepto «bien», que no lo vincula con el requisito de la corporalidad, como de hecho se sigue haciendo en el art. 90 del Código Civil alemán[64]. Por ello el Derecho ha de regular las transacciones patrimoniales que se dan en el ciberespacio, pues no es suficiente limitarse al enfoque personalista de los datos. El análisis de datos recogidos y procesados por tecnologías de tratamiento de *big data* en la era de la hiperconexión da lugar a un activo económico de primer orden que no puede ser legalmente preterido. Señala Thomas Hoeren que, en la sociedad de la información y la economía impulsada por los datos, los datos en sí mismos y el acceso a ellos incontestablemente son un factor económico decisivo, haciéndose eco de los planteamientos de la propia Comisión Europea que recoge: «los datos se han convertido en un recurso esencial para el crecimiento económico, la creación de empleo y el progreso de la sociedad»[65]. No sin razón se ha afirmado que los datos son el nuevo petróleo.

[63] CASTILLO PARRILLA, José Antonio, «Economía digital y datos entendidos como bienes», en *Mercado digital en la Unión Europea*, Dir. Paula Castaños Castro y José Antonio Castillo Parrilla, Ed. Reus, 2019, p. 284.

[64] LEHMANN, Michael, «A European Market for Digital Goods», en *European Contract Law and the Digital Single Market – The Implications of the Digital Revolution*. Ed. Alberto De Franceschi, Cambridge. Intersentia. 2016, pp. 111-126; y Herbert Zech, «Data as Tradeable… p. 79. Thomas HOEREN, «A New Approach to Data Property? », (2018) 2018/2 AMI, pp. 58-60 https://www.ami-online.nl/art/3618/a-new-approach-to-data-property Bernt HUGENHOLTZ, «Data property: Unwelcome guest in the House of IP», 2018 (https://www.ivir.nl/publicaties/download/Data_property_Muenster.pdf).

[65] HOEREN, Thomas, «A New Approach to Data Property?», (2018) 2018/2 AMI, p. 58-60, https://www.ami-online.nl/art/3618/a-new-approach-to-data-property .

Ahora bien, para afrontar este reto se ha de identificar previamente el tipo de economía digital de la cual ha de partirse. Como señala Castillo[66], será muy distinto si se parte de una economía basada en contratos de acceso o de licencia de uso a contenido digital, es decir una «economía de la velocidad»; o si por el contrario se priorizan contratos de adquisición para que el usuario pueda ser titular en propiedad, tal como ocurre con respecto a otros tipos de bienes no corpóreos, y de esta forma se promueva la circulación de la riqueza en una «economía de escala»[67]. Si bien, el escenario que hasta ahora se ha contemplado como adecuado para el desarrollo digital es el de la economía de la velocidad, encontramos voces y argumentos a favor de la economía de escala, pues quizá sea una opción más «democrática» que reparta la riqueza digital entre usuarios y empresas tecnológicas. En 2017 la propia Comisión se refirió a los bienes como objetos de cambio, intangibles y no rivales[68].

Desde la perspectiva de la economía de escala la transmisión del dominio de los datos se haría conforme a las distintas regulaciones estatales. En el caso de España mediante la *traditio* o entrega, conforme al artículo 1464 CC español referido a los bienes inmateriales. Por tanto, en situaciones de pago con datos, tal como señala Castillo, la transmisión se considerará hecha cuando el usuario sea consciente de que sus datos queden en poder y disposición del comprador y los use conforme a las finalidades que se hayan estipulado. Ahora bien, para que dicho consentimiento pueda ser considerado como una contraprestación, el tratamiento de datos debe tener precisamente como base de legitimación el consentimiento del usuario[69].

Si se opta por la opción de la «economía de escala» encontramos diversas alternativas para encauzar su regulación. Helbert Zech aboga por una regulación de *novo ex profeso*[70], de lo cual podría deducirse que nos encontramos con un *tertius genus* con difícil acomodo en la regulación general de bienes, afirmación que no parece del todo exacta, pues los bienes digitales podrían quedar asimilados a los bienes inmateriales, y

Conforme al *European Data Market Study* 2021-2023, 2024, pp. 44-45, el crecimiento interanual de la economía de datos en los 27 estados miembros de la Unión Europea es del 9,3% y ya ha alcanzado los 544 millones de euros (2023).

[66] CASTILLO PARRILLA, «Economía digital…», cit., p. 289.

[67] RIFKIN, Jeremy, «La era del acceso: La revolución de la nueva economía», Ed. Paidós, 2000, Barcelona, p. 135.

[68] Comission Staff Working Document, on the free flow of data and emerging issues of the European data economy, Accompanying the document Communication and Building a European data economy. Bruselas, 10 de enero de 2017, SWD (2017), 2 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?url=CELEX:52017SC0002

[69] CASTILLO PARRILLA y MORAIS CARVALHO, «*Pay or ok*. Pagar con datos personales…», cit., pp. 106 y 116-117.

[70] ZECH, Herbert, «Data as Tradeable... », cit., pp. 319-321.

quedar contemplados en el Código Civil. No obstante, voces autorizadas abogan por esta opción, propugnando desarrollar un derecho de propiedad *ad hoc.*[71]

Lo cierto es que desde una perspectiva teórica encontramos bases jurídicas suficiente para defender la conveniencia de una redistribución de la riqueza digital entre los usuarios que las generan con su conducta digital y plataformas que los procesan con algoritmos e IA[72]. Problema distinto es determinar si esta construcción teórica se puede sostener en la realidad, si es posible aplicar esta teoría a la realidad digital, o si más bien resulta impracticable.

La doctrina[73] ha señalado que el titular de los datos debe ser tanto el particular que los genera con su conducta digital, como la entidad que los procesa para convertirlos en productos útiles[74]. No obstante, es una cuestión debatida, pues aunque hay coincidencia en la existencia de motivos para crear un derecho de propiedad sobre datos no personales y anonimizados a favor del productor de los datos[75], parte de la doctrina cuestiona que dicha opción sea realmente productiva y se discute su oportunidad por los riesgos que generaría[76]. Aunque el debate está abierto, no puede ignorarse la realidad

[71] CASTILLO PARRILLA y MORAIS CARVALHO, «*Pay or ok*. Pagar con datos personales…», cit., p. 116.

[72] Sin duda supone una importante fuente de inspiración en esta materia la lectura del libro de HIDALGO CEREZO, Alberto, *Propiedad y patrimonio en el medio digital. Fundamentos jurídicos y tecnológicos,* ed. Thomson Reuters Aranzadi, Cizur Menor, 2021, obra que se centra en la adquisición de contenidos digitales como motor de la revolución digital y en la que se estudia el problema desde la perspectiva del consumidor y el detrimento que sufren sus derechos fundamentales en el «exitoso» nuevo modelo.

[73] PUYOL MONTERO, Francisco Javier, *Aproximación jurídica y económica al Big Data,* Tirant lo Blanch, Valencia, 2015, p. 352.

[74] CASTILLO PARRILLA, «Derecho al patrimonio digital…», cit., p. 4360.

[75] DREXL, Josef, «Designing Competitive Markets for Industrial Data Between Propertisation and Access», *Journal of Intellectual Property, Information and Electronic Commerce Law*, 8, 2015, (pp. 257-292) p. 260, justifica el derecho de propiedad sobre los datos en tesis utilitaristas. Considera especialmente justificado el derecho de propiedad cuando la producción de los datos ha requerido de una gran cantidad de recursos.

[76] Por todos, STEPANOV, Ivan, «Introducing a property right over data in the EU: The data producer's right – an evaluation», *International Review of Law, Computers & Techonology*, Vol. 34, 2020, Issue 1, (pp. 65-86) p. 80. Refiere la «Tragedy of the anticommons» con relación a la propiedad de los datos, considera que el volumen generado, continuamente en aumento, y los riegos de solapamiento no lo harían factible. Para HUGENHOLTZ, Bernt P. , el volumen y la situación de continuo cambio de los datos impiden identificar un objeto constante que pueda quedar sujeto al derecho de propiedad, lo cual llevaría a la inseguridad jurídica, «Data Property: Unwelcome Guest in the House of IP», *paper* presentado en *Trading Data in the Digital Economy: Legal Concepts and Tools*, Münster, 2017, (pp. 1-17) pp. 12-13. https://pure.uva.nl/ws/files/16856245/Data_property_Muenster.pdf, visto el 17 de julio de 2024.

del mercado digital[77] en el que los datos funcionan como una mercancía objeto de transacción[78].

Han surgido distintas teorías[79] para hacer efectiva dicha redistribución[80], incluso manteniendo que dicha propiedad de los datos por el usuario podría repercutir positivamente en la protección y control de los datos[81]. Posiciones que acogen las limitaciones exigidas por la observación de los derechos fundamentales, y que incluso proponen superar modelos tipificados y optar por fórmulas imaginativas a la hora de regular este nuevo tipo de propiedad[82].

[77] Por otro lado, no debemos obviar que el Reglamento de Protección de datos aborda la cuestión de los datos generados por los Smart goods, (es decir por dispositivos inteligentes), los derechos del usuarios a conocerlos, los derechos de varias empresas al respecto, lo cual encuadra con el tema de la redistribución. Aunque el Reglamento no menciona específicamente los «smart goods», se pueden identificar varios artículos que se aplican a los datos generados por estos dispositivos, proporcionando un marco legal robusto para la protección de los datos generados por estos dispositivos, asegurando que los derechos de los ciudadanos sean respetados y que se promueva la transparencia y la responsabilidad por parte de las empresas.

[78] VILJOEN, Salomé, en «Data as Property? On the problems of pepertarian and dignatarian approaches to data governance», *Phenomenal World,* publicado el 16 octubre de 2020, se postula a favor de la propiedad de los datos pero como una forma de propiedad que debe someterse a una gestión común y recoge las iniciativas llevadas a cabo en Alemania a favor de considerar un derecho real el fideicomiso nacional de datos, comparando a las grandes empresas tecnológicas con las farmacéuticas que disfrutan de un derecho limitado sobre sus productos al servicio del bien público. https://www.phenomenalworld.org/analysis/data-as-property/, visto el 17 de julio de 2024.

[79] CASTILLO PARRILLA, «Derecho al patrimonio digital…», cit., p. 4362. Para Castillo esta atribución de titularidad sería similar a la que sucede en la propiedad intelectual y quedaría supeditada a la prevalencia de la normativa en protección de datos.

[80] ZECH, Herbert, en «Data as Tradeable Commodity – Implications for Contract Law», septiembre de 2017, Josef Drexl, (ed.) Proceedings of the 18th EIPIN Congress: The New Data Economy between Data Ownership, Privacy and Safeguarding Competition, Edward Elgar Publishing, publicado el 2 de noviembre de 2017, p. 74. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063153 , defiende que el derecho de propiedad de datos se sustanciaría sobre la información codificada o bits, independientemente de la información que contuvieran, los cuales se registrarían mediante distintas tecnologías, ya comentadas, a fin de poder ser analizados y convertidos en productos. Este registro de datos se realizaría a gran escala, por si en el futuro son útiles, y exige de dos componentes: la conducta del individuo que las genera y la tecnología que los procesa, por lo que su conversión monetaria debería redundar en ambas esferas y determinaría la titularidad del derecho de propiedad de datos.

[81] PURTOVA, Nadezhda, «Property rights in personal data: Learning from the American discourse», *Computer Law & Security Review,* Vol. 25, Issue 6, November 2009, (pp. 507-521) pp. 520-521.
Autor que considera que la apropiación está llamada a resolver el problema de la pérdida de control sobre la información personal.

[82] HUMMEL, Patrick, BRAUN, Matthias, DABROCK, Peter, «Own Data? Ethical Reflections of Data Ownership», *Philosophy & Technology,* Vol.34, 2021, pp. 567-569. Plantean las siguientes preguntas acerca de la propiedad de datos: ¿Qué datos son míos? ¿Qué garantiza el vínculo entre datos y propietario? ¿Son los datos sobre el sujeto? Si es así, ¿en qué sentido? ¿Es adecuada la noción de datos personales del RGPD? ¿Deberíamos referirnos en su lugar a conceptos alternativos? ¿Qué diferencia supone y debería suponer el hecho de que el sujeto esté explícitamente representado o mencionado en los datos? ¿Podrían las

Lo cierto es que sobre la propiedad de datos está todo por hacer. El problema que subyace no es solo el de la dificultad para valorar económicamente los datos, tal como hemos analizado anteriormente, sino también para calcular el porcentaje de atribución de propiedad al usuario y a la plataforma[83]; o los costes para hacer tales cálculos. Por otro lado si bien la cesión de datos puede ser trazada en determinados supuestos, de forma que, al menos en teoría, sería posible identificar el origen de los datos objeto de transacción económica, en el caso de perfiles digitales la dificultad se acrecienta, precisamente por tratarse de perfiles comportamentales totalmente desconectados de los usuarios que los han generado con su conducta digital. Por dicho motivo no sería posible conectar el perfil abstracto con los usuarios cuyos datos los han alimentado. Analizaremos todos estos problemas con más detenimiento al tratar sobre los posibles remedios ante la contaminación digital, si bien volvemos a señalar aquí que, creemos que, si bien, a día de hoy, parece que no es posible encontrar una fórmula que resuelva el problema de la redistribución de la riqueza digital, es necesario, por distintas razones, que veremos en su momento, que en un futuro, no lejano, sea factible tal redistribución[84].

diferencias en la explicitación -por ejemplo, datos anonimizados frente a datos personales- suponer una diferencia en los derechos de propiedad, y por qué? Señalan que la propiedad sobre los datos puede adoptar muchas formas diferentes y es compatible con diversos objetivos normativos y supuestos de fondo. Consideran que la capacidad de poseer datos en un sentido (cuasi) de propiedad viene determinada por la capacidad de comercializar o de abstenerse de alienar características íntimas, de proteger los datos, pero también de participar en iniciativas impulsadas por los datos y de utilizarlos en beneficio propio o de otros, por lo que es necesario tomarla en serio y fijar una regulación. Añaden que la comercialización se ha de ajustar a las limitaciones que imponen los derechos fundamentales en juego y que, en todo caso, puede servir para motivar su comercio, aprovechar el potencial económico de los datos y poner a los titulares de los datos en situación de venderlos y, por tanto, de recibir una parte del valor que se genere a partir de ellos. Por otro lado, entienden que el bien común condiciona este tipo de propiedad de forma que ha de buscarse un equilibrio entre la protección de los datos y su correcta distribución para que puedan ser compartidos. Todo ello les lleva a concluir que es necesario aceptar la propiedad de datos aunque no se acomode a un modelo tipificado, siendo incluso aceptable considerarla como un tipo de cuasi-propiedad a fin de redistribuir los recursos, reconociendo a los titulares de los datos.

[83] En este punto debemos remitirnos a la filosofía de la *EU Data Act,* aunque solo haga referencia a las relaciones interempresariales, y no al empoderamiento de los usuarios. *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828* (Data Act).

[84] Debemos referir el Reglamento de Gobernanza de Datos que regula los procesos y estructuras que facilitan la puesta en común voluntaria de datos, y los principios de la *EU Data Act* que determina en las relaciones interempresariales quien puede crear valor a partir de los datos y en qué condiciones. Se considera que, juntas, estas dos normas, contribuirán al establecimiento de un mercado único de datos en la UE, lo que en última instancia se entiende que beneficiará tanto a la economía europea como a la sociedad en general. El Considerando segundo del Reglamento (UE) 2022/868 relativo a la Gobernanza Europea de los Datos, afirma que: «Con el fin de hacer partícipes a todos los ciudadanos de la Unión en la economía basada en los datos, debe prestarse especial atención a reducir la brecha digital, a impulsar la participación de las mujeres en la economía de los datos y a promover los conocimientos técnicos

5. LAS CARENCIAS DE LA REGULACIÓN EUROPEA VIGENTE PARA AFRONTAR LA REALIDAD DE LOS PERFILES SINTÉTICOS

Los algoritmos son capaces de segmentar y usar técnicas de microsegmentación para aplicar un perfil sintético a determinado tipo de usuario y poder dirigirle una información de forma individualizada.

Esta dinámica no está completamente observada por el Reglamento de Protección de Datos europeo, pero es que si fuera observada tampoco sería útil porque el Reglamento está pensado para una dinámica digital propia de los años noventa o los dos mil, pero no para la realidad digital vigente. Es decir, el Reglamento controla cómo se genera la información, los consentimientos, el derecho al olvido, cómo se destruyen los datos…, pero no entra en la gestión que se realiza de los datos ya extraídos y procesados conforme al art.4.2 del propio Reglamento. El problema es que el dato gestionado, por ejemplo, en forma de estadística, ya no es un dato personal. El Reglamento se centra en la recogida, analítica y descripción de datos personales, pero una vez que se consigue un perfil comportamental no asociado a una persona, el Reglamento de protección de datos no entra en los pasos intermedios.

Téngase en cuenta que la analítica de datos funciona mediante recogida de datos de información masiva que es elaborada por un procesador que crea un perfil comportamental al que se le hacen preguntas muy simples, como, por ejemplo, si una imagen concreta se corresponde o no con un patrón (por ej., la imagen de un gato). De esta forma una máquina, a partir de una serie de patrones de comportamiento fundados en la lógica inductiva, determina si es probable o no que la imagen que es objeto de contraste con el patrón sea o no un gato. Ahora bien, el contraste puede tener muy diversos contenidos, pues en vez de tener por referencia la imagen de un gato, puede plantearse si una persona que reúna unas determinadas características es probable que cometa un delito o que tenga la intención de votar a un determinado partido político. Pueden contrastarse, igualmente, cuáles son los factores que probablemente influyan en la toma de decisión del voto por un determinado tipo de perfil. Todo ello se consigue por medio de técnicas de análisis y recolección de información. Pero la diferencia respecto a épocas anteriores es que ahora tenemos las herramientas necesarias para llegar a determinadas informaciones y conocimientos en dependencia de las preguntas

europeos de vanguardia en el sector tecnológico...» El Reglamento obvia que la forma más eficaz de hacer partícipe al ciudadano en la economía de datos es reconociendo que los datos son bienes económicos de los que podría ser cotitular el propio ciudadano.

que formulemos a la máquina, este conocimiento nos permite llegar a un producto final, que es un perfil abstracto[85].

El problema es que los perfiles abstractos como tales ni están regulados, ni sometidos al Reglamento europeo de protección de datos porque se trata de perfiles que no están asociados a personas, pues pueden ser usados independientemente de los sujetos de quien han sido extraídos los datos. El Reglamento se preocupa de todo el proceso necesario para que el perfil esté bien hecho desde el punto de vista de protección de datos, pero no se ocupa de cómo se hace uso de un perfil abstracto una vez elaborado. En todo caso, solo podría ser aplicable el art. 22 del Reglamento una vez nos situemos en la fase final de contraste. En resumen, los pasos para llegar al perfil comportamental abstracto sí están regulados por el Reglamento, pero los pasos intermedios antes de la realización del contraste quedan fueran del Reglamento. Por tanto, preguntas como si se pueden almacenar estos perfiles o cómo se pueden utilizar quedan sin contestar. El problema es que los perfiles abstractos pueden servir para identificar comportamientos de personas cuyos datos no se han incorporado a dichos perfiles abstractos mediante una simple aplicación del perfil a la persona[86]. Estos perfiles abstractos recogen características comunes que comparten las personas que componen un grupo, conforme a los criterios que marque el algoritmo. Lo importante es que este grupo no tiene que ser conocido socialmente, sino que es una creación funcional[87]. Se trata de un método de identificación de personalidades y comportamientos que ha sido largamente elaborado desde la psicología y otras ciencias sociales como, por ejemplo, en el desarrollo de técnicas de Programación Neurolingüística, Eneagrama o MBTI que ahora se aplican de forma masiva y con registros de datos inmensurables mediante algoritmos a la ciudadanía en general. Evidentemente, en tanto que estos perfiles comportamentales no se apliquen a una persona, no tendrán la consideración de datos personales[88]. En este sentido téngase en cuenta el artículo 4.1 RGPD a *sensu contrario*.

Sin embargo, el contraste del perfil abstracto con una persona identificada sí que generaría datos personales, a los que por tanto podría ser de aplicación el art. 22 del Reglamento, aunque al tratarse de un texto lacónico e impreciso existen múltiples vías de escape, especialmente para grandes empresas con gabinetes jurídicos potentes.

[85] CASTILLO PARRILLA y FERNÁNDEZ BASSO, «Perfiles abstractos…», cit.
[86] GIL GONZALEZ, «*El interés legítimo…*», cit*.,* p. 29.
[87] CASTILLO PARRILLA, «Privacidad de grupo…», cit*.,* p. 64.
[88] COTINO HUESO, Lorenzo, «Nuevo paradigma en las garantías de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial», en *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Dir. Lorenzo Cotino Hueso, Ed. Aranzadi, Navarra, 2022, p. 88.

Los dos primeros párrafos del art. 22 dicen que: «(1) Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. (2) El apartado 1 no se aplicará si la decisión: (a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; (b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o (c) se basa en el consentimiento explícito del interesado».

Evidentemente, hay múltiples y fáciles vías de escape. En primer lugar, cabe preguntarse cómo interpretar la palabra «únicamente» del párrafo primero (existe un cierto consenso doctrinal que considera que ha de interpretarse en el sentido de que si el humano sigue a la máquina en más del 70% de las ocasiones, se estaría dentro del automatismo[89]). Respecto a los «efectos jurídicos», sería el caso en el que, por ejemplo, si como consecuencia de la aplicación del algoritmo, se recibiera autorización para celebrar un determinado tipo de contrato. Sin embargo, el verdadero caballo de batalla del párrafo primero es lo que debamos de entender por «afectar significativamente», pues evidentemente debe hacer referencia a una situación muy relevante. Igualmente, las excepciones previstas en el párrafo segundo del art. 22 no dejan de ser problemáticas. Así, por ejemplo, cuando se hace referencia a la autorización de la UE, no debemos olvidar que sus propias normas obligan a la evaluación de solvencia para concesión de un crédito[90], ¿pero si una empresa usa técnicas de *microtrageting* a tal fin estaría amparada por la excepción?, ¿cuándo se puede considerar que media consentimiento intrínseco?[91]

[89] Se argumenta que el papel humano se convierte más en una «ratificación» de decisiones automáticas, que en un acto de la autonomía de voluntad. Esta dependencia de la máquina hace que el papel humano se diluya acercándose a la automatización total. En esta línea CHUI, Michael, GEORGE, Katy, MANYIKA, James, y MIREMADI, Mehdi, en «Hombre + máquina: Una nueva era de automatización en manufactura», ed McKinsey & Company, publicado el 7 de septiembre de 2017 https://www.mckinsey.com/capabilities/operations/our-insights/human-plus-machine-a-new-era-of-automation-in-manufacturing/es-ES

[90] El art. 18 de la Ley 5/2019, reguladora de los Contratos de Crédito Inmobiliario, obliga al prestamista a vincular la puesta a disposición del crédito al resultado de la evaluación de solvencia. En la misma línea el art. 18 de la Directiva de Crédito al Consumo 2023/2225.

[91] Debemos referir aquí la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 7 de diciembre de 2023 (asunto C-634/21, OQ vs. Land Hessen), STJUE 7.12.2023, procedimiento entre procedimiento entre OQ y Land Hessen, con intervención de SCHUFA Holding AG, se centra en la interpretación del Reglamento General de Protección de Datos (RGPD). El caso trata sobre la legalidad de dos prácticas relacionadas con el tratamiento de datos personales por parte de agencias de información comercial en Alemania: el *scoring* (calificación crediticia) y la conservación prolongada de información sobre

La UE quiere dar respuesta a estas cuestiones con el Reglamento de Microsegmentación política[92], mediante el refuerzo de la información con sistemas de prohibición de envío de mensajes políticos en determinadas fechas o la prohibición de la aplicación de técnicas de microsegmentación a menores, o estableciendo ciertas limitaciones, por ejemplo, en el futuro si un *influencer* desarrolla campañas de microsegmentación política deberá avisar a la autoridad competente. Igualmente, las plataformas de muy gran tamaño[93] y los *gatekeeper* tienen muy restringida su capacidad de hacer microsegmentación, según lo dispuesto por el art 5 del Reglamento de Mercados Digitales y el art. 38 del Reglamento de Servicios Digitales, especialmente respecto a menores, si bien son unas limitaciones que se aplican con carácter general y no solo con efectos políticos[94].

exoneración de pasivos. El TJUE concluye que el RGPD se opone a la conservación de información durante un largo periodo de tiempo después de la exoneración del pasivo insatisfecho, mientras que la práctica del *scoring* solo está permitida en circunstancias específicas. Además, la sentencia refuerza la protección de los derechos de los interesados, subrayando la necesidad de un tratamiento de datos adecuado, justificado y limitado en el tiempo, de lo cual deducimos que sí se permiten ambas técnicas en determinados supuestos y durante cierto periodo de tiempo (https://curia.europa.eu/juris/document/document.jsf?text=&docid=282187&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=1151346).

[92] El Reglamento (UE) 2024/900 sobre la transparencia y segmentación en la publicidad política, aprobado el 13 de marzo de 2024 por el Parlamento Europeo y el Consejo de la Unión Europea. Tiene como finalidad regular la segmentación y la transparencia en los anuncios políticos, en especial los dirigidos a usuarios dentro de la UE. Este reglamento tiene como fines prioritarios limitar el uso de datos personales en la publicidad política y evitar la manipulación de la información, garantizando un proceso electoral más transparente y equitativo, protegiendo así a los ciudadanos de campañas desinformativas y de influencias externas, para garantizar la integridad de las campañas electorales. Para ello establece obligaciones claras para las plataformas y servicios que difunden publicidad política, exigiendo que revelen información sobre cómo se segmenta a los usuarios para asegurar la transparencia, se considera que será una herramienta útil para luchar contra la injerencia extranjera en procesos electorales de la UE.

[93] El art. 33.1 e3l Reglamento de Servicios Digitales las define como: plataformas que tengan un promedio mensual de destinatarios del servicio activo en la UE igual o superior a cuarenta y cinco millones, y que sean designadas como tales por la Comisión de acuerdo con el procedimiento establecido en el art. 33.4 RSD. No obstante, el Comité Europeo de Protección de Datos incluye dentro de este concepto a los guardianes de acceso del Reglamento de Mercados Digitales y a las plataformas que tengan una posición dominante en el mercado y/o se sirvan del procesado de datos a gran escala. De hecho, la Comisión Europea ha publicado una lista de 19 grandes plataformas digitales, llamadas «Muy Grandes Plataformas en Línea» (VLOP) y «Muy Grandes Motores de Búsqueda» (VLOSE), que estarán sujetas a controles reforzados bajo la Ley de Servicios Digitales (DSA). Esta normativa se aplica a plataformas con más de 45 millones de usuarios mensuales en la UE. Algunas de las plataformas incluidas son Instagram, TikTok, Twitter, Amazon, Google Search, YouTube, LinkedIn, Wikipedia, y la App Store de Apple.

[94] Vid. el ya referido, Reglamento (UE) 2024/900, de 13 de marzo de 2024 sobre la Transparencia y Segmentación en la Publicidad Política,

6. EL ESLABÓN FINAL EN LA CADENA DE LA DIGITALIZACIÓN: LA CREACIÓN DE BURBUJAS DE POLARIZACIÓN Y EL DESAFÍO AL SISTEMA DEMOCRÁTICO VIGENTE

Puede decirse que todo comenzó en 2002 cuando la recién creada Google, llevada por la crisis que en la época sufrió *Silicon Valley,* decidió superar su política contraria a la publicidad. En aquel momento sus creadores se plantearon suministrar solo publicidad relevante para el usuario. Para ello cruzaron límites hasta entonces infranqueables e hicieron uso de toda la información que hasta entonces se había almacenado y analizado, a fin de mejorar el sistema, para redirigir la «publicidad de interés» hacia el usuario idóneo. Fue entonces cuando Zuboff[95] considera que nació el capitalismo de vigilancia, al cual describe como una arquitectura global de modificación de la conducta que amenaza con transfigurar la naturaleza humana en el siglo XXI, al igual que el capitalismo industrial transformó el mundo natural del siglo XX. Se trataría de un paso más en la era del Antropoceno[96], paso en el que una vez que se ha transformado el planeta completo, poniendo en riesgo absolutamente todos los ecosistemas existentes, se avanza hacia el último peldaño, esto es provocar la alienación digital del propio ser humano, posiblemente para que una «mayoría» quede a merced de una «minoría» con una agenda e intereses opacos. El escenario resultante se asimila a una colmena en la que unos pocos se lucran y una mayoría ve cercenados la autonomía de la voluntad, la libertad, la democracia y su futuro como seres humanos[97].

Todo este proceso que amenaza nuestra sociedad parte de herramientas de analítica de datos avanzada y sistemas de inteligencia artificial con los cuales es posible infundir pensamientos, sentimientos, estados de salud, perfilar al individuo y realizar inferencias acerca de su pasado, presente y futuro[98], y que de forma no disimulada persigue manipular la capacidad decisoria del individuo.

Asimismo, se expone a la mente humana a un constante flujo de información y actualidad —una especie de «torbellino permanente» o «tsunami informativo»— que mantiene al sistema cognitivo en un estado de agitación continua. Este ritmo impone una lógica del corto plazo, que resulta perjudicial para la democracia, ya que el pensamiento reflexivo y la toma de decisiones racional requieren tiempo. En este contexto, se observa que las personas tienden a actuar movidas más por sus emociones y sentimientos que por la razón, debido a que estos se procesan con mayor rapidez. La inmediatez no permite

[95] ZUBOFF, Shohana, *La era del capitalismo de la vigilancia,* p. 289.
[96] Vid. ARIAS MALDONADO, Manuel, *Antropoceno: La política en la era humana*. Ed. Taurus, Barcelona, 2018.
[97] ZUBOFF, Shohana, *La era del capitalismo de la vigilancia,* p. 289.
[98] CASTILLO PARRILLA y MORAIS CARVALHO, «*Pay or ok*. Pagar con datos personales…», cit., p. 110.

verificar la veracidad de la información recibida, lo que contribuye a que las noticias falsas capten más atención que los hechos comprobados. Esta es una cuestión estudiada en profundidad por Byung-Chul Han[99] en su obra «Infocracia», autor que subraya como los smartphones se han convertido en dispositivos de registro psicométrico que se alimentan de datos minuto tras minuto. El procesamiento de estos datos, su transformación en perfiles genéricos y la comparación con posibles electores posibilita el envío de contenidos personalizados diseñados para incidir en el subconsciente de las personas. Por ello el autor referido afirma que «La infocracia basada en datos socava el proceso democrático, que presupone la autonomía y el libre albedrío»[100].

Si bien el tratamiento de datos podría en principio quedar justificado por ser necesario para lograr la publicidad comportamental en línea, creando perfiles de usuarios que mediante contraste quedan enlazados a determinados perfiles abstractos conforme a los intereses de los propios usuarios, sin embargo, esta técnica es también una vía para crear burbujas digitales y puede ser usada para fines que sobrepasan la mera publicidad. Señala Han que la microsegmentación hace que de forma encubierta cada grupo de individuos reciba una información diferente y en ocasiones contradictoria convirtiéndolos en ganado manipulable. Considera que todo ello contribuye a la polarización y división de la sociedad, dando como resultado el envenenamiento del discurso y una auténtica guerra de información en la que no vencen ya los mejores argumentos, sino los mejores algoritmos, por lo que la verdad y la veracidad ya no son relevantes[101]. Es decir, mediante las técnicas de la microsegmentación se crean burbujas de polarización que funcionan como compartimentos estancos a fin de influir en el subconsciente de los miembros del grupo y poder manipularlos políticamente. Por ello la red no crea ni opinión pública, ni acción política, no escucha[102]. Estas burbujas cerradas viven ajenas a la existencia del otro; en ellas no hay espacio para el diálogo ni para la confrontación democrática de ideas. La posibilidad de empatía entre personas con

[99] Exponemos en este párrafo el pensamiento de HAN, Byung-Chul, *Infocracia, La digitalización y la crisis de la democracia*, trad. Joaquín Chamorro Mielke, Ed. Penguin, Madrid, 2022, pp. 33-35.

[100] HAN (ibid., p. 36), afirma que «en la microsegmentación los votantes no están informados del programa político de un partido, sino que se los manipula con publicidad electoral adaptada a su psicograma y no pocas veces con *fake news*». Pone como ejemplo el caso de los Estados Unidos y Canadá donde afirma que los votantes son inundados por noticias falsas enviadas por robots, también son manipulados creando estados de opinión inexistentes inflando de manera artificial el número de seguidores (p. 39).

[101] HAN (ibid., pp. 39-42) afirma que la cultura de la inmediatez hace que las noticias falsas sean consideradas como información, pues producen todo su efecto antes de que se ponga en marcha un proceso de verificación. En otras palabras, que la información es más veloz que la verdad, y por tanto no puede ser alcanzada por esta, por lo que la «información falsa» es resistente a la verdad.

[102] HAN (ibid., p. 59) denomina «*racionalidad digital*» a esta forma de racionalidad que prescinde de la comunicación y del debate. El problema es que «la inteligencia artificial no razona, sino que computa. Los algoritmos sustituyen a los argumentos».

distintas condiciones desaparece, y las opiniones se tornan rígidas, cerradas sobre sí mismas, sin apertura al disenso: lo único válido es reafirmarse en las propias creencias. No es que la información contraria no llegue, sino que es descartada de inmediato por percibirse como una amenaza a la identidad personal y a la verdad absoluta que se asume como incuestionable. La exaltación del yo ha desplazado a la esfera pública como espacio común, y el otro deja de ser interlocutor para convertirse en adversario.[103].

Vattimo resume este desafío de forma magistral al señalar que en el postmodernismo lo importante no son los hechos, sino sus interpretaciones, lo importante es el relato impuesto por los medios, independientemente de si es verdad o no[104]. Por ello Habermas denuncia la disminución de la capacidad de persuasión en las sociedades civiles mediante convicciones políticas y culturales y orientaciones de valores de las que, en última instancia, deberían nutrirse los procesos democráticos.[105]

Finalmente, la revolución digital no solo supone un reto para determinados derechos fundamentales, sino también al propio sistema democrático y la propia noción del ser humano. Desde la perspectiva dataísta la democracia de partidos dejará de ser útil dentro de poco y la política será reemplazada por una gestión de sistemas basada en datos. El conductismo digital supera la noción del ser humano libre y autónomo y se centra en el colectivo, concibe a la sociedad como un organismo funcional[106]. Por eso, después de más de siglo y medio, el pensamiento de Gierke[107] vuelve a estar vigente. Un pensamiento que, no debemos olvidar, sirvió de fundamento al nazismo.

[103] Recojo en este párrafo el pensamiento de Byung-Chul HAN, «*Infocracia…*», cit., pp. 43-55.
[104] VATTIMO, Gianni, *Addio a la veritá,* Ed. Melteme, Rome, 2009. Como señala SCHELER, Max, el ser humano vive hoy preso en el relativismo, pues por primera vez ya no sabe quién es, pero simultáneamente es consciente de su falta de conocimiento, lo cual lo convierte en un ser problemático. Citado por EILENBERGER, Wolfram, *Tiempo de magos*, Ed. Taurus, Madrid, 2019, p. 29.
[105] HABERMAS, «Moralischer Universalismus…», cit., p. 7, considera que los signos de regresión política en las democracias occidentales son aterradores, sin que se pueda apreciar ni una alternativa normativamente convincente para preservar los principios constitucionales, ni una forma estable de «democracia iliberal» que sea compatible a largo plazo con los requisitos funcionales de las sociedades modernas dominadas por el mundo digital.
[106] HAN, «*Infocracia…*», cit., pp. 57-70.
[107] La teoría orgánica o antropomórfica, fue formulada por GIERKE, Otto von, en *Das Deutsche Genossenschaftrecht*, obra escrita entre 1868 y 1881. Desde esta óptica se considera que la persona colectiva quiere y obra por medio de sus órganos, hay una ligazón orgánica sobre los miembros que conforman la persona colectiva, que es un ente único, pero simultáneamente colectivo. Opinaba que la persona jurídica era un ente compuesto de seres humanos que conformaba una nueva personalidad de un orden más alto, dotada de voluntad propia y con esfera de vida propia. Afirmaba que «la corporación es una unión de individuos con una personalidad que brota de sí misma: su alma es una voluntad común unitaria; su cuerpo, un organismo social».

La digitalización ejerce hoy un paternalismo que crea una humanidad infantilizada, que se configura como un enjambre entregado al consumo, que ha sumido a las democracias occidentales en una crisis de identidad que las hace sucumbir ante una auténtica «dictadura tecnológica»[108]. Esta dictadura tiende a sumergir al ser humano en una libertad asistida, pues la saturación informativa le lleva a la delegación decisoria, dando lugar a un problema que no es solo moral, sino sobre todo político, pues el hombre-masa que describiera Ortega y Gasset está hoy más vigente que nunca. La consecuencia de esta transformación es lo que Lassalle denomina el «hombre *digitalis*»: un sujeto en situación de crisis, desplazado por la estructura digital que lo sustituye progresivamente. El problema no radica únicamente en la merma de derechos fundamentales, sino en algo aún más profundo: la pérdida de la capacidad humana para comprender e interpretar la realidad[109].

7. REMEDIOS JURÍDICOS ANTE EL RETO DIGITAL

El equilibrio entre el derecho a la protección de los datos personales y el de circulación de datos es difícil de alcanzar. En tanto que no es posible prohibir la libre circulación de datos en el actual ecosistema de la sociedad de la información basado en la economía de los datos, ha de optarse por establecer cautelas que protejan a los ciudadanos de los abusos que les acechan en el ciberespacio, especialmente en el ejercicio de sus derechos fundamentales tales como la libertad de expresión o el derecho de sufragio.

7.1. *Análisis de riesgos*

Procede el análisis de los riesgos que asoman tras la revolución digital y de los posibles remedios que desde el derecho podrían plantearse. Respecto a los riesgos, el envite del postmodernismo y del transhumanismo doblegan la visión humanista del ser humano y lo relegan a un nivel secundario frente al avance de la cibernética. El maridaje entre datos y algoritmos es el nuevo eje sobre el que gira el mundo, mientras que el ser humano deja de ser la medida de todas las cosas. Es precisamente aquí donde la libertad de la que está dotado el ser humano le puede permitir negarse a seguir los pasos diseñados para lograr su alienación digital. Norteamérica y China están desarrollando una guerra cibernética que fomenta la dictadura tecnológica. En este punto coincidimos con Lassalle en que es Europa quien puede ejercer un papel fundamental a la hora de ofrecer un diseño humanístico de la transformación digital[110]. En esta tarea podría estar

[108] LASSALLE RUIZ, *Ciberleviatá*n. *El colapso de la democracia liberal…,* cit.*,* pp. 18-20.
[109] En este párrafo se refleja el pensamiento del autor: LASSALLE RUIZ, *Ciberleviatán. ,* cit*.,* pp. 47-52.
[110] En este punto coincide plenamente con RIEMEN, Rob, en *Para combatir esta era. Consideraciones urgentes sobre fascismo y humanismo,* Ed. Taurus, traducción Romeo Tello, Madrid, 2017. Por otro lado, HARARI, Yuval Noah, en *Nexus: A brief history of information networks from the Stone Age to AI,* Ed. Vintage

acompañada de América Latina, en tanto que comparte unos mismos principios culturales. Por esta vía se podría poner de manifiesto la fragilidad de la «realidad digital» y reestablecer un equilibrio que respete la integridad y autenticidad del ser humano. Señala Lassalle que Este nuevo equilibrio debería traducirse en un acuerdo donde el Derecho asuma un rol central. Así como a finales del siglo XIX Estados Unidos logró impulsar leyes antimonopolio, hoy, en pleno siglo XXI, existe la posibilidad de frenar el avance hacia una forma de tiranía digital. Para ello, sería necesario limitar las grandes concentraciones de poder en el ámbito tecnológico, establecer mecanismos para regular —en la medida de lo posible— la propiedad de los datos, superar la noción de «consentimiento no informado» que Lassalle critica como insuficiente, someter los algoritmos a condiciones y límites, y promover un debate público que permita armonizar el desarrollo digital con los principios humanistas. Todo ello sin olvidar que la libertad solo puede sostenerse sobre la base del Derecho.[111]. A este propósito podría ser de gran utilidad el modelo de la Carta de Derechos Digitales que ha elaborado el Gobierno de España[112].

La sociedad de la información nos ha llevado a un escenario en el que según un sector doctrinal la opinión pública queda convertida en ganado manipulable por algoritmos de origen desconocido, mediante la técnica de la microsegmentación dirigida a amplias capas de posibles votantes, haciendo uso de todo tipo de *fake news*, teorías de la conspiración y mensajes individualizados cuya única finalidad es relativizar la realidad y privar a los ciudadanos de la posibilidad de un discurso democrático. La democracia está en peligro y, sin duda, en una situación precaria, pues la verdad no tiene oportunidad de imponerse sobre las *fake news* en una dinámica de rapidez mediática que no deja tiempo para procesar y contrastar la información recibida con apariencia de verdadera.

7.2. *Remedios jurídicos*

7.2.1. Luchas contra la contaminación digital

En segundo lugar, nos preguntamos cuáles son las opciones que tenemos para luchar contra estos desafíos que abaten nuestro sistema democrático. Si observamos esta materia desde el prisma de la contaminación digital podemos vislumbrar una perspectiva

publishing, London, 2024, pp. 15 y ss. igualmente afirma que ante la desinformación y la crisis existencial actual, determinada por la era de IA, es necesario optar por una «humanidad compartida» que pueda encauzar la IA dentro de unos parámetros respetuosos con la condición humana.

[111] LASSALLE RUIZ, *Ciberleviatán,* cit*.,* pp. 135-161. Recojo en este párrafo las conclusiones a las que llega en el último capítulo del libro.

[112] Vid. CÁMARA LAPUENTE, Sergio, «La propuesta de Carta de Derechos Digitales: reflexiones de derecho privado y técnica legislativa», *Diario La Ley*, nº 7, octubre-diciembre 2020, pp. 1-10.

jurídica que nos permite avanzar. Al igual que se ha afirmado que los datos son el nuevo petróleo, puede afirmarse que su procesamiento produce, al igual que el petróleo, una alta contaminación, caracterizada por una hipervigilancia omnipresente y por la pérdida del anonimato del ser humano. Al igual que la contaminación ambiental ha sido un perjuicio generado por la revolución industrial, la contaminación digital es un perjuicio generado por la revolución digital. Zuboff denuncia que esta contaminación implica una importante injerencia al libre albedrío humano, que puede quedar mediatizado por algoritmos que condicionan la conducta humana[113].

Partiendo desde esta perspectiva es necesario avanzar a partir de una concepción del derecho de protección de datos como un derecho fundamental de no injerencia por parte del Estado, gobernado por la autonomía de la voluntad de su titular, hacia un nuevo derecho fundamental de nueva generación que lucha contra la contaminación de las libertades amenazadas por las nuevas tecnologías. Pérez Luño, ya en 1991, en su magnífico artículo «Las generaciones de los derechos humanos», hace referencia a los derechos humanos de tercera generación, que supera las dos anteriores identificadas con las libertades de signo individual y con los derechos económicos, sociales y culturales. La tercera generación se presenta como «una respuesta al fenómeno de la denominada «contaminación de las libertades» tal como señala Pérez Luño[114]. Desde esta perspectiva puede considerarse el derecho a un entorno digital no contaminado como un derecho de tercera generación al igual que el derecho a un medio ambiente saludable[115]. Estos derechos de tercera generación exigen de una respuesta comunitaria conjunta de carácter global.

Por tanto, al igual que en el ámbito del derecho ya está previsto que las empresas que generen CO2 contribuyan a su neutralización por muy diversos medios, esto también podríamos extenderlo a las empresas que causan esta llamada «contaminación digital». Podría trazarse un paralelismo entre la lucha jurídica contra la contaminación medioambiental y la lucha jurídica contra la contaminación digital, adoptando medidas similares de carácter administrativo, fiscal, preventivo y sancionador.

7.2.2. Acciones de clase

Cabría la posibilidad de inspirarse en el derecho norteamericano y hacer uso de las acciones de clase o colectivas a fin de reclamar daños por contaminación digital, al igual

[113] ZUBOFF, Shohana, *La era del capitalismo de la vigilancia,* p. 589.
[114] PÉREZ LUÑO, Antonio Enrique, «Las generaciones de derechos humanos», *Revista del Centro de Estudios Constitucionales*, n. 10, 1991, pp. 206-208.
[115] Recoge estas categorías de derechos fundamentales CASTILLO PARRILLA, «Privacidad de grupo…», cit*.*, pp. 62-63.

que se permite ejercitar las acciones de clase para actuar contra las empresas que generan contaminación ambiental[116], supuesto que *prima facie* en España no prosperaría a día de hoy, pues solo se contemplan las acciones de clase en el ámbito del derecho de consumo. En hipótesis la técnica de las acciones colectivas permitiría dirigir estas acciones contra las grandes empresas responsables en última instancia de estos abusos. Pensemos, por ejemplo, en el caso de Cambridge Analytica que aplica técnicas de microsegmentación tanto al ámbito de la publicidad como de la política, mediante la aplicación de un modelo de personalidad llamado OCEAN, cuyo test invita a contestar a todo visitante de su página web. Cambridge Analytica informa en dicha página web de que «está construyendo un futuro en el que cada individuo pueda tener una relación verdaderamente personal con sus marcas y causas favoritas, mostrando a las organizaciones no sólo dónde están las personas, sino qué les importa realmente y qué impulsa su comportamiento»[117]. Por tanto, está mostrando al cliente los puntos débiles de cada grupo objeto de segmentación para influir en sus decisiones conforme a los «impulsos de su comportamiento». Lo cierto es que esta empresa extrajo indebidamente datos personales de Facebook que fueron usados tanto en la campaña electoral de Donald Trump para las elecciones presidenciales de 2016, como en la campaña del BREXIT en Reino Unido, datos que fueron usados para condicionar el voto. El colectivo que podría formar parte de la acción de clase estaría compuesto, por ejemplo, por todas aquellas personas que hubieran sido segmentadas digitalmente en grupos de comportamiento con fines que interfiriesen en el pleno ejercicio de sus derechos fundamentales. Lo cierto es que puede servir como un antecedente valioso en este camino la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) C-319/20 de 28 de abril de 2022, que estableció que las asociaciones de consumidores estaban legitimadas para actuar en defensa de la protección de datos personales[118].

[116] Estados Unidos está experimentando un verdadero auge de las acciones de clase relacionadas con la protección del medio ambiente, sirva de ejemplo la referencia a dos de los casos más recientes: *Maria Guadalupe Ellis, et al. v. Nike USA, Inc., et al.(* United States District Court, Eastern District of Missouri, publicada el 28 de marzo de 2024), y *Mayanna Berrin v. Delta Air Lines Inc (*District Court, C.D. California, 2:23-cv-04150, (C.D. Cal.) publicada el 8 de agosto de 2024). Por el contrario, en España el ejercicio de las acciones de clase queda limitado en el artículo 11 de la Ley de Enjuiciamiento Civil al ámbito del derecho de consumo, por lo que no son operativas frente al daño medioambiental. Quizá la única forma de encauzarla en España pudiera ser extendiendo la protección de los consumidores a la protección de datos, tal como apunta COTINO HUESO, Lorenzo, en «Nuevo paradigma…», cit*.,* pp. 83-85, y como recoge CASTILLO PARRILLA, «Privacidad de grupo…», cit*.,* p. 67. Si bien Castillo no ve viable el ejercicio de acciones colectivas en esta materia.

[117] https://cambridgeanalytica.org/products/

[118] Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) C-319/20, que entendió que las asociaciones de consumidores pueden presentar acciones judiciales (acción de representación) sin necesidad de un mandato específico de los individuos afectados. Esto se basa en el hecho de que el tratamiento de datos que afecta a los derechos de las personas identificadas o identificables permite a las

7.2.3. Daños morales y su posible reclamación mediante acciones de clase

Un paso más sería la posibilidad de reclamar daños morales a las empresas causantes de la contaminación digital. Se ha dicho que el problema para enfocar el asunto como daño moral es que se parte de perfiles sintéticos, es decir perfiles artificiales que no se identifican con personas concretas, pues ya no es necesario. Los datos se usan para construir perfiles de forma que se diluyen como un grano en un saco de arena: una vez hecho el perfil sintético se pierde su rastro. Por tanto, sería muy difícil individualizar una posible víctima de cualquier tipo de daño, si consideramos que la víctima es usuario del que se han extraído los datos. Sin embargo, el enfoque que proponemos es distinto, pues una vez realizados estos perfiles sintéticos, el algoritmo simplemente es capaz de identificar perfiles humanos reales que reúnan las características que se correspondan con el perfil sintético, mediante el contraste. Nuestra propuesta es considerar víctima precisamente a la persona sobre la que se ha realizado el contraste cuando, como consecuencia del mismo se haya sufrido cualquier tipo de daño o abuso. Esta opción permitiría obtener una indemnización, que podría ser elevada, sin necesidad de acudir a la lógica de los daños punitivos, no aplicables en Europa. Respecto a los daños morales, hay que decir que si una persona toma consciencia de que su autonomía de la voluntad ha sido condicionada o incluso manipulada haciendo uso de técnicas digitales y, por tanto, han quedado afectados derechos fundamentales básicos como el de libertad de expresión o el de libre sufragio, puede hacerse patente el daño moral que puede sufrir. En este caso la víctima no sería tanto el individuo cuyos datos han sido utilizados para generar un perfil comportamental abstracto (que no es identificable), como la persona que ha sufrido el hostigamiento digital por haber sido identificada como miembro del grupo al que se dirigía el algoritmo tras realizar el contraste.

Por otro lado, la dificultad que provoca la valoración de los daños materiales que puedan causarse a una determinada persona como consecuencia de sufrir un uso abusivo de perfiles digitales determina que la mejor vía para reclamar daños sea el recurso de los daños morales. Al igual que ocurre cuando se atenta contra el derecho al honor, intimidad personal y familiar y propia imagen, los daños morales se revelan como la mejor herramienta a favor de la víctima para obtener protección y compensación. Es cierto que ello provoca una cierta subjetivación por depender en última instancia de la

asociaciones actuar en interés público, buscando garantizar el respeto de los derechos establecidos por el Reglamento General de Protección de Datos. El caso en cuestión involucró a una asociación de consumidores alemana que demandó a Facebook Irlanda por supuestas infracciones relacionadas con el tratamiento de datos en el contexto de aplicaciones de juegos gratuitos. La decisión del TJUE enfatiza que no es necesario demostrar un daño específico a personas individuales para que estas acciones sean válidas. Vid. https://noticias.juridicas.com/actualidad/jurisprudencia/17291-las-asociaciones-de-consumidores-si-pueden-denunciar-infracciones-de-proteccion-de-datos-/?utm_campaign=twitter .

valoración pecuniaria que realice el juez *ex quo* en un caso concreto, valoración que ciertamente puede variar. No obstante al igual que dicha objeción no ha supuesto un verdadero obstáculo a la hora de admitir la compensación de daños morales cuando se atenta contra la intimidad personal, tampoco creemos que en este caso pueda suponer un obstáculo mayor.

En el caso de que existiera una previa relación contractual entre empresa e individuo, en cuyo marco se hubiese realizado el contraste, por ejemplo, caso de una plataforma que hiciera uso de los algoritmos para segmentar sus usuarios y hacerles llegar publicidad maliciosa o incluso información tendente para manipular sus decisiones, entre ellas las electorales, sí que nos encontraríamos en una relación entre empresario y usuarios que podrían ser calificados de consumidores, lo cual podría dar pie al ejercicio de las acciones colectivas o acciones de clase, de estos últimos frente a la empresa para reclamar colectivamente responsabilidad.

La dificultad ahora estaría en poder incluir daños morales en tal supuesto, si bien la doctrina ha señalado la viabilidad de esta posibilidad, lo cual podría abrir una nueva puerta para proteger a los usuarios/consumidores de forma efectiva[119]. Lo cierto es que

[119] MARÍN LÓPEZ, Juan José, afirma que en España las acciones de clase pueden ejercitarse para obtener indemnización de todo tipo de daños, lo cual viene permitido por la propia Ley de Enjuiciamiento civil al no hacer ningún tipo de distingo. Esto significa, que a diferencia de lo que ocurre en los EEUU, en el derecho español sí es posible reclamar daños morales, como parte del resarcimiento de los daños personales, cuando se ejercite una acción de clase. A lo cual añade Marín López que tampoco existe límite cuantitativo para el ejercicio de las acciones de clase, ni superior, ni inferior, por lo que su articulación procesal sería posible, cualquiera que fuera la cuantía de los daños que se reclamasen. «Las acciones de clase en el Derecho español», *InDret* 03/2001, p. 6. En la misma línea Aihnoa VEIGA TORREGROSA en «Class/Collective actions in Spain: overview», *Practical Law Country Q&A 4-617-9400*, publicado el 1 de noviembre de 2020, p. 14. https://www.araozyrueda.com/wp-content/uploads/2021/01/Classcollective-actions-in-Spain-overview-2021-DEF.pdf
La principal dificultad sería como cuantificar el daño moral de forma colectiva, sin atender a las circunstancias personales de cada individuo, sin considerar su «sufrimiento o padecimiento personal». Para tal supuesto podríamos guiarnos por la pauta recogida en la STJUE que refiero en el texto cuando señala que «no es necesario demostrar un daño específico a personas individuales para que estas acciones sean válidas», que por analogía podríamos trasladar al supuesto de daño moral.
Lo cierto es que en España hay precedentes en los que se ha intentado reclamar daños morales mediante el ejercicio de acciones colectivas, por ejemplo en el caso resuelto por el Auto de 28 de febrero de 2014 de la Audiencia Provincial de A Coruña, Sección 3ª, procedimiento instado por ADICAE contra NCG Banco (Caixa Galicia), ante el Juzgado de de Primera Instancia nº9 de A Coruña, procedimiento ordinario 41/2011. Adicae solictaba la devolución a los afectados de las cantidades pagadas, así como una indemnización por daños morales de 3000 euros para cada uno, superando en conjunto los 7,5 millones de euros en la reclamación. Vid. https://observatoriohipotecario.adicae.net/wp-content/uploads/2020/12/Libro-accion-colectiva-2014.pdf
Por otro lado, en Bélgica, la reciente transposición de la Directiva relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores (Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection

el TJUE en sentencia de 28 de abril de 2022 ha reconocido legitimación para ejercitar acción de representación a asociaciones de usuarios en defensa de la protección de los datos personales. La sentencia nos interesa porque considera que estas asociaciones pueden presentar acciones judiciales sin necesidad de un mandato específico de los individuos afectados y, muy especialmente, porque señaló que no es necesario demostrar un daño específico a personas individuales para que estas acciones sean válidas. Sobre la cuantificación de los daños morales en estas acciones colectivas podría servir de referencia la solución aportada por la Audiencia Provincial de Baleares en la sentencia de 12 de febrero de 2020[120], caso en el que se comprobó una manipulación fraudulenta en la venta de automóvil, consistente en la instalación de un software que desactivava las emisiones de NOx cuando detectaba que el vehículo estaba siendo objeto de un control de emisiones, para falsear los resultados de las mediciones de emisiones contaminantes, supuesto en el que se estableció el criterio de cuantificar los daños morales en 500 euros. Criterio seguido por otras AAPP y avalado por la STS de 11 de marzo de 2020[121].

of the collective interests of consumers and repealing Directive 2009/22/EC) ha extendido el campo de acción de las acciones de clase incluyendo la posibilidad de ejercitar acciones colectivas por daños morales, para lo cual se exige siempre la inclusión voluntaria. Debe destacarse que dicha previsión no se contempla directamente en la Directiva, si bien este precedente podría considerarse en la transposición española. Vid. RASKING, Lauren y VAN ESPEN, Loren, «New Law expands Belgian "class actions" framework», A & O Sherarman, publicado el 7 de junio de 2024. https://www.aoshearman.com/en/insights/new-law-expands-belgian-class-actions-framework Vid. «Demanda colectiva documento de base teórica 2022-2023», *Collective Redress-Spain,* Septiembre 2022, publicado por Consumerpro, p.23 consulta online 25 septiembre de 2024.
https://www.beuc.eu/sites/default/files/publications/consumerpro_redress_ES_2022.pdf
Por último, recientemente hemos visto como también en Chile se ha dado carta de naturaleza a este tipo de acciones en el ámbito del consumo, estando antes vedadas, vid. Eduardo REVECO SOTO, «Comentario a dos fallos erráticos que han estimado precedente la indemnización del daño moral en el marco de acciones colectivas. ¿Una antesala de su estandarización, quantum y determinación de los "montos mínimos comunes" indemnizables mediante la Ley nº21.081», *Revista de Derecho y Consumo* nº 3, agosto 2019, pp. 74-101. Por todo ello, parece que estamos ante un incipiente giro en la protección del consumidor en el ámbito colectivo que podría incluir el daño moral.

[120] SAP de Baleares de 12 de febrero de 2020, Ponente: Ilmo. Sr. D. Álvaro Latorre López, AC\2020\768,

[121] STS de 11 de marzo de 2020, pleno, Ponente: Rafael Saraza Jimena, RJ\2020\752. Debe tenerse en cuenta que tal como decía Díez-Picazo en su libro «El escándalo del daño moral» los tribunales instrumentalizan en ocasiones el daño moral para justificar así la concesión de daños (muchas veces materiales) que resulta claro que se han producido, pero que son de difícil o de muy costosa prueba para los perjudicados. En estos casos, se recurre al daño moral, cuya cuantificación corresponde a los tribunales sin necesidad de rigurosas pruebas. Es lo que parece que ha ocurrido en el caso de los fabricantes de automóviles que se recoge en estas sentencias. Esta forma de proceder por parte de la jurisprudencia hace que pueda ser factible una reclamación de daño moral en una acción colectiva, por la propia configuración que, en ocasiones, hace la jurisprudencia del daño moral. Cuando en un grupo de casos se instrumentaliza de esta forma el daño moral, se abre la posibilidad de poder ejercitar una acción colectiva, a pesar de que cuando nos referimos al daño moral propiamente dicho, que requiere de una individualización personal, dicha posibilidad no sería observable.

7.2.4. Vigilancia activa y restricción de uso de *cookies*

Castillo propone como herramientas útiles para intentar neutralizar la omnipresente contaminación digital, la prevención de la sobreemisión de consentimientos, el control de la calidad de los datos y realizar una interpretación integral del artículo 22 del RGPD[122]. La masiva recopilación de datos encuentra su principal título de legitimación en la aceptación de *cookies* por parte de los usuarios de internet. Por ello, el primer paso ha de ser la verdadera concienciación del usuario sobre qué es lo que consiente[123]. Estos datos extraídos de unos pocos serán usados para aplicárselos a miles mediante perfiles abstractos, produciendo una contaminación digital desmesurada. Por ello se propone: (1) Potenciar la vigilancia activa de las autoridades de control para garantizar la transparencia a fin de que el usuario sea verdaderamente consciente de la finalidad del tratamiento de datos a que consiente; (2) Regular y clarificar el pago con datos digitales; y (3) Concienciar sobre la trascendencia individual y social de estos consentimientos[124]. De esta forma, siguiendo la línea de las iniciativas ya iniciadas en el seno de la Unión Europea podrían establecerse restricciones para que el uso de *cookies* quedase limitado y que cuando se acceda, por ejemplo, a la lectura gratuita de un diario online, no sea necesario aceptar *cookies* o bien que esta aceptación no implique una contraprestación.

7.2.5. Limitación de los sistemas de IA de alto riesgo

El control de la calidad de los datos es esencial para encarar el desafío que supone la expansión de la Inteligencia Artificial. En esta línea resulta muy relevante el artículo 17 del Reglamento de Inteligencia Artificial[125] que establece un sistema de gestión de calidad que han de seguir los proveedores de sistemas de IA de alto riesgo[126], incluyendo el sistema de gestión de riesgos previsto en el art.9 y al establecimiento, aplicación y mantenimiento de un sistema de vigilancia poscomercialización de conformidad con el artículo 72. El Reglamento en el Anexo III considera de alto riesgo los sistemas de IA destinados a influir en el resultado de una elección o referéndum o en el

[122] CASTILLO PARRILLA, «Privacidad de grupo…», cit., pp. 68-81.
[123] GIL GONZÁLEZ, *El interés legítimo…,* cit., p. 69.
[124] CASTILLO PARRILLA, «Privacidad de grupo…», cit., pp. 71-72.
[125] Reglamento (UE) 2024/1689 de Inteligencia Artificial, de 13 de junio de 2024 constituye una aportación pionera, que si bien supera la Orden Ejecutiva presidencial de EEUU de 31 de octubre de 2023, que intentó regular la IA generativa y su investigación para aportar seguridad, sin embargo queda muy lejos de aportar verdaderos principios éticos, quizá por el miedo a que dicha introducción pueda limitar la carrera en la investigación frente a competidores avanzados.
[126] Los proveedores de alto riesgo están enumerados en el Anexo III del Reglamento e incluyen los sistemas de IA que formen parte de biometría (especialmente la identificación mediante biometría remota), infraestructuras críticas, educación y formación profesional, empleo, acceso a servicios privados esenciales y servicios y prestaciones públicos esenciales y su disfrute, garantía del cumplimiento del Derecho, migración, asilo y gestión del control fronterizo, administración de justicia y procesos democráticos.

comportamiento electoral de personas físicas que ejerzan su derecho de voto en elecciones o referendos, los cuales quedan sujetos al régimen establecido por el Capítulo Tercero del Reglamento (arts.8-15). Igualmente, en el considerando 67 del Reglamento se establece que el dato de calidad deberá ser pertinente, lo suficientemente representativo y, en la mayor medida posible, estar libre de errores y ser completo en vista de la finalidad prevista del sistema[127].

7.2.6. Distribución de la riqueza digital

Finalmente proponemos una última reflexión sobre el debate de comercialización de los datos, y la distribución de la titularidad dominical de los mismos. Se trata de un debate, aún abierto, al que hemos dedicado parte de este trabajo. Son muchas las voces que piden no volver la espalda a la realidad y reconocer que la recolección de datos se hace principalmente mediante acuerdos transaccionales entre partes, fundados en la aceptación de *cookies*. Estos acuerdos suponen pagar una contraprestación mediante el consentimiento al tratamiento de los datos digitales y, por tanto, suponen la mercantilización de estos datos personales. La Unión Europea debería aceptar que parte de dichas transacciones son aceptables desde el punto de vista jurídico, al igual que desde hace décadas se permite comerciar con el derecho a la intimidad y a la propia imagen. De hecho, ya se recogió que cuando se hacen contratos digitales se celebran transacciones económicas en los considerandos 13 y 14 de la propuesta 634/2015, que es la actual Directiva (UE) 2019/770 del Parlamento europeo y del Consejo de 20 de mayo de 2019, en la que se suprimió dicha referencia a los datos como activos económicos tras la queja y oposición del Supervisor europeo de datos. En todo caso, la STJUE del caso C-252/21 ha validado la fórmula *pay or ok*, que brinda a los usuarios la posibilidad de entregar datos o pagar dinero.

El siguiente paso sería plantearse una posible redistribución de la riqueza digital. Esta es una cuestión vital y pasa por considerar como titular de la misma, al menos en parte, al usuario que con su comportamiento ha generado los datos[128]. Se trata de dar respuesta

[127] Respecto a la gobernanza de datos el art. 10 del Reglamento establece que las prácticas de gobernanza se centrarán en (f) el examen atendiendo a posibles sesgos que puedan afectar a la salud y a la seguridad de las personas, afectar negativamente a los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión, especialmente cuando las salidas de datos influyan en las informaciones de entrada de futuras operaciones. Lo cual ha de ponerse en relación con el principio de exactitud del art. 5.1 RGPD y del art.4 LOPDGDD que señalan que los datos han de ser exactos y que deben adoptarse las medidas razonables para suprimir o rectificar sin demora aquellos datos personales que sean inexactos con respecto a la finalidad para la que se tratan.

[128] Podría plantearse, si en tal caso, dicha propiedad conllevaría responsabilidad. Se ha señalado que la responsabilidad del usuario parte de la libertad del consentimiento, de lo contrario estaríamos ante una irresponsabilidad que determinaría un desequilibrio contractual inaceptable. Alberto DE FRANCESCHI, *La*

a la necesidad de ofrecer una nueva distribución equitativa de la riqueza digital y reconocer el valor añadido que aporta el ser humano frente a las máquinas, a fin de poner coto al despotismo tecnocrático de unos pocos fundado en los datos[129]. Se afirma que de lo contrario los algoritmos convertidos en una IA hegemónica pueden terminar por esclavizar a la mayoría de la humanidad doblegada por el poder de los datos y sometida a la servidumbre de ceder la capacidad decisoria a dichos algoritmos, que están controlados por unos pocos[130].

Es el momento de profundizar en la aplicación práctica de esta opción teórica, que si bien puede tener apoyo jurídico, sin embargo, una parte importante de la doctrina ha señalado que puede plantear problemas que la hagan impracticable. El primero devendría de la dificultad de valorar los datos una vez realizada la transacción conforme a la regla *pay or ok*. Se trata de una cuestión ya mencionada anteriormente y que para la que, al día de hoy, no se encuentra respuesta adecuada, debido, principalmente, a la quiebra de la paradoja de la escasez, válida para los bienes físicos, pero no para los datos como bienes digitales, por lo que resulta muy difícil determinar su precio, a lo que ha de añadirse la dificultad de calcular el aprovechamiento económico que puede aportar un dato por las muchas variables que pueden concurrir, o el hecho de que los datos se reutilizan por lo que pueden incrementar su valor en el tiempo. Por otro lado, los datos no permiten que se les apliquen barreras legales que permitan que su tráfico jurídico se asemeje al tráfico jurídico de los bienes muebles físicos, los datos no dejan de ser mera información que va navegando por la red, no se puede limitar su circulación, por lo que no sería posible una solución paralela a las limitaciones legales establecidas en materia de propiedad intelectual. Por lo que concluimos siguiendo a Castillo Parrilla que no se pueden poner puertas al campo, por lo que el usuario ha de asumir que una vez cedido ha perdido el control económico del dato[131].

En segundo lugar, y respecto a la distribución de la riqueza digital, otro problema que ya hemos tratado sería el del cálculo de los porcentajes que deberían corresponder respectivamente a usuario y plataforma en la propiedad del dato, que en su caso, podrían derivarse de la obtención de dichos cálculos. En resumen, como señala Castillo Parrilla es muy difícil saber cuánto ha pesado la información de un determinado usuario en la alimentación de un algoritmo, y si fuera posible saberlo, su cálculo podría ser muy

circolazione dei dati personale tra privacy e contratto, Napoli, Edizione Scientifiche Italiana, 2017, pp. 55-56 y 111-117.

[129] LASSALLE RUIZ, *Civilización,* cit., pp. 138-139.

[130] Ibid., p. 140, quien refiere que la IA podría adoptar el papel de un demiurgo tecnológico.

[131] Recojo aquí un apunte de CASTILLO PARRILLA, Seminario online sobre mercantilización de datos, 23 de septiembre de 2024.

costoso. Autor que propone luchar contra esta erosión social en términos de privacidad colectiva causada por la segmentación digital de una forma alternativa, es decir, introducir un gravamen o tributo sobre las empresas que se nutren y generan la riqueza digital, que compense dicha erosión social, al igual que se impone un tributo a los carburantes o hidrocarburos[132].

Por último, señalar que en el caso de los perfiles digitales la identificación del usuario cuyos datos los han alimentado se plantea como una quimera, precisamente por la desconexión que se produce, ya que los datos contenidos en los perfiles sintéticos no son personales, al perder toda conexión con el usuario del que se tomaron. En otros casos, en lo que una empresa transmite directamente los datos de sus usuarios, el seguimiento podría ser factible, si bien, reiteramos que resulta desalentador el coste que este seguimiento podría implicar.

CONCLUSIONES

A partir del análisis de la regulación de esta materia a nivel nacional y europeo hemos propuesto posibles remedios para frenar la creciente contaminación digital y sus consecuencias para la sociedad democrática, aunque consideramos que el primer paso ha de ser analizar jurídicamente la realidad de los datos.

Entre los remedios propuestos nos hacemos eco de varias opciones propuestas por la doctrina. En primer lugar, y siguiendo a Castillo Parrilla, considerar la contaminación digital generada por un entorno de hipervigilancia digital creada por la revolución digital del mismo modo que la revolución industrial ha causado la contaminación de la naturaleza. Por tanto, sería viable hacer uso de distintas técnicas jurídicas de carácter preventivo, fiscal y sancionador al igual que se hace en la lucha contra la contaminación medioambiental. Debe ser de especial importancia garantizar que el usuario sea plenamente consciente del contenido y efectos del consentimiento que realiza y de la trascendencia social del mismo. Igualmente, la solución ha de pasar por la regulación del pago con *cookies* y en su caso excluir dicha opción o excluir que su consentimiento implique el pago con datos. Otras medidas han de ir en la línea del Reglamento europeo de Inteligencia Artificial que considera de alto riesgo los sistemas de IA «destinados a ser utilizados para influir en el resultado de una elección o referéndum o en el comportamiento electoral de personas físicas que ejerzan su derecho de voto en elecciones o referendos», estableciendo una regulación específica para estos supuestos en los artículos 8-15.

[132] Id.

La posibilidad de seguir el modelo de las acciones de clase norteamericanas contra la contaminación medioambiental y aplicarlo a la contaminación digital no sería, *prima facie,* factible en España, donde las acciones de clase se limitan al ámbito del consumo y, por tanto, no podría extenderse a supuestos de contaminación ambiental y por analogía de contaminación digital.

Por otro lado, podría plantearse la posibilidad de reclamar daños morales si se prueba que una empresa concreta, fruto del contraste con un perfil abstracto, ha segmentado a un individuo y ha influido en su conducta de forma perjudicial o maliciosa. De mediar previa relación contractual entre empresa e individuo, en cuyo marco se hubiese realizado el contraste, por ejemplo, caso de una plataforma que hiciera uso de los algoritmos para segmentar sus usuarios y hacerles llegar publicidad maliciosa o incluso información tendente para manipular sus decisiones, entre ellas las electorales, podríamos considerar que se trataría de una relación sujeta al derecho de consumo. Tal supuesto podría dar pie al ejercicio de las acciones colectivas o de clase. La dificultad ahora estaría en poder incluir daños morales en tal supuesto, parte de la doctrina ha defendido la viabilidad de esta posibilidad como vía efectiva para la protección de los usuarios/consumidores. Respecto al problema de la valoración del daño moral, podría servirnos de guía la STJUE C-319-20 ha admitido que las asociaciones de consumidores puedan presentar acciones judiciales sin necesidad de un mandato específico de los individuos afectados, añade que no es necesario demostrar un daño específico a personas individuales para que estas acciones ejercitadas por asociaciones de consumidores sean válidas.

En todo caso, creemos que debemos buscar las herramientas necesarias para neutralizar esta deriva. El reto es alcanzar el equilibrio entre todos los intereses en juego dando prioridad a los valores humanos sobre la tecnología.

La propuesta del reparto de la riqueza digital entre usuarios y empresas se presenta como una solución natural para luchar contra el desequilibrio abismal creado por la revolución digital. Sin embargo, cuando se transita del marco teórico a su aplicación práctica encontramos todo tipo de dificultades que parecen hacerla una propuesta impracticable. Problemas respecto a la propia valoración de los datos, cálculo del porcentaje de usuarios y empresas en caso de una copropiedad de los datos, costes que tendrían dichos cálculos, dificultad que presentan los perfiles sintéticos para seguir la huella hasta las personas cuyos datos se han incluido en los mismos, lo cual imposibilita todo control económico por el usuario, etc… De alguna forma las grandes plataformas deberían compartir con la sociedad el beneficio que obtienen de ella, pues lo datos digitales son generados a partir del comportamiento de los usuarios, en esta línea las herramientas tributarias podrían ser útiles.

No obstante, el desafío que supone la revolución digital, o si se prefiere la revolución de la IA, mediante la contaminación digital está provocando la debilitación y decadencia del propio sistema democrático, así como un creciente desequilibrio entre clases sociales, al concentrar toda la riqueza digital en manos de unos pocos, lo que está derivando a un creciente deterioro social. Por todo ello, estamos convencidos de que la solución ha de pasar por una nueva redistribución de la riqueza digital que termine con el absoluto monopolio de las grandes plataformas, e incluya a los ciudadanos como coparticipes de los nuevos bienes digitales. Por todo ello, es necesario encontrar un método para solidarizar la riqueza digital con el fin de hacer realmente partícipes a los ciudadanos en la economía basada en los datos.

BIBLIOGRAFÍA

ARIAS MALDONADO, Manuel, *Antropoceno: La política en la era humana*. Ed. Taurus, Barcelona, 2018.

BALKIN, Jack, «The three laws of robotics in the age of big data», *Ohio State Law Journal*, 78, 2017, pp. 1217-1241.

BAROCAS, Solon y NISSEBAUM, Helen, «Big data's end run around anonymity and consent», *Privacy, big data and the public good. Frameworks for engagement,* Eds. Julia Lane, Victoria Dtodden, Stefan Bender y Helen Nissebaum, Cambridge University Press, 2014, pp. 44-75.

CÁMARA LAPUENTE, Sergio, «El régimen de la falta de conformidad en el contrato de suministro de contenidos digitales según la propuesta de Directiva de 9 de diciembre de 2015», *InDret, Revista para el Análisis del Derecho,* n.3.16, julio, 2016. https://indret.com/wp-content/uploads/2018/05/1242.pdf, pp. 1-92.

CÁMARA LAPUENTE, Sergio, «Una perspectiva crítica sobre el régimen de los contratos de suministro de contenidos digitales», en *Derecho digital: retos y cuestiones actuales,* Aranzadi, Navarra, 2018, pp. 19-55, coord. M.A. Fernández Scagliusi, dirs.: F. Capillar Roncero, M. Espejo Lerdo de Tejada, F.J. Aranguren Urriza, J.P. Murga Fernández, 2018, pp. 19-55.

CÁMARA LAPUENTE, Sergio, «Los contenidos digitales como objeto de propiedad: aspectos problemáticos de su transmisión (en particular, en contratos con consumidores)», en *El derecho de propiedad en la construcción del derecho privado europeo,* coord. Elena Lauroba Lacasa y Jaume Tarabal Bosch, ed. Tirant Lo Blanch, 2018, pp. 325-363.

CÁMARA LAPUENTE, Sergio, «La propuesta de Carta de Derechos Digitales: reflexiones de derecho privado y técnica legislativa», *Diario La Ley*, nº7, octubre-diciembre 2020, pp. 1-10.

CÁMARA LAPUENTE, Sergio, «Un primer balance de las novedades del RDL 7/2021, de 27 de abril, para la defensa de los consumidores en el suministro de contenidos y servicios digitales. La transposición de las Directivas 2019/770 y 2019/771), *Diario La Ley,* nº9881, 29 de junio de 2021, pp. 1-32.

CÁMARA LAPUENTE, Sergio, «Nuevos perfiles del consentimiento en la contratación en la Unión Europea ¿navegar es contratar (servicios digitales "gratuitos")?», en *Estudios de Derecho contractual europeo,* dirs. Fernando Gómez Pomar e Ignacio Fernández Chacón, ed. Thomson Reuters Aranzadi, Cizur Menor, Navarra, 2022, pp. 331-405.

CARR, Nicholas, *The Shallows: What the Internet is doing to our Brains*, Ed. W.W. Norton & Company, Nueva York, 2010.

CASTILLO PARRILLA, José Antonio y MORAIS CARVALHO, Jorge, «*Pay or ok*. Pagar con datos personales tras la Directiva 2019/770: una visión comparada entre España y Portugal», en *Revista electrónica de Dereito*, junho 2024, nº2, Vol.34, pp. 100-144.

CASTILLO PARRILLA, José Antonio, «Derecho al patrimonio digital. Bienes digitales y datos como bienes», *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, Dir. Antonio Troncoso Reigada, Ed. Civital Thomson-Reuter, Cizur Menor, 2021, pp. 4337-4368.

CASTILLO PARRILLA, José Antonio, «Economía digital y datos entendidos como bienes», en el *Mercado digital en la Unión Europea,* Dir. Paula Castaños Castro y José Antonio Castillo Parrilla, Ed. Reus, 2019, pp. 279-301.

CASTILLO PARRILLA, José Antonio, «Privacidad de grupo: Un reto para el derecho de protección de datos a la luz de la evolución de la inteligencia artificial», *Derecho Privado y Constitución*, 43, 2023, (pp.53-88) p.61.

CASTILLO PARRILLA, José Antonio, *Propuesta de construcción jurídica de los bienes digitales informáticos,* Tesis doctoral Università di Bologna, 2018.

COBO ROMANÍ, Juan Cristóbal, *Acepto las condiciones – Usos y abusos de las tecnologías digitales,* Fundación Santillana, Madrid, 2019.

COTINO HUESO, Lorenzo, «Nuevo paradigma en las garantías de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial», en *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Dir. Lorenzo Cotino Hueso, Ed. Aranzadi, Navarra, 2022, pp. 69-105.

CHUI, Michael, GEORGE, Katy, MANYIKA, James, y MIREMADI, Mehdi, en «Hombre + máquina: Una nueva era de automatización en manufactura», ed McKinsey & Company, publicado el 7 de septiembre de 2017

https://www.mckinsey.com/capabilities/operations/our-insights/human-plus-machine-a-new-era-of-automation-in-manufacturing/es-ES

DE FRANCESCHI, Alberto, *La circolazione dei dati personale tra privacy e contratto*, Napoli, Edizione Scientifiche Italiana, 2017.

DOMÍNGUEZ YAMASAKI, María Isabel, «El tratamiento de datos personales como prestación contractual. Gratuidad de contenidos y servicios digitales a elección del usuario», *Revista de Derecho Privado*, N. 4, julio-agosto 2020, pp. 93-120.

DREXL, Josef, «Designing Competitive Markets for Industrial Data Between Propertisation and Access», *Journal of Intellectual Property, Information and Electronic Commerce Law*, 8, 2015, pp. 257-292.

EILENBERGER, Wolfram, *Tiempo de magos*, Ed. Taurus, Madrid, 2019.

FENOLLOSA, Carlos, *La singularidad*, ed. Arpa, 2024, Barcelona, pp. 9 y ss.

FINK, Leonard, «Big Data and Artificial Intelligence», *Zeitschrift für Geistiges Eigentum – Intellectual Property Journal*, Volume 9, 2019, fascículo 3, Band 9, pp. 288-298,

GARCÍA PÉREZ, Rosa María, «Datos como contraprestación: ¿El principio del fin del modelo "consiente o paga" en el acceso a los servicios digialtes», *Actualidad Civil* nº6, junio 2024, editorial La Ley, pp. 1-29.

GIERKE, Otto von, *Das Deutsche Genossenschaftrecht*, obra escrita entre 1868 y 1881.

GIL GONZÁLEZ, Elena, *El interés legítimo en el tratamiento de datos personales*, Ed. Wolters Kluwer, Madrid, 2022.

GÜNTHER, Wendy Arianne, MEHRIZI, Mohammad H. Rezazade, HUYSMAN, Marleen y FELDBERD, Frans, «Debating bid data. A literatura review on realizing value from big data», *Journal of Strategic Information Systems*, 26, 2017, pp. 191-209.

HABERMAS, Jürgen, «Moralischer Universalismus in Zeiten politischer Regression. Jürgen Habermas im Gesprächt über die Gegenwart und sein Lebenswerkt», en *Leviathan*, 48, 1, 2020, pp. 7-28.

HABERMAS, Jürgen, *Historia crítica de la opinión pública, La transformación estructural de la vida pública,* (*Strukturwandel der Öffentlichkeit),* Ed. Gustavo Gili (GG) Mass Media, trad. Antoni Domènech, 1982, 2ª edición, Barcelona/Buenos Aires/México.

HAN, Byung-Chul, *La digitalización y la crisis de la democracia. Infocracia,* Ed. Taurus, trad. Joaquín Chamorro Mielke, 2022.

HARARI, Yuval Noah, *Nexus: A brief history of information networks from the Stone Age to AI,* Ed. Vintage publishing, London, 2024

HIDALGO CEREZO, Alberto, *Propiedad y patrimonio en el medio digital*, ed. Aranzadi, Pamplona, 2021.

HOEREN, Thomas, «A New Approach to Data Property?» (2018) 2018/2 AMI p. 58-60 https://www.ami-online.nl/art/3618/a-new-approach-to-data-property

HUGENHOLTZ, Bernt P., «Data Property: Unwelcome Guest in the House of IP», paper presented at *Trading Data in the Digital Economy: Legal Concepts and Tools*, Münster,

2017, pp. 1-17. https://pure.uva.nl/ws/files/16856245/Data_property_Muenster.pdf, visto el 17 de julio de 2024.

HUMMEL, Patrick, BRAUN, Matthias, DABROCK, Peter, «Own Data? Ethical Reflections of Data Ownership», *Philosophy & Tecnology,* Vol.34, 2021, pp. 545-572.

LASSALLE RUIZ, José María, *Ciberleviatán. El colapso de la democracia liberal frente a la revolución digital*, Ed. Arpa, Barcelona 2019.

LASSALLE RUIZ, José María, *Civilización artificial*, Ed. Arpa, Barcelona 2024.

LEHMANN, Michael, «A European Market for Digital Goods», en *European Contract Law and the Digital Single Market – The Implications of the Digital Revolution*. Ed. Alberto De Franceschi, Cambridge. Intersentia. 2016, pp. 111-126.

MARÍN LÓPEZ, Juan José, «Las acciones de clase en el Derecho español», *InDret* 03/2001, pp. 1-13

PÉREZ LUÑO, Antonio Enrique, «Las generaciones de derechos humanos», *Revista del Centro de Estudios Constitucionales*, n.10, 1991, pp. 203-217.

PURTOVA, Nadezhda, «Property rights in personal data: Learning from the American discourse», *Computer Law & Security Review,* Vol. 25, Issue 6, November 2009, pp. 507-521.

PUYOL MONTERO, Francisco Javier, *Aproximación jurídica y económica al Big Data,* Ed. Tirant lo Blanch, Valencia, 2015.

QUAH, Danny, «Digital Goods and the New Economy», *Journal Research Gate Online,* publicado el 1 de abril de 2003. Consultado el 23 de julio de 2023. https://www.researchgate.net/publication/4808107_Digital_Goods_and_the_New_Economy

RAMÓN Y CAJAL, Santiago, *Reglas y consejos sobre investigación científica. Los tónicos de la voluntad,* Ed. Austral, 1898, Séptima impresión, 2020.

RASKING, Lauren y VAN ESPEN, Loren, «New Law expands Belgian "class actions" framework», A & O Sherarman, publicado el 7 de junio de 2024. https://www.aoshearman.com/en/insights/new-law-expands-belgian-class-actions-framework

RIFKIN, Jeremy, *La era del acceso: La revolución de la nueva economía*, Ed. Paidós, 2000, Barcelona, p. 135.

SGANGA, Caterina, *Dei Beni in generale,* libro de la colección *Il Codice Civile Commentario: art. 820-821*, dir.: Francesco Donato Brusnelli, Giuffrè Editore, Milan, 2015, p. 61.

STEPANOV, Ivan, «Introducing a property right over data in the EU: The data producer's right – an evaluation», *International Review of Law, Computers & Techonology*, Vol. 34, 2020, Issue 1, pp. 65-86.

VATTIMO, Gianni, *Addio a la veritá,* Ed. Melteme, Rome, 2009.

TRUJILLO CABRERA, Carlos, «Los nuevos *cookies walls*: "Consent or pay". A propósito de la Sentencia del Tribunal de Justicia de la Unión Europea de 4 de julio de 2023», *Revista de Derecho Civil,* vol. XI, N.2 (abril-junio 2024), Estudios, pp. 75-112.

VEIGA TORREGROSA, Aihnoa en «Class/Collective actions in Spain: overview», *Practical Law Country Q&A 4-617-9400*, publicado el 1 de noviembre de 2020. https://www.araozyrueda.com/wp-content/uploads/2021/01/Classcollective-actions-in-Spain-overview-2021-DEF.pdf

VILJOEN, Salomé, «Data as Property? On the problems of pepertarian and dignatarian approaches to data governance», *Phenomenal World,* publicado el 16 octubre de 2020, https://www.phenomenalworld.org/analysis/data-as-property/, visto el 17 de julio de 2024.

VIZCAINO DELGADO, Diego, ROMERO PANIAGUA, María, LLORENTE PINTO, Alejandro, Dir. Emilio ONTIVEROS BAEZA, Coord. Verónica PÉREZ SABATER, *Economía de datos. Riqueza 4.0,* Ed. Fundación Telefónica, Madrid, 2018.

WEBER, Robert H. «Improvement of Data Economy Through Compulsory Licenses? », Ed. Lohsse, S.; Schulze, R., Staudenmayer, D. Trading Data in the Digital Economy: Legal Concepts and Tools – Münster Colloquia on EU Law and the Digital Economy, Hart & Nomos Verlagsges, 2017, Baden Baden.

ZECH, Herbert, «Data as Tradeable Commodity – Implications for Contract Law», septiembre 2017, Josef Drexl, (ed.) Proceedings of the 18th EIPIN Congress: The New Data Economy between Data Ownership, Privacy and Safeguarding Competition, Edward Elgar Publishing, publicado el 2 de noviembre de 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063153

ZUBOFF, Shohana, *La era del capitalismo de la vigilancia. La lucha por un futuro humano frente a las nuevas fronteras de poder*, trad. Albino Santos Mosquera, Ed. Paidós Ibérica, 2020, Barcelona, París.

Fecha de recepción: 08.10.2024

Fecha de aceptación: 21.03.2025