DE LA FRAGMENTACIÓN, SEGMENTACIÓN Y DESCONTEXTUALIZACIÓN DE LA INFORMACIÓN AL *SPLINTERNET*: UN DERECHO A LA INFORMACIÓN EN MUTACIÓN EN LA ERA DE LA INTELIGENCIA ARTIFICIAL[1]

From fragmentation, segmentation and decontextualization of information to the splinternet: a mutation of the right to information in AI era

ROSA MARÍA GARCÍA SANZ[2]
Universidad Complutense de Madrid
rosamaga@ucm.es

Cómo citar/Citation
García Sanz, R. M.ª (2025).
De la fragmentación, segmentación y descontextualización de la información al *splinternet*: un derecho a la información en mutación en la era de la inteligencia artificial.
Revista Española de Derecho Constitucional, 135, 111-149.
doi: https://doi.org/10.18042/cepc/redc.135.04

Resumen

La fragmentación, segmentación y descontextualización de la información en las plataformas y el progresivo *splintering* de internet global, tanto por los Estados como por la empresas tecnológicas, han impactado en el derecho a la información, que manifiesta algunas «mutaciones». Un pacto global sobre la IA se presenta como la solución no solo para evitar el *splinternet*, sino también para reducir la problemática de la información/desinformación en las plataformas sociales.

---

[1] Este trabajo es consecuencia de una estancia de investigación en la Universidad de California Los Ángeles (UCLA) y parte del proyecto Ted2021-130876b-I00, «La ciberseguridad en los procesos electorales. Garantías frente a la desinformación y otros desórdenes informativos en plataformas» (2022-2023). Fondos Next Generation.

[2] Pocos días después de que nos enviase el texto definitivo de su trabajo, falleció la autora, víctima de un accidente. En esta publicación póstuma, la Revista expresa su pesar por esa inesperada tragedia.

Palabras clave

Inteligencia artificial; desinformación; *splinternet*; plataformas sociales.

Abstract

Fragmentation, segmentation and decontextualization of information on digital platforms and the progressive splintering of the global Internet, as much from governments as from the technological companies, are making a big impact on the right to information and leading to some "mutations". A global AI agreement looks like the right solution to avoid not only *the splinternet* but also the disinformation problems on social media.

Keywords

Artificial intelligence; disinformation; splinternet; social media platforms.

SUMARIO

I. INTRODUCCIÓN

La descontextualización, la segmentación y la fragmentación de la información[3] sirven de andamiaje a la desinformación y el disenso, lo que propicia la erosión del sistema democrático. Pero, además, la «desinformación», no en estricto sentido jurídico, sino como concepto técnico objetivado (como una abstracción política), señala las estrategias, maniobras y acciones de los sujetos que forman parte de la lucha por el poder en el ciberespacio[4]: entre el Estado y las empresas privadas tecnológicas, entre Estados y las diversas alianzas entre ellos. Este contencioso muestra una de sus expresiones en las operaciones de influencia indebida de actores tanto extranjeros como nacionales (guerra híbrida, amenazas híbridas), lo que, unido a un entendimiento desacertado de la (des)información (Herz y Molnar, 2012), podría inducir a las partes a sucumbir a la tentación de un total *splinternet*[5] (llamado también *balcanización*

[3] El conocimiento y uso de los datos por los algoritmos permite clasificar o segmentar a las personas y trocear o fragmentar la información conforme a ideologías o tendencias, la cual se descontextualiza al desplazarse desde su espacio y finalidad de origen a otros contextos de diferente naturaleza.

[4] Lucha que se manifestó desde los orígenes de internet: en los noventa, se proclamaba que el Estado no controlaría internet libre de fronteras; en los dos mil, se empezó a demandar que el Estado protegiera internet, tanto de las telecoms como de Gobiernos extranjeros. Después se ha confirmado, incluso para los libertarios, la doble posición: unos desconfían de los Estados, y otros, de las empresas tecnológicas privadas (Goldsmith y Wu, 2008). También véase: https://is.gd/KkkirN.

[5] La Internet Society explica el concepto, fusión de los términos *internet* y *split* («dividir», en inglés), que hace referencia a la creciente fragmentación de la red global, que podría conducir a los Estados o a las corporaciones tecnológicas a desgajarse del

de internet), lo cual significaría una histórica y rotunda vulneración del derecho fundamental a la información conforme al estado del arte. Probada la eficacia de las plataformas en reconducir la opinión pública mediante algoritmos[6] (inducida artificialmente y de dudoso valor democrático) (Rubio *et al*., 2024), e identificada la descontextualización de datos o información y de los espacios y tiempos, así como la fragmentación ideológica como causa y efecto de la segmentación[7], podrían, tanto el Estado como los mismos gigantes tecnológicos, alegar razones sobradas para «romper internet». La escalada de restricciones a internet (Bischoff, 2023), también en países democráticos, hace vislumbrar el camino que encabezaron China, Irán o Corea del Norte y, más recientemente, Rusia (Nachbar, 2022) al realizar el casi total *splinternet*, ejerciendo así el poder inmenso que ofrecen las tecnologías digitales. E incluso la idea de los metaversos[8] podría conducir a la fragmentación de la red global. La relación tensa

internet *backbone* y convertirse en *intranets* aisladas de la red global. Véase: https://is.gd/IkdvEA.

6 Todos los sistemas de inteligencia artificial (IA) en la UE deben someterse en el futuro a la normativa del Reglamento de Inteligencia artificial (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 (RIA). Este Reglamento, conforme al art. 113, «[s]erá aplicable a partir del 2 de agosto de 2026». No obstante, se establecen en el este tres períodos progresivos de aplicación de las distintas partes hasta 2027. El RIA se vertebra en torno a principios éticos: acción y supervisión humana; solidez técnica y seguridad; gestión de la privacidad y de los datos; diversidad, no discriminación y equidad; bienestar social y ambiental, y rendición de cuentas (Directrices éticas para una IA fiable, de 2019, elaboradas por el grupo independiente de expertos de alto nivel sobre IA creado por la Comisión). Y se complementará con el Convenio IA del Consejo de Europa de 9 de mayo 2024 (CIA), *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. Estados Unidos se adelantó y aprobó la Orden Ejecutiva Presidencial de IA el 30 de octubre de 2023: *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. The White House* (ya derogada en 2025 por el presidente Trump). Sobre la relación entre RIA y CIA, véase, por todos, Presno Linera y Meuwese (2024).

7 «Los algoritmos aprenden del comportamiento de los usuarios y, por tanto, influyen en nuestras acciones colectivas. Esto significa que nuestros prejuicios y tendencias se incorporan a las piezas de código que siguen influyendo en aquello a lo que estamos expuestos en línea, reflejando de nuevo estas tendencias de una manera generalmente amplificada» (Williams, 2021: 256).

8 Resolución del Parlamento Europeo, de 17 de enero de 2024, sobre los mundos virtuales: oportunidades, riesgos y repercusiones estratégicas para el mercado único (2022/2198(INI)).

pero interesada entre Estados y tecnológicas[9] invita, para trascenderla, a un nuevo contrato social, global e inclusivo (Estados, empresas privadas tecnológicas y ciudadanos) cuyo centro debe ser el pacto sobre la inteligencia artificial y sus algoritmos, con el fin de devolver al ciudadano el pleno ejercicio de sus derechos y evitar la posible balcanización de internet y los riesgos de censura y control absoluto que podría conllevar (AccesNow, 2023). Todo apunta a que sin un nuevo pacto social global es muy difícil la «gobernabilidad de la IA[10]» con el fin de sanar el proceso de comunicación pública digital y su impacto en la democracia, pues no resulta realista pensar que el Estado pueda prescindir de las plataformas (ni de los ciudadanos) para este fin[11].

La doctrina, en general, percibe que el derecho trata de asir sin éxito la nueva realidad digital y la transformación del poder basado en la tecnología (IA) de las empresas privadas tecnológicas, que se escapa a las riendas del Estado constitucional. Autores como Balaguer (2023: 32) entienden que el cambio de paradigma «pasa por la constitucionalización de la nueva realidad digital, sometiéndola a los principios y valores constitucionales y por la digitalización de la Constitución». Sin embargo, no se trata de «maquillar de digital» lo viejo, sino de abrirse a lo nuevo e identificar en la nueva realidad los valores y principios que subyacen (que podrían ser distintos). Estamos de acuerdo con Bustos (2024: 7) al afirmar que «una aproximación jurídico-constitucional defensiva (basada en los riesgos) es esencial, pero una aproximación proactiva (basada en las oportunidades) también es básica». Afrontar las problemáticas de los algoritmos (IA) en el Estado democrático exige enfocar el análisis en los derechos fundamentales y, especialmente, en el derecho a la información, por su papel tradicional de pilar de la democracia y su importancia incuestionable

9 Véase https://is.gd/jJn06M.

10 Bajo el paraguas del término «IA» existen multiplicidad de definiciones, campos y subcampos. Aquí nos ceñimos a las conceptualizaciones del RIA (art. 3) y del CIA (art. 2).

11 Resulta esclarecedor el esfuerzo del RIA por establecer un concepto común, consciente el legislador europeo de la importancia de un consenso al respecto. Así, el largo considerando 12 comienza: «Debe definirse con claridad el concepto de "sistema de IA" en el presente Reglamento y armonizarlo estrechamente con los trabajos de las organizaciones internacionales que se ocupan de la IA, a fin de garantizar la seguridad jurídica y facilitar la convergencia a escala internacional y una amplia aceptación, al mismo tiempo que se prevé la flexibilidad necesaria para dar cabida a los rápidos avances tecnológicos en este ámbito». Igualmente, la derogada Orden Ejecutiva de IA de Estados Unidos contiene previsiones en este mismo sentido. Y, sobre todo, el Convenio de IA del Consejo de Europa, por su vocación global y de derechos humanos.

entre los derechos fundamentales[12]. Sin duda, reseñan algunos autores (Sánchez Muñoz, 2024), en el cambio del sistema de comunicación digital se encuentra el origen del cambio de paradigma y el declive del sistema democrático actual. Así, se observa cómo la descontextualización, la segmentación y la fragmentación de la información han impactado en este derecho, y cómo el funcionamiento mismo de las plataformas lo ha desacoplado de su anclaje constitucional actual, con sus derivadas en el espacio público democrático (cuestión esta ya muy documentada en la literatura jurídica) (Rubio *et al*., 2024). Al mismo tiempo parece necesario identificar las trazas, que muestran signos de mutación, del nuevo modo de ejercer las libertades informativas mediante los algoritmos e inteligencia artificial (conscientes de las diferentes plataformas y modelos jurídicos, especialmente Estados Unidos/UE). Todo parece indicar que se está ante un derecho a la información en transformación y que se avanza hacia un nuevo orden de la comunicación, que podría accidentalmente degenerar, si no se adoptan las justas medidas, en un total *splinternet*.

II. DE LA FRAGMENTACIÓN, SEGMENTACIÓN Y DESCONTEXTUALIZACIÓN DE LA INFORMACIÓN EN LAS PLATAFORMAS DIGITALES A LA TENTACIÓN DEL *SPLINTERNET*

Al afrontar la problemática y la regulación de la IA (especialmente la de última generación), cierta doctrina encuentra muy útil la experiencia histórica, entre otras, de la protección de datos personales[13] (Bustos, 2024), lo cual no produce extrañeza, pues, como afirma Balkin (2018: 984), existe una íntima interconexión entre las libertades informativas y el derecho a la protección de datos personales (*privacy*), y se da la ironía de que cuanta más libertad de expresión, menos privacidad. La cuestión de los de datos personales es clave en la diferencia de los modelos legales Estados Unidos/UE, y que se ahonda con la regulación de la IA. También resulta útil remontarse a los comienzos de internet y a la misma transformación de lo analógico en digital en el ciberespacio, con todas sus disrupciones legales, sociales y económicas. Habría que recordar que el sistema tecnológico y organizativo tradicional de la comunicación se vio «revolucionado» por internet (Benkler, 2007) y puso en solfa todos los elementos clave para la formación de la opinión pública (medios de

[12] Así lo ha reiterado el Tribunal Constitucional: entre muchas, STC 165/1987, de 27 de octubre.

[13] Art. 10 y considerandos del RIA, entre muchos, 67 a 72 y 105, pues la cuestión de los datos (de todo tipo) es transversal en el Reglamento.

comunicación, partidos políticos, parlamento), con sus derivadas en los derechos de participación, que todavía están en proceso de transformación. La abundancia de información, que ya anunció Benkler (2007: 1), condujo a la escasez de atención, como anticipó Simon (1971), y los algoritmos supieron administrar eficientemente después. La misma digitalización de la información supuso su conversión en ceros y unos, o sea, en datos, y, por lo tanto, la cuestión del flujo de datos (personales/no personales o factuales) se vio precipitada, especialmente la protección de los datos personales, que, con los logros de las ciencias de la computación más tarde, el *big data* y la IA, se agravó[14]. En ese nuevo estadio de evolución, podría afirmarse que todos los datos, técnicamente, se pueden reconducir como personales en la red (la anonimización total no es posible en realidad —Barocas, 2014—). El libre flujo de los datos (información) propició su descontextualización, de la que advirtió Nissebaum (2010) como un ataque a la «integridad social», que luego los algoritmos (Barocas *et al.*, 2013) acelerarían llevándola «casi» hasta sus últimas consecuencias (Xu, 2024), con diversos fines (por la segmentación de audiencias, mercados o electorados) en redes, plataformas y motores de búsqueda, propiciando mensajes personalizados, aunque descontextualizados y fragmentados por la segregación de los usuarios en nichos (segmentación y microsegmentación). Los desórdenes informativos (*fake news*, desinformación, posverdad, discurso del odio —Herz y Molnar, 2012— o polarización) fueron surgiendo en este proceso (Hasen, 2022). Con la inteligencia artificial se entró en una nueva fase, que, a su vez, está siendo revolucionada con la IA generativa[15] y otros avances como las neurotecnologías, que plantean nuevos desafíos a los derechos, especialmente al derecho a la información y/o datos. Los modelos de IA generativa son, conforme al RIA, modelos de uso general que permiten la generación flexible de contenidos de texto, audio o vídeo (considerandos 97 y 99), con problemáticas propias.

---

[14] En Estados Unidos, en el caso *Sorrell v. IMS Health, Inc.*, 564 U.S. 552 (2011), el TS americano reconoció la libertad de datos como libertad de expresión.

[15] Véase, por todos, Rubio *et al.* (2024: 8): «A pesar de que la desinformación ha causado daños sociales incluso antes de la interiorización de las nuevas herramientas de IA, lo cierto es que la IA lleva el problema a una nueva dimensión. Las nuevas tecnologías promueven cambios cuantitativos y cualitativos en el almacén *de fake news*, ya que agilizan, abaratan y facilitan la fabricación circular de contenidos desinformativos, además de permitir formas más sofisticadas de engaño y manipulación, como los *deepfakes*. Además, la IA permite microsegmentar la comunicación a gran escala creando cámaras de eco e intensificando el sectarismo, la intolerancia ideológica y otros fenómenos que instrumentalizan habitualmente el extremismo y encienden el "reguero de pólvora" (Sunstein, 2020, p. 62) de la "cultura de la ira y la conspiración" (Fisher, 2023, p. 76)».

La emergencia de esta IA de última generación vuelve a poner en primer plano la cuestión de los datos. Datos que sirven a la necesaria ingesta de la IA para su entrenamiento y aprendizaje, que pueden ser de diferente naturaleza y protección jurídica (derecho a la protección datos personales, propiedad intelectual, propia imagen, derecho a la información, etc.) y entrar en conflicto[16]. Y es que, siguiendo el itinerario histórico, en el ámbito digital y computacional, los datos (en todo su espectro de categorías) son la materia prima compartida de distintos derechos, es decir, con el mismo objeto, aunque con bienes jurídicos protegidos diferenciados: entre los mencionados, el derecho a la información, a la protección de datos personales (y no personales), a la propia imagen y al derecho de autor y de la propiedad intelectual (Higueras, 1995). Objeto común que subyace en estos derechos[17] con una íntima interrelación entre estos y sus límites. Las llamadas *deepfakes*[18] son

[16] En Estados Unidos hay varios casos judiciales abiertos: *NY Times vs. OpenAI* (27/12/23); *Sarah Silverman et al. vs. OpenAI* (13/2/24); *Universal, ABKCO and Concord vs. Anthropic* (14/2/24), y *Reddit vs. Google* (22/2/24), entre otros. Por su parte, el Reglamento de Inteligencia Artificial hace referencia a esta confluencia de datos y derechos. Así, el art. 53, b) y c), y en el considerando 105 se lee: «Los modelos de IA de uso general, en particular los grandes modelos de IA generativos, capaces de generar texto, imágenes y otros contenidos, presentan unas oportunidades de innovación únicas, pero también representan un desafío para los artistas, autores y demás creadores y para la manera en que se crea, distribuye, utiliza y consume su contenido creativo. El desarrollo y el entrenamiento de estos modelos requiere acceder a grandes cantidades de texto, imágenes, vídeos y otros datos. Las técnicas de prospección de textos y datos pueden utilizarse ampliamente en este contexto para la recuperación y el análisis de tales contenidos, que pueden estar protegidos por derechos de autor y derechos afines. Todo uso de contenidos protegidos por derechos de autor requiere la autorización del titular de los derechos de que se trate, salvo que se apliquen las excepciones y limitaciones pertinentes en materia de derechos de autor. La Directiva (UE) 2019/790 introdujo excepciones y limitaciones que permiten reproducciones y extracciones de obras y otras prestaciones con fines de prospección de textos y datos en determinadas circunstancias». Además de tener muy presentes los datos personales y no personales, conforme se lee en el considerando 10.

[17] «*Los datos se convierten* en *información* de diferentes maneras: *contextualizando* (relacionar los datos con un contexto), *categorizando*, corrigiendo o condensando (los datos se han podido resumir de forma más concisa) y restando incertidumbre. Para convertir datos en información, los *Data Brokers* necesitan de *algoritmos*» (Hicham Qaissi, 2022: 56). Disponible en: https://is.gd/JpY8i3. También hay que recordar la STC 292/2000, de 30 de noviembre, FJ 8.

[18] Los términos *deep* o «aprendizaje profundo» y *fake* o «falso» se refieren al contenido de audio, vídeo o imágenes generado por IA y que puede mostrar personas reales o

ejemplo de una necesaria y nueva armonización entre estos (RIA, el art. 13, 50, y considerandos 105 y 134). Para las máquinas solo hay datos sin diferenciación de derechos (aunque la IA puede aprender a diferenciarlos) y la aceleración de todas estas problemáticas podría estar provocando un progresivo *splinternet*. En este orden de cosas, los conceptos[19] y metodologías que han servido para la regulación de los datos personales y la construcción de su disciplina (García Mahamut y Rallo Lombarte, 2015) parecen herramientas útiles para esta nueva fase. Sin embargo, esta sistemática y conceptualización, si bien es de gran complejidad, en realidad, no ha sido tan eficaz para solucionar los trascendentes problemas de los datos que, principalmente, se encuentran en las plataformas en línea y redes sociales, donde se produce la comunicación e interacción *online* en tiempo real de los usuarios[20] (RIA, los art. 13, sistemas de alto riesgo[21], y art. 50, en interactuación directa con la persona, exigen el principio de transparencia).

1. EN LAS PLATAFORMAS DIGITALES Y SU IMPACTO EN EL DERECHO A LA INFORMACIÓN Y OTROS DERECHOS FUNDAMENTALES

En estas plataformas de naturaleza comercial, concebidas como soportes técnicos de modelos de negocio publicitario, se ha superpuesto la «plaza

inexistentes (réplicas digitales). Resultan iluminadores dos informes de la Oficina de Derechos de Autor de Estados Unidos (U.S Copyright Office) sobre «Derecho de Autor e Inteligencia Artificial» (julio de 2024 y enero de 2025). Accesible el último en: https://is.gd/UTOrx6, y el de 2024 en: https://is.gd/PL5VxF.

19 Por ejemplo, *privacy by design* o el de «ciclo de vida» del dato. El concepto de «ciclo de vida» también lo utiliza el Reglamento de IA a lo largo de todo su articulado para las inteligencias artificiales.

20 Esta metodología permite una regulación, probablemente, muy útil para algunas aplicaciones y espacios organizativos cerrados, como las Administraciones, pero posiblemente no tan eficiente en espacios abiertos y en tiempo real, como los medios sociales. Estas tecnologías utilizadas en los *social media*, plataformas y motores de búsqueda comportan serios riesgos sistémicos, como los define el RIA (art. 3.6.5).

21 El art. 3.2 del RIA define el riesgo, que es el enfoque de su regulación (sistemas prohibidos, de alto riesgo o riesgo limitado). En general, muchas herramientas IA para la comunicación se clasifican de alto riesgo (art. 9) y de riesgo limitado; sin embargo, por las capacidades y riesgos sistémicos que comportan en determinadas situaciones y actuaciones deben considerarse de alto riesgo, por su impacto en los derechos fundamentales y en la democracia (considerandos 26, 46, 47 y 48, 62 y 63, entre otros).

pública». El espacio privado de negocio convive con el espacio público digital generando contradicción de intereses y principios jurídicos. DiResta (2024: 331) lo observa en este sentido también: «In reality, the current system is simply an attention and revenue maximization engine built by a for profit company». Es un hecho que en el modelo que exportaron las empresas tecnológicas americanas al resto del mundo se exportó un modelo jurídico, sociopolítico y económico. Igualmente, el llamado «efecto Bruselas» supone una implantación del modelo europeo en otros países. Y de ello se sigue un cambio de contexto debido al desplazamiento del modelo y de su espacio y tiempo. En esta línea de descontextualización, los contenidos, a veces, aparecen sin línea temporal[22], descontextualizados en el tiempo y el espacio (por el mismo funcionamiento técnico, no siempre es intencional). La descontextualización de los mensajes o datos se produce tanto en la curación[23] como en la moderación y recomendación de contenidos por la red social. Dado que los datos personales se segmentan y microsegmentan, se facilita la personalización de los mensajes, aislando a los sujetos y creando comunidades paralelas que no se conectan y se encapsulan (fragmentadas) en burbujas ideológicas[24]. Afirma Balkin (2018: 1156) que la tecnología ha hecho posible que el poder esté más distribuido que nunca, aunque, al mismo tiempo, sea también mucho menos democrático, a pesar de las «aparentes» bondades de las redes sociales. Y para entender los desafíos políticos de la «sociedad algorítmica» hay que entender la capacidad del *big data* de recoger y analizar los datos-información de las personas. Esto impacta en todos los elementos objetivos y subjetivos del derecho a la información y en su ejercicio en las plataformas. Conviene, pues, identificar estas y otras disrupciones en las distintas categorías de estudio del derecho a la información[25]:

---

[22] Aunque se van ofreciendo soluciones, como el hilo de las conversaciones.

[23] Organización de contenidos que determina el prestador, entre otros medios, con algoritmos automáticos, en particular mediante la presentación, el etiquetado y la secuenciación.

[24] Véase https://is.gd/6ybYZf.

[25] Existe una muy numerosa doctrina jurisprudencial sobre la delimitación del derecho a la información y sus elementos, por todas: STC 20/1990, de 15 de febrero (libertad de expresión); STC 192/1999, de 25 de octubre (la que mejor ha definido «interés público»); STC 31/1994, de 31 enero (prohibición de censura); STC 178/1993, de 31 de mayo (personas públicas o privadas o asuntos de interés general); STC 165/1987, de 27 de octubre (sobre la posición preferente del derecho a la información), y STC 165/1987, de 27 de octubre (protección reforzada a los profesionales de la información en medios de comunicación institucionalizados).

— El *sujeto*, los usuarios de todo tipo, se mezclan y confunden en la plataforma, sin diferenciación ni contextualización entre todos ellos[26]. Al sujeto usuario[27] (ciudadano) se le iguala al profesional de la información y a los medios de comunicación[28], al *influencer*, sea o no profesional[29], o a cargos públicos (como los presidentes de Gobierno) que se expresan a veces como autoridad y otras como personas privadas[30]. Todo lo cual conduce al sin sentido, por ejemplo, de exigir a los

[26] El Reglamento Europeo sobre la Libertad de los Medios de Comunicación (UE) 2024/1083 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, podría pretender corregirlo, por ejemplo, en el art. 20, estableciendo el «derecho a personalizar la oferta de medios de comunicación» en la plataforma.

[27] El TJUE defendió la posible protección de la libertad de información para los usuarios en sus «actividades periodísticas»: STJUE de 15 de marzo de 2022, asunto *Sr. A y Autorité des marches financiers (AMF)*, *C*-302/20, 69.

[28] Medios de comunicación que en las redes han encontrado un distribuidor y un competidor. Y, hasta ahora, solo han intentado promocionar y maximizar su negocio sin lograr una influencia o control relevante en estas. Habrá que ver, una vez que se aplique en su totalidad, el impacto del Reglamento Europeo sobre la Libertad de los Medios. En su considerando 9 establece: «La definición de un servicio de medios de comunicación debe incluir, en particular, las emisiones de televisión o de radio, los servicios de medios de comunicación audiovisuales a petición, los pódcast de audio o las publicaciones de prensa. Debe excluir los contenidos generados por los usuarios […] salvo que constituyan una actividad profesional prestada normalmente a título oneroso […], la definición […] debe abarcar un amplio espectro de agentes profesionales de los medios de comunicación que entran en el ámbito de aplicación de la definición de servicio de medios de comunicación, incluidos los profesionales independientes». Parece aplicarse el Reglamento solo a los profesionales, aunque no los define, ni tampoco determina legalmente qué es medio de comunicación, dando margen a posible inseguridad jurídica y a la arbitrariedad. Y ello sobre todo si tenemos en cuenta el art. 18.1 del Reglamento, que establece que las plataformas de gran tamaño facilitarán una función para que los «destinatarios de sus servicios: a) declarar que son prestadores de servicios de medios de comunicación». Luego queda a merced de los propios destinatarios y de la plataforma, que decidirán al respecto.

[29] Para ser considerado *influencer* profesional la ley exige unos ingresos y/o audiencias significativas: Real Decreto 444/2024, de 30 de abril, por el que se regulan los requisitos a efectos de ser considerado usuario de especial relevancia de los servicios de intercambio de vídeos a través de plataforma, en desarrollo del art. 94 de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.

[30] *Garnier v. O'Connor-Ratcliff, 41 F.4th 1158 (9th Cir. 2022) Cert. granted, 143 S.Ct. 1779 (April 24, 2023).*

usuarios las mismas obligaciones que a los profesionales[31], pero sin disponer de sus mismas garantías constitucionales en el ejercicio del derecho. O a suspender la cuenta de un presidente en Estados Unidos conforme a criterios particulares de un moderador en Twitter o Facebook[32], sin control jurisdiccional. Desafortunadamente, la sentencia del Tribunal Supremo Americano *Missori v. Biden*[33] dispuso que no pudo identificarse una conexión entre la comunicación del Gobierno y las decisiones de moderación de las plataformas (que libremente deciden sus políticas de moderación) y no aclaró cuáles deben ser las relaciones entre el Estado y las plataformas privadas conforme a derecho. En el caso europeo no existe jurisprudencia en este sentido, pero la numerosa normativa de la UE que regula directa[34] o indirectamente las plataformas habla por sí misma. Strauss (2022: 13-14)[35] apunta que los mensajes del Gobierno en las redes pueden provocar distintas reacciones y, entre ellas, un efecto disuasorio al inhibir o silenciar a los usuarios («In that respect government speech resembles suppression […] that is what creates the fault line»), es decir, la descontextualización no facilita el sentido del mensaje. Y reconoce que, «de alguna manera, internet, incluidas las redes sociales, podrían hacer que el contradiscurso sea más efectivo».

— El *objeto*, que abarca todo tipo de mensajes —se diferencia entre libertad de información o noticias y libertad de expresión, que son opiniones e

---

31 Entre muchas, STC 297/2000, de 11 de diciembre, FJ 9. Y, además, véanse las reflexiones de Elvira Perales (2023: 228), para quien la profesionalidad debe analizarse por factores como la regularidad, el contenido y el carácter de las publicaciones, coherente con la citada STJUE de 15 de marzo de 2022.

32 En España, Twitter suspendió la cuenta de Vox durante ocho días en la campaña de las elecciones catalanas de 2021, al considerar que se incitaba al odio. La Junta Electoral Central lo consideró razonable y proporcional y el Tribunal Supremo lo confirmó: STS 652/2022, de 8 de marzo, Sala de lo Contencioso-Administrativo. Sección Cuarta. También véase la respuesta de Facebook sobre el caso Trump: *Case decision 2021-001-FB-FBR (FB Oversight Board Ruling on Trump)*, disponible en: https://is.gd/LVe8UH.

33 *603 U.S. 2024. Supreme Court of United States, No. 23-411. Vivek H. Murthy, Surgeon General, Et Al., Petitioners v. Missouri, Et Al (June 26, 2024)*. Los antecedentes son los siguientes: *Missouri v. Biden, F. Supp. 3d 2023 WL 4335270 (WD La., July 4, 2023)* y *Missouri v. Biden, F. 4th. 2023 WL 6425697, *27 (CA5, Oct.3, 2023)*.

34 Especialmente el Reglamento de Servicios Digitales (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre.

35 *Fault lines* que también existen *offline*, pero *online* se exacerban.

ideas[36]—, en las plataformas no se manifiesta con diferenciación de mensajes, sino que en una continuidad de interacciones se confunde y uniforma. Dificultad de identificación, exacerbada al extremo en los *social media*, que ha sido puesta de manifiesto por el TC español y otros tribunales europeos[37], lo cual también tiene trascendencia en los límites. Así, por ejemplo, las llamadas *fighting words* (palabras hirientes) en las redes (Strauss, 2022), al no estar contextualizadas; es difícil precisar la *fault line* (límite), es decir, cuándo ciertas expresiones se pueden permitir para el debate público, a pesar incluso de su posible ilegalidad. El TC español también lo ha justificado por un principio de necesidad para la formación de la opinión pública[38]. Serían formas de inhibir la conversación pública digital (*op. cit.*), lo que, aunque no es nuevo, se exacerba en los *social media*. Y es que la importancia del contexto ya fue puesta de relevancia para los medios tradicionales[39]. En mimetismo con el lenguaje de la computación, la información fluye como una cadena indiferenciada. Es así que en Estados Unidos se protege la libertad de datos como libertad de expresión (*Sorrel*) y ello explica que la *First Admendment* haya experimentado una impensable expansión (Netanel, 2023: 24). Lo público y lo privado, lo comercial y lo político-social, aparecen en el mismo espacio, pero sin relación alguna (fuera de contexto). Los datos privados se desplazan a la esfera pública por el consentimiento de los usuarios mismos (que aceptan los términos de

[36] Tanto en la jurisprudencia del TC como en la de los altos tribunales europeos e incluso en el TS americano.

[37] Véanse, por todas, STEDH (Gran Sala) de 5 de abril de 2022, caso *NIT S.R.L c. República de Moldavia*, apl. n.º 28470/12, § 111, y STC 8/2022, de 27 de enero, respecto a un caso de bulos en redes sociales y donde manifiesta que la protección en estas de los derechos no puede ser automática por sus particularidades. Asimismo, ahondando en este sentido, el Tribunal Constitucional alemán ha señalado que también quedan fuera del ámbito amparado por la libertad de opinión aquellas exposiciones de hechos que de manera probada o conocida son falsos (la falsedad debe ser evidente y estar indubitadamente contrastada). BVerfGE 90, 241 (247). Sala Primera, 13 de abril de 1994 —1 BvR 23/94—. Se reitera esta doctrina en la Decisión de la Sala Primera de 28 de marzo de 2017 —1 BvR 1384/16—. También el Tribunal Europeo de Derechos Humanos ha señalado que la transmisión de una opinión, en la que se transmiten hechos, «ha de tener la suficiente base factual, sin lo cual sería excesiva» (STEDH de 27 de febrero de 2001, caso *Jerusalén c. Austria*).

[38] Entre muchas, STC 85/92, de 8 de junio, y STC 3/97, 13 de enero.

[39] TC español, entre muchas: STC 3/1997, de 13 de enero, y STC 477/2001, de 26 febrero. También la STS de 30 de abril de 1990.

uso de la red) y por las máquinas silenciosamente, lo que permite microsegmentación, *profiling* y personalización[40] de mensajes, propiciando nichos y *bubles*, con consecuencias previsibles en la opinión pública y en la democracia. Datos que alimentan a los algoritmos (en tiempo real) y que, obviamente, contienen nuestros sesgos, que luego se reflejarán en los resultados. Esos resultados que modelan la información (e imponen el tema) que recibimos (*feeds*), a la que accedemos y difundimos a través de la plataforma. Y sesgos que se desplazan a otros espacios y usuarios por nosotros mismos y por las mismas máquinas (viralidad, *shares*, *retweet*, *trending topics*, *bots*, etc.), descontextualizando aspectos sociales, educacionales, religiosos o ideológicos. El tiempo/espacio digital (viralidad, visibilidad, atención) ha permitido que se descontextualicen los espacios y los tiempos[41], cambiando su significado originario y desplazando lo privado a lo público (y viceversa). Merced de esos trasvases de datos, también se descontextualizan culturas, religiones y jurisdicciones, entrando, posiblemente, en conflicto en el lugar de destino y sin relación alguna. Así, la llamada *content neutrality* no diferencia entre contextos democráticos y no democráticos (Haupt, 2021: 757), pero «el enfoque de este régimen se centra en el papel de los participantes en el discurso público democrático, más que en la protección acontextual y del discurso en sí mismo» (*ibid*.: 778). Sin embargo, explica Khan (2018: 215): «Post, especialmente tras la controversia de la Caricatura Danesa, presentó su teoría como de alcance global. Si bien Post se ha refugiado desde entonces en el contextualismo, su experiencia plantea una pregunta que persiste […]: ¿Ha llegado finalmente a su fin la era del absolutismo de la Primera Enmienda, si es que alguna vez existió?».

Ahora bien, es necesario también poner la «descontextualización[42]» en contexto, para evitar un entendimiento interesado o equivocado que pudiera ser pretexto para «romper» internet. Cierto que el contexto

[40] «Evidentemente, cuanto más íntimo y sensible es el dato obtenido sobre una persona, más interés tiene, ya que puede suponer una fuente para prácticas de marketing personalizado» (Qaissi, 2022: 56).

[41] Por ejemplo, cuando los *influencers* utilizan su espacio dedicado a moda para introducir noticias u opiniones de todo tipo con influencia político-social.

[42] El funcionamiento libre de internet, el libre flujo global de la información y el uso de datos necesarios para el funcionamiento de todo el sistema (algoritmos) propician la falta de contexto. Diferente es la descontextualización intencionada, negligente o amplificada para alcanzar ciertos objetivos.

ayuda a explicar por qué un sujeto, grupo o sociedad se expresa, reacciona o actúa ante ciertos discursos, pero no es el único parámetro que indica lo que es verdadero o falso (sea respecto a una información o una determinada regulación). Entienden algunos autores (Herz y Molnar, 2012: 210) que, «si se puede malinterpretar el contexto, se pueden exagerar las presiones de la globalización. Si bien algunos autores como Ruti Teitel ven una convergencia global emergente de normas, estas "normas globales" aún deben aplicarse en contextos concretos. Si bien Haraszti tiene razón al afirmar que internet puede proporcionar información sin restricciones de distancia, reglas ni cultura, el impacto de ese discurso en una concreta sociedad se verá moldeado por estos factores». Aceptado el argumento, habría que añadir que, de todas formas, la descontextualización (especialmente la intencionada[43]) no ayuda al consenso, pues la información puede volverse conflictiva. Teniendo en cuenta que, en principio, la descontextualización no es desinformación (según su caracterización por la UE[44], con intención de engañar u obtener un beneficio), aunque pudiera constituir otras formas de esta (según las precisiones doctrinales) o manipularse con fines propiamente de desinformación. Dicho esto, y enlazando con lo citado, no se puede ignorar la libre voluntad y acción humana: tanto la que manipula y explota la descontextualización de la información (ayudándose de los algoritmos) para generar disenso como la de los usuarios para entenderla, rechazarla o combatirla[45]. Afirma Starbird (2024) que «la desinformación no es una pieza de contenido. Es una estrategia»[46]. En el mismo sentido observa Cotino (2022: 200) que, «desde distintos ámbitos —como, por ejemplo, las plataformas y redes—, en vez de fijar la atención en si los contenidos son desinformación desinformativos [*sic*], se subrayan los elementos descriptivos de la conducta y el comportamiento de los sujetos que desinforman a través de las nuevas tecnologías. Así, objetivar el concepto, hacerlo más técnico e incluso aséptico, de este modo se mitiga el siempre sensible juicio de la falsedad del contenido de la información». Y en el mismo sentido, fuentes de la Unión Europa (unidades

43 Véase https://is.gd/zinJyZ.

44 Consejo de la UE. *Plan de Acción contra la desinformación*, Bruselas, 12 de diciembre de 2018, disponible en: https://is.gd/BcRN4B.

45 De ahí la importancia de que la plataforma ofrezca por el algoritmo *affordance* (funciones) que permitan *agency* (decisión propia). Ejemplo: Blue Sky.

46 Véase *El País*, 24 de noviembre de 2024, disponible en: https://is.gd/74vy7h.

especializadas en injerencias extranjeras de desinformación) señalan que «se mira fundamentalmente el comportamiento, no la narrativa»[47]. Se maneja muy frecuentemente un concepto abstracto u objetivado de «desinformación» que, en realidad, no hace referencia al objeto del derecho a la información (en estricto sentido jurídico), sino a estrategias o luchas de poder entre Estados, Estados y plataformas o todos ellos en alianzas de unos u otros. Se necesita cautela, la confusión del concepto podría conducir a la vulneración de los derechos fundamentales y erosionar las instituciones democráticas. No se trata de minimizar los riesgos de los mensajes que no se ajusten a los estándares constitucionales, pero hay que estar advertidos de que pueden ser síntoma y no causa y servir a un argumento que conduzca al *splinternet*.

— Respecto al *contenido y ejercicio* del derecho, en palabras de Álvarez (2023: 174-175), «las redes sociales cambiaron para siempre la forma en la que se accede, se difunde y se comparte la información. Los algoritmos median e intervienen en la selección y en la promoción de contenidos a partir de la ultrasegmentación de los perfiles y preferencias de los usuarios». Advertidos de que expresamos por la navegación e interacción *online,* nuestra tendencia se refleja por los *feeds* (contenido que nos provee la red social) y recomendaciones que satisfacen nuestra facultad de recibir e «impulsan» nuestra facultad de difundir (*retweet*, *share*, *likes*, *links*, etc.) e investigar (al buscar los que nos sugiere la máquina). DiResta (2022: 125) observa que «[l]os algoritmos se utilizan principalmente para activar funciones que actúan sobre los usuarios sin que estos realicen una acción directa en ese momento», y, en este ejercicio dirigido, señala cómo los seguidores son «creadores y amplificadores de contenido». Es decir, hay una apariencia del ejercicio del contenido, que en realidad lo pilotan los algoritmos y algunos usuarios muy «resabidos» en el funcionamiento del algoritmo, que explotan y conducen la conversación hacia determinados intereses. Se ha caracterizado (DiResta, 2024: 314) como «trinity of influencers, algorithms and crowds—the new means of shaping public opinion», la orquestación y uso que algunos activistas hacen del sistema para imponer sus intereses en la conversación pública. Y en el funcionamiento se observa que los límites del derecho se difuminan o no son de fácil reconocimiento al no aparecer con nitidez el objeto del derecho (tipo de mensaje) y porque en ocasiones han sido traspasados esos límites por la máquina y no por el usuario.

[47] Véase *El País*, 24 de noviembre de 2024, disponible en: https://is.gd/VtZxaa.

Esta fragmentación, segmentación y descontextualización se produce en los distintos momentos del funcionamiento de los *social media*. En la curación, tanto humana como artificial (Singh, 2019), hay una incapacidad de dar contexto a cada mensaje o información. En la moderación (con o sin regulación legal), los términos legales y las normas de moderación son una «talla única» (sin atender al contexto local) para todo, pues su aplicabilidad diferenciada, ponderada y contextual es muy difícil aun con moderadores humanos y artificiales[48], incluidos *factchekers*. Esta misma falta de contextualización la constata Douek (2022), y Singh (2019: 11-18) manifiesta de la IA «[i]ncapacidad para interpretar el contexto», y añade que «las plataformas deberían permitir a los usuarios proporcionar más contexto e información durante el proceso de apelación». Reclama un «decentralized model […], enable more localized […], culture-specific and context-specific moderation to take place». En la recomendación de contenidos, finalmente, el sistema le devuelve sus opiniones al usuario. Se forman nichos, se segrega al sujeto y a la información sin contextualización. Situación que contrasta con las medidas estructurales que exige el Convenio IA del Consejo de Europa, en su art. 5, que incluye la libre formación de la opinión y el acceso y participación en el debate público. También lo confirman Rubio *et al.* (2024: 53): «En este nuevo orden comunicativo, moldeado en grandes proporciones por los efectos de la IA, la información viaja de forma dirigida, según un modo distributivo dictado predominantemente por la inescrutable voluntad de los algoritmos que, en definitiva, condicionan activamente el acceso a la información. Al mismo tiempo, la segregación de los usuarios en nichos relacionales fragmentados […]». En los mismos autores (*ibid.*: 70-86) se encuentra una detallada taxonomía de prácticas mediante herramientas IA para la generación, difusión de mensajes y acceso a fuentes[49], donde se describe, técnicamente, cómo operan y su posible impacto en los derechos de participación política[50] (IA al servicio

[48] Podría requerir tiempo que para el ejercicio de la libertad de expresión en la red social pueda tener un efecto de desaliento o disuasivo.

[49] Infoxicación, *astroturfing* (falsificación de la opinión pública en comunidades virtuales de cualquier tipo), *firehosing* (campañas intensivas de defraudación), tergiversación de la realidad, *cheapfakes* (manipulaciones audiovisuales con *software* barato), *shallowfakes* (manipulación audiovisual poco sofisticada), *deepfakes* (Rubio *et al.*, 2024: 70-86).

[50] Considerando 62 RIA: «Sin perjuicio de las normas previstas en el Reglamento (UE) 2024/900 […] y a fin de hacer frente a los riesgos de injerencia externa indebida en el derecho de voto consagrado en el artículo 39 de la Carta, y de efectos adversos sobre la democracia y el Estado de Derecho, deben clasificarse como sistemas de IA de alto riesgo los sistemas de IA destinados a ser utilizados para influir en el resultado de una

de/o contra la democracia); y, también, por supuesto, en el derecho a la información[51] y en el de protección de datos personales (privacidad), pues son herramientas que generan, difunden y distribuyen contenidos para el usuario y «suplantando» al usuario. Múltiples herramientas para generar «disenso» y, sobre todo, para «explotar el disenso», resultando una opinión pública dividida. Ahora bien, si la desinformación es munición (amenaza y/o guerra híbrida), moneda de cambio o acicate entre plataformas y Estados (o entre Estados) con distintos fines, el disenso que se propicia y explota es parte del mismo intercambio y juego de intereses. El disenso técnicamente es posible, pero el consenso es, en mayor o menor medida, posible también. DiResta (2022: 128-137) ha manifestado: «[…] what we are contending with now is not the manufacture of consent but the manipulation of consensus». *Contrario sensu*, Strauss (2022) y Harari (2024) observan que esta sofisticada *network* técnica refuerza, sin embargo, el derecho de asociación.

2. EL PROGRESIVO *SPLINTERING* Y EL IMPACTO EN EL DERECHO A LA INFORMACIÓN Y OTROS DERECHOS FUNDAMENTALES

Que la red de redes global está cada día más fragmentada es ya un lugar común. Las infraestructuras de telecomunicaciones se van fragmentando: a la propiedad pública del Estado se ha unido una propiedad privada[52] en continua expansión, de las grandes empresas de telecomunicaciones a las mismas compañías tecnológicas de las plataformas[53] (Nugent, 2023). Incluso «[l]a propia columna vertebral de internet no es inmune a la balcanización. Cada vez hay

elección o un referéndum, o en el comportamiento electoral de las personas físicas en el ejercicio de su voto en elecciones o referendos, con excepción». Véanse el art. 6 y el anexo 3. Y en el capítulo III (Garantías y requisitos), respecto a los sistemas relacionados con el derecho al voto. Y en el Convenio del Consejo de Europa, el art. 5.

51 Manipulación rudimentaria de acontecimientos y contextos en piezas de comunicación, *deepfakes*, *cheapfakes*, *bots* y *chatbots*, asistentes virtuales, *spear phishing*, discriminación algorítmica, silenciamiento algorítmico, pseudomedios, robots periodistas, blogs panfletarios, etc. (Rubio *et al.*, 2024: 94).

52 Nugent (2023: 534): «The history of the "public internet" is one of privatization. Although originally developed and administered by the U.S. Department of Defense and the National Science Foundation, […] the internet incrementally transitioned from governmental to private control. […] (ICANN), today's public internet is very much a private network, where private parties act as gatekeepers for who can say what, when, where, how, and to whom».

53 Véase https://is.gd/VnZPQT.

más iniciativas por parte de empresas y proveedores de servicios de internet (ISP) para filtrar sitios maliciosos a nivel del Sistema de Nombres de Dominio (DNS) para que nunca sean accesibles, ni siquiera en su sistema de servidores» (Lemley, 2021: 1415). Sin ignorar que las nuevas infraestructuras del 5G son problemáticas entre los Estados[54]. Igualmente, el *software* y toda la logística de las redes cada día dividen más al mundo por la no interoperabilidad e incompatibilidad, de manera que a lo que se puede acceder desde un país no se alcanza desde otro[55]. Las plataformas centralizadas permanecen cerradas unas a otras, sus *apps* no son interoperables[56] e, incluso, siendo las mismas en diferentes países, la experiencia es completamente distinta. Su gobernanza diferenciada por los algoritmos, los términos de uso y la legislación separa a los países cada vez más (UE y Estados Unidos, y sin obviar a China) (Bradford, 2023). Ocurre también que el mercado del *hardware* está cada vez más dividido (teléfonos móviles, chips o semiconductores). «Estados Unidos está actualmente en proceso de prohibir los teléfonos chinos en el mercado. El Estado considera la tecnología de los teléfonos Huawei y ZTE un riesgo para la seguridad, al igual que TikTok» (Lemley, 2021: 1411). A ello se añade ahora que los sistemas de IA desarrollados en diferentes partes del mundo podrían no autorizarse ni comercializarse en todos los países, al no ajustarse a las distintas legislaciones, como la europea, lo que puede fragmentar más el ciberespacio y comprometer definitivamente la neutralidad de internet. La tecnología y sus usos muestran el desanclaje del derecho a la información del derecho constitucional. Y en un posible intento de «corregir» los usos disruptivos conforme a derecho, las progresivas restricciones técnicas y jurídicas de acceso a internet aumentan, incluso en los países democráticos. El horizonte de *splinternet* total se contempla cada vez más cercano y las «excusas» pueden ser muchas, desde un fin de reparar el ejercicio

[54] «China is building a 5G network, and it's not just building it in China. Through the Belt and Road Initiative, it's building that network in Africa, Latin America, and Asia as well. Those countries will use a 5G network that may well be incompatible with the U.S. 5G network because we are building different hardware systems that don't necessarily talk to each other. And even if data can pass between the networks, it will increasingly be on software platforms that are nation specific» (Lemley, 2021: 1413).

[55] «It's not just differences in local regulations that are leading to different software in different countries. Rather, it's increasingly hard for foreign internet programs to penetrate local markets as a structural matter. Russia, for instance, has blocked LinkedIn, is requiring local Russian apps to be loaded on all smartphones» (Lemley, 2021:1406)

[56] Y no solo en países autoritarios, sino también en países democráticos, como Estados Unidos respecto a TikTok (Lemley, 2021).

del derecho a la información a explotar las «anomalías» para el control casi absoluto de internet. Las distintas opciones reflejan, en realidad, los modelos legales respecto a internet[57] y la lucha[58] por dominarlo (Lemley, 2021: 1402): «The competition is […] between regulatory models that are going to determine whether the internet as we know it will continue to exist in any given country». Este fraccionamiento progresivo (reflejo de luchas de poder), sin embargo, no es nuevo: «Estamos volviendo a los jardines amurallados. Algunos de estos jardines están gestionados por empresas privadas, pero cada vez más se crean trazando fronteras nacionales en torno a internet […]. La balcanización de internet es algo negativo, y deberíamos detenerla si podemos» (Lemley, 2021: 1399). Conviene seguir ahondando sobre las razones, ya tratadas más arriba, que empujan tanto a las empresas privadas como a los Estados a avanzar en este inquietante movimiento. Se ha visto que la descontextualización, la segmentación y la fragmentación son el andamiaje que sostiene la desinformación, tanto en un sentido político (estrategias de poder) como en un sentido jurídico estricto (objeto del derecho a la información). Así, una de las principales causas de este troceamiento de la red es la creciente preocupación de los Estados por la soberanía digital[59] y la ciberseguridad, por lo que buscan controlar el flujo de información dentro de sus fronteras para prevenir amenazas externas mediante la desinformación. Además, las diferencias culturales, religiosas o sociales se perciben como causas desestabilizadoras, lo cual contribuye al *splinternet*.

Se insiste en que «evolving technology of computing and its potential impact on democracy […] could represent a technical triumph and a social disaster» (DiResta, 2024: 38). En este mismo sentido, Harari sostiene (2024:

---

57 «If you look at the rest of the world, what you see is actually an ongoing nation-by-nation competition for who gets the internet» (Lemley, 2021: 1401).

58 Desde los primeros tiempos de internet, los *cyber-expeptionalists* quisieron ver un internet libre de Estados, jurisdicciones territoriales y sus leyes. Se equivocaron. Véanse, entre otros, Lessig (1996a), Johnson y Post (1996), Post (1996), Goldsmith y Wu (2008), y Bloch-Wehba (2019).

59 Robles Carrillo (2023: 159) recoge conceptos de soberanía digital que van desde «autores como Chander y Sun, para quienes la soberanía digital debe definirse de forma amplia como el poder soberano de un Estado para regular no solo el flujo transfronterizo de datos, sino también las actividades de acceso y comunicación de las tecnologías», hasta Csernatoni, para el que «se trata de la capacidad de los ciudadanos, las empresas, los Estados y las comunidades de Estados para actuar de manera independiente desde el punto de vista digital», o Posch, que «define la soberanía digital como la capacidad de tener pleno conocimiento y control por parte de un sujeto sobre sus propios datos».

7-10) que el orden establecido está desintegrándose, y la nueva infraestructura de la información, a pesar de su potencial de conexión técnica, no ofrece un «nexo» de interés público general y, en crisis el concepto hasta ahora predominante de información, que el autor califica de *naïve*, no aprehende «la realidad universal» ni narra unos hechos captando «la verdad universal». Aun aceptando que existe una realidad universal, no existe una verdad universal, pues la realidad es compleja y existen muchos puntos de vista y «cada verdad» pone su atención en cierto aspectos de la realidad e ignora otros. Y la información (sin *link* esencial con «la verdad») representaría, en todo caso, una realidad histórica que se desmorona (Harari, 2024: 11). Y aunque DiResta (2024: 328) apunta a «la curación de los algoritmos para dar forma al consenso que, aun así, se ve eclipsada por la moderación de contenido, que intenta separar lo "bueno" de lo "malo"», todo resulta en que no se alcanza nexo ni consenso entre las distintas comunidades y realidades. Esta situación, unida a los desórdenes de la información, que se propician, bien desde el exterior por terceros países[60] (se impone la ciberseguridad con fines de seguridad nacional), bien desde el interior, es especialmente crítica en períodos electorales, pero también en momentos sensibles políticos o sociales, y puede ser un poderoso argumento para dividir internet, tanto por el Estado como por las empresas privadas tecnológicas[61]. Advierten algunos autores (Khan, 2018: 210-211) que los Estados pueden responder a estos problemas troceando la red de redes y reduciéndola a pequeñas *intranets* ejerciendo su soberanía nacional y/o soberanía digital. «Además, la idea de que la única respuesta al odio en línea es que los Estados destruyan la autopista de la información y la reemplacen con sus propias "intranets" mucho más pequeñas es cuestionable. […] con la ayuda del sector privado, los Estados pueden tomar medidas para regular el odio en línea sin necesidad de desmantelar Internet». Bichoff (2023)[62] ha elaborado un mapa global de

[60] Access Now (https://is.gd/YvZD3g) informa continuamente de acciones técnicas, políticas y jurídicas en este sentido.

[61] Un estudio ilustrativo de cómo funcionan estas empresas en este sentido en Romano *et al.* (2023: 2): «[…] their consequences for Russian users, including the spread of pro-war propaganda and their isolation from the global TikTok community. Our findings contribute to the understanding of how TikTok policies can contribute to the creation of a 'Splinternet' — a scenario in which countries have vastly different information online and separate internet infrastructures».

[62] «We scored each country on six criteria. Each of these is worth two points aside from messaging/VoIP apps which is worth one (this is due to many countries banning or restricting certain apps but allowing ones run by the government/telecoms providers within the country). A country receives one point if the content—torrents, pornography, news media, social media, VPNs, messaging/VoIP apps—is restricted but

restricciones a internet, clasificando los países en función de su acción censora legal y técnica (cierres, denegación de acceso, bloqueos, etc.). Por supuesto, China, Irán, Corea del Norte o Rusia[63] ocupan el primer puesto, pero sorprende el avance en esta medidas en países democráticos (Estados Unidos, UE o Australia). Robles Carrillo (2023) explica que el concepto de soberanía digital se ha trasladado de los países autocráticos a los democráticos y las diferencias de este en ambos[64]. Nachbar (2022)[65] explica que la guerra de Ucrania ha dado lugar a numerosas peticiones y actuaciones para desconectar a los países involucrados de la red mundial y que la arquitectura técnica de internet y el funcionamiento de la ICANN han hecho casi imposible una desconexión total. En la UE el enfoque de la ciberseguridad es esencial[66], y se ha desarrollado una intensa y profusa actividad dirigida primero al fenómeno de la desinformación y después a su utilización en la llamada guerra híbrida y amenazas híbridas que provienen de injerencias extranjeras. Esta actividad tuvo un hito en 2018

accessible, and two points if it is banned entirely. The higher the score, the more censorship» (Bichoff, 2023: 3).

63 Epifanova (2020: 2). En Rusia, la llamada *Sovereign Internet Law*, de 2019, introduce, de hecho, algunas enmiendas a la anterior ley: «Officially, the amendments aim to protect the internet within Russia from external threats. In fact, they provide the crucial legal framework for creating a centralized management system of the internet by the state authority — theoretically enabling the isolation of Russia's network from the global internet. These three amendments have particularly far reaching implications».

64 «[…] la diferencia fundamental se encuentra en que el concepto de soberanía digital en los Estados autocráticos sirve para asegurar el poder del Estado y mantener las estructuras autocráticas mientras que, en los países democráticos, se plantea como un medio eficaz para preservar los valores liberales y, en general, una concepción del mundo digital basada en valores y principios democráticos. Una segunda diferencia, no menos importante, se advierte en el hecho de que estos países no solo otorgan objetivos y funciones distintas a la soberanía digital, sino que, en general, no asocian este concepto con el principio de soberanía cibernética ni comparten esa interpretación extensiva de la soberanía» (Robles Carrillo, 2023: 145).

65 Nachbar, T. (2022): «The larger concern with ICANN is not its purported neutrality but its design, which replaces accountability to the population of the world, as organized by governments, with accountability to the world of technology interests, as organized by ICANN».

66 Ciberseguridad con causas y objetivos muy diferentes, pues detrás de la construcción de infraestructuras propias, los bloqueos o las limitaciones a la conectividad hay razones, básicamente, de seguridad nacional, estabilidad social, estrategia económica e informativa o defensa de los derechos fundamentales.

con el Plan de Acción contra la desinformación[67], que incluye el Código de buenas prácticas[68]. Desde 2020 las acciones de la UE cobraron nuevo impulso con el compendio de ciberseguridad destinado a proteger la integridad de las elecciones en marzo de 2024[69], el Paquete de Defensa de la Democracia en diciembre de 2023, y los Reglamentos de Servicios Digitales[70] en octubre de 2022, de Mercados Digitales en septiembre de 2020[71] y de Libertad de los Medios de Comunicación en abril de 2024. Y recientemente la Comisión Europea ha anunciado un nuevo «escudo europeo de la desinformación» para combatir las injerencias extranjeras[72]. Resulta, sin embargo, asombroso que, tras la invasión de Ucrania, blindándose contra la desinformación rusa y sobre tal base[73], la Comisión ordenara el bloqueo de los canales de difusión rusos *Russia Today* y *Sputnik*, lo que supone una grave injerencia en el derecho a la libertad de expresión en una sociedad democrática. Una medida de gran amplitud y sin ningún género de garantías: se bloquean estos medios de forma

---

67 Consejo de la UE, Plan de Acción contra la desinformación, Bruselas, 12 de diciembre de 2018, disponible en: https://is.gd/BcRN4B.

68 Comisión Europea, COM(2021) 262 final, Orientaciones de la Comisión Europea sobre el refuerzo del Código de Buenas Prácticas en materia de Desinformación, Bruselas, 26-5-2021.

69 Con motivo de las elecciones al Parlamento Europeo de 2024, se han adoptado una serie de medidas que contienen referencias concretas a sus posibles aplicaciones en las campañas electorales. Las medidas se derivan del Plan de Acción Europeo para la Democracia (2020), que busca «empoderar a los ciudadanos y aumentar la resiliencia democrática en toda la Unión promoviendo elecciones libres y justas, reforzando la libertad de los medios de comunicación y combatiendo la desinformación». El Plan se desarrolló por fases, con hitos en noviembre de 2021 y diciembre de 2023. Véase: Comisión Europea, Comunicación COM(2020) 790 final, Plan de Acción para la Democracia Europea, 3 de diciembre de 2020.

70 El RSD, en su art. 36.2, reconoce unos poderes exorbitantes a la Comisión Europea para afrontar «crisis», entendidas estas cuando «se produzcan circunstancias extraordinarias que den lugar a una amenaza grave para la seguridad pública o la salud pública en la Unión o en partes significativas de esta».

71 Además del citado Reglamento sobre Libertad de Medios de Comunicación 2024/1083 o el de Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, sobre transparencia y segmentación en la publicidad política, entre los destacados.

72 Véase https://goo.su/VnzK7H.

73 Reglamento (UE) 833/2014 —modificado por Reglamento (UE) 2022/350 de 1 de marzo, relativo a medidas restrictivas motivadas por acciones de Rusia que desestabilizan la situación en Ucrania—. Art. 2.f.

radical y absoluta. Un bloqueo que se extiende a todas las vías de difusión: radio, televisión, plataformas de internet y motores de búsqueda, sin otros matices más allá de entender que la medida es temporal (aunque no está sujeta a un término cierto). El Reglamento (UE 2022/350) justifica la medida porque Rusia ha seguido una «sistemática» campaña de «manipulación y distorsión de los hechos» en su estrategia de desestabilización. Y una «propaganda» «repetida y constantemente dirigida a partidos políticos especialmente en períodos electorales» (considerandos 6 y 7). De todos los bloqueos, solo el de RT France fue impugnado ante el Tribunal de Luxemburgo, que mediante la Sentencia del Tribunal General de la Unión Europea (Gran Sala) de 27 de julio de 2022, T-125/22, *RT France c. Consejo de la UE*, ha confirmado la legitimidad de la medida adoptada por el Consejo, validando el bloqueo de los canales rusos, desde la perspectiva de la protección de la libertad de expresión en Europa. Tristante y Teruel (2023: 325), en un análisis muy crítico de la sentencia[74], discrepan con su fallo, entendiendo que «la prohibición impuesta es difícilmente conciliable con las garantías exigibles para adoptar una medida de esta severidad, de acuerdo con la doctrina del Tribunal de Estrasburgo». En especial, sí consideramos que el TEDH ha reputado ilegítimas restricciones a la libertad teniendo en cuenta: «i) el alcance excepcionalmente amplio de la injerencia; ii) su duración excesiva; iii) la falta de motivación de la medida por parte del tribunal nacional, y iv) la imposibilidad de los demandantes de impugnarla antes de su ejecución». Aun así el Tribunal consideró que el canal demandante no goza de la «protección reforzada» de la Carta, que reconoce la libertad de expresión de prensa. Por otra parte y conectado con las anteriores críticas, advierte Robles Carrillo (2023) de que democracia y legitimidad son conceptos que en este debate de la soberanía digital «habría que trabajar para evitar que un concepto ideado para defender el modelo europeo de valores y principios no responda suficientemente a esos criterios de democracia y legitimidad» (Robles Carrillo, 2023: 164).

Hay que concluir con Lemley (2021: 1403-1404) que, «[e]n Europa, en cambio, las industrias de contenidos y el Estado ejercen un control mayor y

[74] «En concreto, para enjuiciar la limitación a la libertad de expresión, el Tribunal General ha estudiado cuatro requisitos: primero, que estuviera "establecida por ley", […] segundo, que respetara el contenido esencial de la libertad de expresión; tercero, que respondiera […] a un objetivo de interés general […]; y, cuarto, que se tratara de una medida proporcionada. En definitiva, como reconoce el propio Tribunal General en la sentencia, para valorar la injerencia en la libertad de expresión ha optado por recurrir a un test que se corresponde "esencialmente" con el triple test de Estrasburgo».

más efectivo sobre internet que en Estados Unidos. […] Y todo eso significa que la Unión Europea busca y ejerce cada vez más control sobre lo que se publica en internet». Este progresivo control, que supone una escalada de restricciones a internet[75] y del libre flujo informativo, so pretexto de influencias indebidas, extranjeras o internas, y de la ciberseguridad, está apuntando al *splinternet*. Además, muchas de estas medidas caracterizadas por su excepcionalidad se convierten en normalidad (se mantienen más allá de un período definido de guerra o electoral). España, dando respuesta nacional al Plan de la UE, aprobó la Orden PCM/1030/2020, de 30 de octubre, sobre el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional. Orden recurrida ante el Tribunal Supremo, que, mediante sentencia de 18 de octubre de 2021, inadmitió a trámite el recurso al entender que no regula contenidos ni atisba ningún tipo de restricción. Más llamativo fue el Real Decreto Ley 14/2019 («el decretazo digital»), modificando la Ley General de Telecomunicaciones 9/2014, por el que se permite la intervención y el control del Gobierno de redes y servicios de comunicación electrónicas en aras de la seguridad pública y nacional. El decreto fue recurrido ante el TC por sendos recursos de inconstitucionalidad que declaró en parte extinguidos y en parte desestimados[76]. Y con ello se puso fin a las aspiraciones de una «república digital catalana».

La cuestión de la seguridad nacional y el orden público es asunto de vital importancia tanto en la UE como en Estados Unidos[77] y la ciberseguridad no es cuestión menor para el mantenimiento de la soberanía digital. Ahora bien, las decisiones pueden deslizarse hasta el *splinternet* e imponer fronteras electrónicas: tanto para restablecer el orden democrático como para establecer totalitarismos (Harari, 2024), aprovechando estas herramientas digitales de inigualable capacidad de control (*surveillance*) en la historia de la humanidad. Tampoco se descarta la idea del s*plinternet* con el fin de dar luz a los metaversos por los Estados y/o empresas. John Gilmore, citado por Lemley (2021: 1400), lo dijo ya en 1993: «[L]a red interpreta la censura como un daño y la evita». Y

---

75 El Reglamento de Libertad de Medios de Comunicación, en el art. 17, exhibe un poder «desorbitante» respecto a medios establecidos fuera de la Unión «cuando perjudiquen o entrañen un riesgo serio y grave».

76 Sentencia del TC 36/2023, de 19 de abril de 2023. Recurso de inconstitucionalidad 1220-2021. Interpuesto por el Consejo de Gobierno de la comunidad autónoma del País Vasco en relación con diversos preceptos del Real Decreto Ley 14/2019, de 31 de octubre. En el mismo sentido, la Sentencia del TC 60/2023, de 24 de mayo, del recurso de inconstitucionalidad interpuesto por el Parlamento de Cataluña.

77 Véase https://is.gd/WiQsgm.

añade Lemley: «La idea era que tuviéramos una red distribuida que pudiera evitar el control centralizado. Hoy, creo que es más justo decir que la censura interpreta la red internet como un daño y la evita. Como argumento aquí, los Estados han encontrado maneras de evitar o controlar los esfuerzos de internet por eludir su censura». Pero no solo los Estados, también las empresas tecnológicas, pues, siguiendo a Nugent (2023: 532), el *deplatforming* (prohibir el acceso a alguien a una plataforma) «está llegando ahora al núcleo de la infraestructura de internet. Estos esfuerzos, y otros similares, plantean la posibilidad muy real de que la privatización completa de internet […] pronto produzca un mundo en el que los puntos de vista más impopulares puedan ser excluidos por completo de internet, un fenómeno que denomino exclusión de puntos de vista». Aún más, la desconfianza de los Estados (Estados Unidos) respecto alguna plataforma extranjera (TikTok), como amenaza a su seguridad nacional, se vive actualmente en contienda judicial[78]. Muestra también su preocupación Haupt (2021: 775-776) por las posturas enfrentadas de UE y Estados Unidos, y, tomando las palabras de Balkin, afirma que en nuestros días son los valores de uno de los países menos censores —Estados Unidos— los que han gobernado internet. Pero si los Estados pueden globalmente *filtering* (filtrar), *blocking* (bloquear) o *delinking* (desconectar), internet será gobernado finalmente por los más censores. Y «[t]his will undermine the global public good of a free internet». Internet libre ha sido siempre global (Leiner *et al.*, 1997) y ese es el modelo defendido por Estados Unidos y Europa hasta ahora. Y su defensa es imprescindible para proteger y potenciar las libertades de expresión e información (conforme al estado del arte) y, por ende, de todos los derechos. La desconexión a la internet global supone una rotunda vulneración del art. 19 de la Declaración Universal de los Derechos Humanos de 1948 y del resto de los convenios y pactos internacionales en la materia.

3. UN DERECHO A LA INFORMACIÓN EN TRANSFORMACIÓN: IDENTIFICANDO MUTACIONES Y SU TRASCENDENCIA DEMOCRÁTICA

La fragmentación de la información en las plataformas y el progresivo *splintering* de la red global, tanto por los Estados como por la empresas tecnológicas, han impactado en el derecho a la información, que manifiesta algunas «mutaciones». Y advertidos de que el continuo *splintering* puede conducir a un

[78] El Tribunal Supremo norteamericano ha confirmado la ley que permite suspender la actividad de TikTok en Estados Unidos. *Tiktok Inc. V. Garland 604 U. S. (2025). January 17, 2025*.

splinternet total que, en los países democráticos, supondría no una mutación, sino una vulneración absoluta del derecho a la información (Harari, 2024), con onda expansiva en todos los derechos fundamentales y en la democracia misma. La necesidad de repensar una nueva relación jurídico-informativa se va revelando más necesaria: la presencia de nuevos sujetos (tecnológicas/máquinas IA) y su posible atribución de derechos y responsabilidades; el déficit del ejercicio de las facultades del derecho por los usuarios, déficit que se corresponde con el ejercicio que han «acaparado» ya los nuevos sujetos (máquinas IA); la forma de ejercer la libertad de expresión por los usuarios, a través de «todos» sus datos públicos y privados en la navegación e interacción en la red, manifestada indirecta y posteriormente por los algoritmos y materializada en forma de mensajes por los *feeds* o recomendaciones a los usuarios; cambios en el objeto, mensajes/datos sin diferenciación, y, posiblemente, también en el contenido esencial, que se vacía para los usuarios y se llena de contenido para la máquina; en los límites del derecho, que se desdibujan por la falta de diferenciación y contextualización de los mensajes, lo cual está llamando a redibujar los límites, y no solo para el sujeto usuario, sino también ya para las máquinas. Todas estas «anomalías» o posibles mutaciones (que abajo se describen con más detalle) calan en el derecho a la información en todas sus categorías de análisis: sujeto, objeto, contenido, herramientas tecnológicas y espacio-tiempo. En general, se advierte que la persona, titular del derecho a la información, está siendo desplazada, en mayor o menor medida, por la máquina en el ejercicio de las facultades que contiene el derecho. Parece que se estuviera fraguando un nuevo rol del derecho a la información: conectar a la persona con la máquina, propiciando con sus datos e información el diálogo con la máquina y entre *máquinas*, que se conectan y dialogan entre sí, propiciando unas narrativas que conformen la conversación pública, la opinión pública, las comunidades virtuales, sus *norms* y su gobernanza. Así lo ha expresado DiResta: «La relación entre humanos y algoritmos se configura como un "bucle viral" en el que el usuario envía señales a la máquina mediante sus acciones y el consumo de contenido. El algoritmo las interpreta y las refleja en su sugerencia, y luego los humanos reaccionan a la nueva provocación. No existe una única fuerza impulsora responsable, sino la interacción entre algoritmos, funciones y capacidades que ha transformado el discurso y la comunidad» (2021: 123).

Advierte Harari (2024: 12) que en este nuevo sistema, a semejanza de otros en la naturaleza como en biología, la información no representa una realidad, sino que su rol es conectar cosas: «[…] the rol of information in connecting things is of course not unique to human history. A case can be made that this is the chief role of information biology». Y, como en el ADN,

un error en la transmisión es un error de copia de lo anterior, una mutación con posible propósito de un cambio, pero no es desinformación, siguiendo al mismo autor. Por su parte, Lessig (1996b: 869-904), en los comienzos de internet, llamó la atención de que estamos «haciendo el ciberespacio» y no «descubriéndolo», porque se trata de un producto técnico humano (no de la naturaleza)[79]. Y la tecnología rara vez es determinista, en también observación de Harari (2024: 309). Ahora bien, sin minimizar la fuerza transformadora de las tecnologías e infraestructuras digitales. Es imposible ignorar que, a diferencia de otros sistemas de información en la historia, estas tecnologías tienen capacidad de tomar decisiones y generar ideas por sí mismas, es decir, poseen autonomía. Pero todavía se está a tiempo de intervenir (en los albores de la IA generativa y otras tecnologías), estableciendo mecanismos técnico-jurídicos que puedan actuar en este proceso de disrupción democrática. Advierte de nuevo Harari (2024: 346): «Si no podemos descubrir qué ha fallado y solucionarlo, las democracias a gran escala podrían no sobrevivir al auge de la tecnología informática. Si esto realmente sucede, ¿qué podría reemplazar a la democracia como sistema político dominante?». Seguidamente se describen algunos de los cambios (o mutaciones) que están transformando el derecho fundamental.

Cambios en los *sujetos* del proceso: a los usuarios como generadores y receptores de contenidos, hay que añadir los usuarios de especial relevancia como los *influencers*[80]. DiResta (2022: 127) advierte que «a new class of communicators had emerged: influencers and hyperpartisan demi-media» (los pseudomedios), y la misma autora después (2024: 314) los caracteriza dentro de «la trinidad» (*the trinity of influencers, users and algorithms*). Los *factchekers*[81] se han sumado al ecosistema de las plataformas (aunque no dependen de ningún prestador de plataforma en línea, RSD art. 22.2b). Y sin obviar el papel de los *prompters*, cuyo rol puede ser decisivo para el diálogo con la IA generativa. Los modelos de IA y/o sus algoritmos (entre ellos, ChatGPT, Copilot, Gemini, etc.) podrían constituirse como un nuevo sujeto titular[82] (Fernández Carballo, 2021) de derechos y deberes (muy debatido en el ámbito del derecho de autor). Afirma Balkin (2018: 1150) que el problema no es tanto si las

[79] Lessig, L. (1996b): «[…] they are making, not finding, the nature of cyberspace; their decisions are in part responsible for what cyberspace will become» (p. 869); «[…] cyberspace has not permanent nature, save the nature of a place of unlimited plasticity» (p. 888).

[80] Algunos *influencers* no se ajustan a la norma al no alcanzar las audiencias o ingresos significativos conforme al RD 444/2024, de 30 de abril.

[81] Reglamento de Servicios Digitales, en su art. 22: «alertadores fiables».

[82] Puesto que poseen autonomía, pueden tomar decisiones y generar información.

máquinas deben ser titulares de derechos, sino si las tecnológicas, propietarias de estas tecnologías, van a ser los titulares. Cuestión esta que no es baladí, pues nos sitúa en la cuestión de la responsabilidad[83] en el ejercicio del derecho. Las propias compañías tecnológicas, titulares de las plataformas, son instituciones clave controladoras del proceso de comunicación (Rubio *et al.*, 2024: 7), cuya naturaleza jurídica está aún por definir, pues no son solo sujetos privados (o no cualquiera), sino que actúan como Estados soberanos (sin serlo), y están llamadas, probablemente, a tener un estatus jurídico diferente (Bustos, 2024). Sin desconocer que la función reguladora se ha desplazado a las plataformas (o en colaboración con las plataformas en UE) y el derecho se ejerce frente al Estado, pero también frente las plataformas[84] y frente a todos (quizás incluidas máquinas). Además, el Reglamento europeo de IA prevé obligaciones y responsabilidades para estos sujetos, tanto en virtud de la posible titularidad de la propiedad intelectual de la IA como por el despliegue que hagan de esta por sus usos en las plataformas. El considerando 93 precisa:

> Aunque los riesgos relacionados con los sistemas de IA pueden derivarse de su diseño, también pueden derivarse riesgos del uso que se hace de ellos. Por ello, los responsables del despliegue de un sistema de IA de alto riesgo desempeñan un papel fundamental a la hora de garantizar la protección de los derechos fundamentales […]. Los responsables del despliegue se encuentran en una posición óptima para comprender el uso concreto que se le dará al sistema de IA de alto riesgo y pueden, por lo tanto, detectar potenciales riesgos significativos que no se previeron en la fase de desarrollo, al tener un conocimiento más preciso del contexto de uso y de las personas o los colectivos de personas que probablemente se vean afectados.

Dependiendo del grado de riesgo de la IA, estos proveedores y/o responsables del despliegue de los algoritmos deben cumplir con las obligaciones y requisitos que el RIA impone para su empleo en la UE (arts. 16 a 26 de los de alto riesgo, y arts. 50, 51 y 53 para los de riesgo limitado). A su vez, el Reglamento de Servicios Digitales ofrece numerosas vías para denunciar (art. 16) y exigir responsabilidades a las plataformas tanto por sus propios algoritmos como del uso que hagan de estos los usuarios (considerandos 84, 89, 96), por ejemplo,

---

[83] Responsabilidad de la máquina que se une al deber de transparencia, explicabilidad y trazabilidad que podría constituir la facultad o derecho al contexto que podría ampliar el contenido del derecho a la información.

[84] Esto no se produce en Estados Unidos, como se evidenció en la Sentencia del Tribunal del Distrito Norte de California de 6 de mayo de 2022, asunto *Trump et al. v. Twitter*, c. 21-cv-09378-JD.

subiendo contenidos generados con IA (*deepfakes*). Asimismo, el RSD, es su considerando 84, alerta contra el «uso no auténtico» del servicio. Por otra parte, el Reglamento de Mercados Digitales incluye a las plataformas y motores de búsqueda como «guardianes del mercado» en los términos del art. 3 y siguientes. Habría que añadir a los profesionales de la información que están presentes, tanto individualmente como mediante sus medios de comunicación, para los que las redes son, a la vez, sus canales de distribución y sus competidores[85]. Ya se ha observado la circunstancia de tratar en las redes a los usuarios como profesionales (con dudas de que el Reglamento de Libertad de Medios lo revierta), lo cual tiene trascendencia en el ejercicio del derecho a la información, pues se les somete a obligaciones profesionales, pero sin las debidas garantías constitucionales, restringiendo aún más el ámbito de ejercicio de su derecho.

Cambios en el *objeto*: la diferenciación de mensajes se difumina en la red (buena prueba es que a todos ellos se refiere la expresión de *fake news*). Además, la falta de contextualización no permite su reconocimiento o diferenciación y la propia forma de presentarse (secuencia) hace difícil su distinción, como bien observa Harari (2024: 13): «Su existencia también se ve comprometida por la pérdida de contacto entre sus partes constituyentes, más que por representaciones inexactas de la realidad». En el RSD, considerando 12, se adopta un concepto único y amplio sobre «contenido ilícito» e «información», sin diferenciar tipos de información o mensajes concretos, ni su contexto en plataformas. Se obvia toda distinción en su origen, naturaleza y efectos y se han fundido en un solo régimen. El considerando 84 se refiere a «información que no sea ilícita», pero que contribuye a los riesgos sistémicos identificados, en un esfuerzo por abarcar cualquier «desorden informativo».

Los contenidos sintéticos, generados por la IA (texto, audio o vídeo), se han incorporado y no siempre es fácil su clasificación (*v. gr.*, las *deepfakes*[86]). Los

[85] Para compensar desequilibrios, en Australia se ha establecido el *News Media Bargaining Code*, que obliga a las plataformas al pago por la difusión de las publicaciones de los *media*. Y en la UE, la Directiva 2019/790, sobre Derechos de Autor y Derechos Afines, en su art. 15, «Protección de las publicaciones de prensa en lo relativo a los usos en línea». Además, en la UE habrá que observar los efectos del Reglamento Europeo sobre la Libertad de los Medios de Comunicación. Considerando 4: «[…] las plataformas en línea de alcance mundial actúan como puertas de entrada a los contenidos de los medios de comunicación, con modelos de negocio que tienden a eliminar la intermediación para el acceso a los servicios de medios de comunicación y a amplificar los contenidos polarizadores y la desinformación».

[86] En el Reglamento de Inteligencia artificial, las tecnologías con las que se crean las *deepfakes* se considerarán sistemas de IA generativa, basados en modelos fundacionales, pues en el considerando 105 se lee: «Los modelos de IA de uso general, en

prompts, directrices con las que nos comunicamos con la aplicación de inteligencia generativa (GTP), podrían constituir un tipo de mensaje e incluso de creación. El mensaje de noticias (libertad de información en TC), quizás el más comprometido, comporta una crisis existencial, pues su elemento constitutivo, que es la «verdad» de los hechos, está muy cuestionado (Harari, 2024) y no encuentra su identidad en esta cultura del algoritmo[87]. Algunos autores llaman la atención sobre la «verdad algorítmica» (Rubio *et al.*, 2024) y Balaguer (2023) sugiere un nuevo consenso. Algunos profesionales subrayan la falta de presupuestos comunes culturales, educacionales[88] o sociales para abordarla. Y otros señalan a la crisis de objetividad (Sulzberg, 2023). Por su parte, Harari (2024: 7-10) ofrece una mirada distinta que arroja luz al problema: «La visión ingenua sostiene que la información es un intento de representar la realidad, y cuando este intento tiene éxito, lo llamamos verdad». Pero la verdad captada representa solo ciertos aspectos de la realidad, la cual es muy compleja («La verdad y la realidad son, sin embargo, cosas diferentes porque, por muy veraz que sea un relato, nunca podrá representar la realidad en todos sus aspectos»), pues tiene muchos aspectos (lo cual se observa en las redes). Y, añade, se asume que se puede separar «el error» si se representan tanto el nivel objetivo como el subjetivo de la realidad (creencias objetivadas), incluso se puede distinguir la verdad de la falsedad siempre, sin atender a contextos. Pero esto no es siempre así, y «cada verdad» pone su atención en ciertos aspectos de la realidad e ignora otros. Incluso

particular los grandes modelos de IA generativos, capaces de generar texto, imágenes y otros contenidos, presentan unas oportunidades de innovación únicas, pero también representan un desafío para los artistas, autores y demás creadores y para la manera en que se crea, distribuye, utiliza y consume su contenido creativo». Esta IA de riesgo limitado está sometida a obligaciones de transparencia contempladas en el art. 50.2 de RIA. Este precepto, además, establece otro conjunto de obligaciones que deberán observar sus proveedores, y, en particular, en art. 50.4 (obligaciones de transparencia). Esta obligación no se aplicará cuando el uso esté autorizado por ley o cuando el contenido generado por IA haya sido sometido a un proceso de revisión humana o de control editorial y cuando una persona física o jurídica tenga la responsabilidad editorial por la publicación del contenido. Y el art. 53.1 —a), b), c) y d)— establece obligaciones de los proveedores de modelos de IA de uso general, que se refieren a la explicabilidad, la interpretabilidad y la trazabilidad del modelo. También es necesario observar lo establecido en el art. 51 por si el modelo de IA presenta riesgos sistémicos. Además, el citado Reglamento de Libertad de Medios, en su art. 18.1.e), impone a las grandes plataformas asegurarse de que los medios no ofrecen contenidos generados por IA sin revisión humana.

87 Véase https://is.gd/ULeCg2.

88 Véase https://is.gd/Ux2smG.

puede no representar bien la realidad, como ocurre con la desinformación (*disinformation/misinformation*) (Harari, 2024: 10 y ss.). Obviamente, todo ello no es un buen pegamento entre los elementos en las plataformas de las redes sociales, lo que produce desintegración. Es decir, la información está fallando en representar una realidad histórica (pasada), dando lugar a «errores», pero «los errores en la copia del ADN no siempre reducen la aptitud. […] Sin estas mutaciones, no habría proceso evolutivo. […] crea nuevas realidades. La información crea nuevas realidades al conectar diferentes puntos en una red». Este enfoque de Harari, en un momento de emergencia la IA generativa (junto con otras tecnologías revolucionarias), pone la mirada en la idea de la inteligencia artificial en sus aspectos positivos como oportunidad. Las *fuentes informativas*, necesarias para la formación de mensajes, se han visto igualmente afectadas (Pauner Chulvi, 2024), pues los algoritmos (sujeto-objeto) se constituyen tanto en fuentes en sí mismos, proveedoras de información cuyo origen en muchos casos desconocemos (IA generativa, *feeds*), y en sujetos investigadores de fuentes, al constituirse en herramientas-agentes capaces de «explorar» (incluso ilegalmente, *v. gr.*, *Pegasus*) fuentes de todo tipo (Estados[89], empresas, periodistas, etc.)[90]. Inquietante resulta el art. 4, apartados 4 y 5, del Reglamento de Libertad de los Medios de Comunicación, que, mediante la vía de la excepción, permite a los Estados medidas e instalación de programas informáticos intrusivos para conocer las fuentes periodísticas. En cuanto a la libertad de expresión, el mensaje de opinión[91], que por su naturaleza es uno de los más comunes en las redes junto con el de ideas o propaganda, frecuentemente, se presentan como hechos (Rubio *et al.*, 2024: 55), generando confusión. Se desdibujan o difuminan los límites y genera inseguridad jurídica. Sin embargo, no es tanto nuestro mensaje opinático o ideológico en sí mismo el que importa, sino el que el algoritmo cristaliza al captar y procesar todos nuestros datos y comportamientos en la red (públicos o privados), acrisolando las que son «realmente» nuestras opiniones e ideas. La privacidad representa un «obstáculo para el libre comercio», afirma Morozov (2018: 71). El llamado *interés público general* queda decidido por los algoritmos cuantitativamente y sin lograr consenso entre las comunidades fragmentadas.

---

89 La STEDH de 8 de noviembre de 2016, *Magyar Helsinki Bizottság c. Hungría*, considera el derecho de acceso a fuentes públicas como derecho fundamental siempre como ejercicio periodístico cuya información sea de interés general para el público.

90 Sin embargo, ya algunas aplicaciones de IA generativa nos ofrecen las fuentes como parte del servicio y de su transparencia. Por ejemplo, Gemini de Google.

91 En el Convenio de IA del Consejo de Europa (art. 5) llaman a la libertad real del individuo de formar y expresar sus opiniones para la formación de la opinión pública y el ejercicio del voto.

Las afectaciones en el *contenido esencial del derecho y su ejercicio* son relevantes, como ya ha sido constatado empíricamente por Rubio *et al.* (2024: 55-56). La no diferenciación de mensajes y su descontextualización han desdibujado los límites del derecho, provocando conflicto e inseguridad jurídica, que no es fácil de recomponer[92] en la curación o moderación de contenidos, conforme el RSD en nuestro caso. Delinear los perfiles del contenido esencial del derecho requiere una labor de ponderación que solo en sede judicial puede hacerse con todas las garantías jurídicas[93]. Además, el contenido esencial y los límites de su ejercicio se extienden ahora a las máquinas, que han asumido gran parte del ejercicio de las facultades del derecho, lo que explica, a su vez, la deficiencia de ejercicio por parte de los usuarios, que ven vaciado de contenido su derecho. Hay que recordar que, de acuerdo con la jurisprudencia del TEDH, cualquier restricción a estas libertades debe estar «prevista por ley», entendiéndose esta exigencia en sentido sustantivo y no formal. Las facultades de recibir, difundir o investigar están muy interconectadas, y la privación de una puede restringir las otras (Tristante y Teruel, 2023)[94]. Las máquinas nos sustituyen una vez que hemos iniciado el proceso: los algoritmos ejercen en gran medida la facultad de recibir (nos proveen *feeds*, *links*, *respuestas de los motores de búsqueda o de la IA generativa*); la de difundir poniendo a disposición funcionalidades de *likes*, *retweets*, *share*, etc., para difundir, visibilizar y viralizar, conforme a los criterios del algoritmo, e investigan fuentes por nosotros para ofrecernos lo que nos interesa (que es lo que interesa a la máquina que nos conoce). Diferente de este funcionamiento es «el ejercicio no autentico» del servicio o usos no debidos de los que nos alertan tanto el RSD como el RIA por posible manipulación[95].

Por el papel activo que han asumido los sistemas IA en el ejercicio del derecho, deben someterse a los principios de transparencia, explicabilidad y trazabilidad que exige el RIA[96]. Además, observar los «entornos», es decir, respetar los

---

92 Sobre el respeto contenido esencial, el TC se muestra muy protector por ser el derecho a la información fundamento de la democracia: STC 11/1981, de 8 de abril, FJ 8, y STC 235/2007, de 7 de noviembre, FJ 6

93 Véase Riquelme Vázquez (2022). Y la STC 235/2007, de 7 de noviembre, FJ 6. De forma general, sobre el contenido esencial, STC 11/1981, de 8 de abril, FJ 8.

94 La ya citada Sentencia del Tribunal General (Gran Sala) de 27 de julio de 2022, T-125/22, *Rt France c. Consejo de la UE*, muestra la interconexión de estas facultades y la importancia del tipo de mensaje.

95 Un usuario malicioso podría crear cuentas verificadas e interactuar masivamente con las narrativas que le interese para explotar el algoritmo (*El País*, 4 de noviembre de 2024: «Por qué hay tantos usuarios indios respondiendo a mensajes de la dana en X»).

96 Reglamento IA, considerando 27: «Por "transparencia" se entiende que los sistemas de IA se desarrollan y utilizan de un modo que permita una trazabilidad y explicabilidad

«contextos» en los que está previsto que se utilice el sistema (RIA: considerando 12, y CIA, art. 16) para evitar riesgos para los derechos humanos, la democracia y el Estado de derecho en las plataformas sociales. Podría interpretarse, sin violentar el contenido del derecho, pero ampliándolo, que se trata de una nueva facultad al contexto[97] y un límite de descontextualización que puede producirse tanto en el diseño del algoritmo y por los datos (sesgados) de entrenamiento de la IA (descontextualizados) como por los entornos donde se despliega el sistema. Conscientes de que somos nosotros mismos los que suministramos los datos en cada interacción con nuestro consentimiento (Kaminski, 2019). El principio de transparencia se impone, pues la «comprensión del funcionamiento del sistema ayuda a establecer responsabilidades en caso de fallos, accidentes o manipulación intencional facilitando […] exigir que haya cierta rendición de cuentas» (Degli-Esposti, 2023: 59-60). Ahora bien, como reconoce el considerando 12 del RIA, puede haber funcionamientos del sistema de la IA que dificulten no solo la contextualización, sino la misma identificación de responsabilidades:

> Los objetivos del sistema de IA pueden ser diferentes de la finalidad prevista del sistema de IA en un contexto específico. A los efectos del presente Reglamento, debe entenderse por entornos los contextos en los que funcionan los sistemas de IA, mientras que los resultados de salida generados por el sistema de IA reflejan las distintas funciones desempeñadas por los sistemas de IA e incluyen predicciones, contenidos, recomendaciones o decisiones. Los sistemas de IA están diseñados para funcionar con distintos niveles de autonomía, lo que significa que pueden actuar con cierto grado de independencia con respecto a la actuación humana y tienen ciertas capacidades para funcionar sin intervención humana. La capacidad de adaptación que un sistema de IA podría mostrar tras su despliegue se refiere a las capacidades de autoaprendizaje que permiten al sistema cambiar mientras está en uso.

Luego, quién ejerce la responsabilidad (Xu, 2024) es una cuestión abierta. Y es que asistimos a un cambio incuestionable de paradigma: las tecnologías

adecuadas, y que, al mismo tiempo, haga que las personas sean conscientes de que se comunican o interactúan con un sistema de IA […] se evitan los efectos discriminatorios y los sesgos injustos prohibidos […]. La aplicación de esos principios debe traducirse, cuando sea posible, en el diseño y el uso de modelos de IA».

97 Considerando 67: «[…] En particular, los conjuntos de datos deben tener en cuenta, en la medida en que lo exija su finalidad prevista, los rasgos, características o elementos particulares del entorno geográfico, contextual, conductual o funcional específico en el que esté previsto que se utilice el sistema de IA […]».

digitales y los propios sistemas IA y/o algoritmos que, a diferencia de los *media legacy*, pueden generar ideas y tomar decisiones, es decir, poseen autonomía (considerando 12 RIA) y posible identidad digital (Ebers, 2024)[98], y comportan un parámetro tiempo-espacio (atención y viralidad) de trascendentes efectos jurídicos (censor y descontextualización).

III A MODO DE CONCLUSIÓN: LA IA COMO SOLUCIÓN

No todas las mutaciones serán útiles y permanecerán en el nuevo paradigma. Requerirán un examen conforme a un principio teleológico: la máxima satisfacción del derecho a la información y en armonía con el resto de los derechos fundamentales (Higueras, 1995), conscientes de que nuevos derechos están naciendo (Ebers, 2024). Pues se va forjando una identidad digital (de usuarios y máquinas), que reclama personalidad jurídica para la atribución de derechos y deberes[99]. Y los principios jurídicos que se han de reidentificar en el nuevo paradigma digital de la comunicación (Bustos, 2024) deben ser tributarios de las grandes declaraciones y convenios internacionales de derechos humanos con el fin de propiciar un pacto global de la IA[100], sin el cual el internet global, abierto y descentralizado se vuelve casi imposible, al igual que la neutralidad en la red. En este sentido, la doctrina es coincidente: DiResta

---

98 Algunas de estas herramientas IA en las plataformas sociales pueden, en principio, considerarse de riesgo limitado, pero por su contacto directo con los usuarios pueden evolucionar rápidamente a de alto riesgo, requiriendo mayor control (RIA, cons. 93, 50, y arts. 16 a 26 de los de alto riesgo, y arts. 50, 51 y 53 para los de riesgo limitado).

99 Resolución del Parlamento Europeo, de 17 de enero de 2024, sobre los mundos virtuales: oportunidades, riesgos y repercusiones estratégicas para el mercado único (2022/2198(INI)). Sin confundirlo con el criticado Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital.

100 En esta dirección apunta el Convenio europeo de IA (CIA), por su vocación de globalidad, su carácter marco, principalista, que establece (art. 1, 1 y 2) que sus disposiciones tienen por «objeto garantizar que las actividades […] durante el ciclo de vida de los sistemas de IA sean plenamente compatibles con los derechos humanos, la democracia y el Estado de Derecho». También, en esta misma dirección de globalidad, los Principios de la OCDE sobre IA (22-5-2019). Sin embargo, no es suficiente. Dado el carácter voluntario de estos últimos, o del CIA, en la medida que los Estados se incorporen voluntariamente a él será obligatorio. Además, se requiere que no solo los Estados, sino también todo el sector público y privado, se obliguen, incluidas las personas.

(2024), al igual que Harari (2024), propone rediseñar los sistemas de IA conforme a principios. Y Bloch-Wehba (2019) ilustra un rango de posibilidades que arrancan desde principios jurídicos globales (Daskal), hasta un enfoque basado en derechos humanos internacionales (Evelyn Aswad). En definitiva, un nuevo contrato social global que pacifique el ciberespacio, establezca consensos sobre la IA y permita así resolver las problemáticas de la desinformación y evitar el *splinternet*. Asimismo, que establezca unas condiciones[101] que faciliten la posible transformación del derecho a la información sin manipulaciones interesadas. La nueva arquitectura de poder triangular (Balkin, 2019) requiere que este «nuevo contrato social global» incluya al Estado, a las empresas privadas y a los ciudadanos, y así se facilite un nuevo proceso constitucional multifacético e inclusivo (Celeste, 2021). Pues no resulta realista pensar que el Estado pueda prescindir de las tecnológicas que son propietarias de las tecnologías y del *big data*, o prescindir de los usuarios, que deben hacer valer su poder: son dueños de sus datos personales y en internet todos los datos son finalmente datos personales. Sin datos no son posibles los algoritmos ni la IA, hasta ahora. Luego, se puede concluir que los algoritmos y la IA son del usuario (también). A la persona le pertenecen (igualmente). Pues el progresivo *splinternet* no ha venido a armonizar los derechos de privacidad y de información, sino, por el contrario, a ejercer más control sobre ambos, sobre la información y los datos.

Bibliografía

AccesNow. (2023). *What they did in the shadows: Internet shutdowns and atrocities in Ukraine.* Disponible: https://is.gd/YvZD3g.

Álvarez, A. (2023). IA y mediación de los algoritmos: las iniciativas de autorregulación de las plataformas digitales ante conflictos democráticos. En T. Vázquez-Barrio e I. Salazar García (eds.). *Inteligencia artificial, periodismo y democracia* (pp. 171-185). Valencia: Tirant lo Blanch.

Balaguer, F. (2023). *La Constitución del algoritmo.* Zaragoza: Fundación Manuel Giménez Abad.

Balkin, J. M. (2018). The First Amendment in the Second Gilded Age. *Buffalo Law Review*, 66, 979-1012.

Balkin, J. M. (2018). Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation. *University of California Davis*, 51, 1149-1209. Disponible en: https://doi.org/10.2139/ssrn.3038939.

Balkin, J. M. (2019). Free Speech is a Triangle. *Columbia Law Review*, 7 (118), 2011-2056.

[101] Puede resultar inspirador https://is.gd/Bm8HLx.

Barocas, S. (2014). Big Data's End Run around Anonymity and Consent. En V. Stodden, S. Stefan Bender, H. Nissenbaum y J. Lane (eds.). *Privacy, Big Data, and the Public Good* (pp. 43-75). NY: Cambridge University. Disponible en: https://doi.org/10.1017/CBO9781107590205.004.

Barocas, S., Hood, S. y Ziewitz, M. (2013). *Governing Algorithms: A Provocation Piece*. Disponible en: https://is.gd/miqD6U.

Benkler, Y. (2007). *The Wealth of Networks. How Social Production Transforms Markets and Freedom*. New Haven-London: Yale University Press.

Bichoff, P. (2023). Internet Censorship 2023: A Global Map of Internet Restrictions. *Comparitech* [blog], 16-10-2023. Disponible en: https://is.gd/8O2ukC.

Bloch-Wehba, H. (2019). Global Platform Governance: Private Power in the Shadow of the State. *SMU Law Review*, 72, 27-79.

Bradford, A. (2023). *Digital Empires: The Global Battle to Regulate Technology*. NY: Oxford University Press. Disponible en: https://doi.org/10.1093/oso/9780197649268.001.0001.

Bustos, R. (2024). El constitucionalista europeo ante la inteligencia artificial: reflexiones metodológicas de un recién llegado. *Revista Española de Derecho Constitucional*, 131, 149-178.

Celeste, E. (2021). Constitucionalismo digital: mapeando a resposta constitucional aos desafios da tecnologia digital. *Direitos Fundamentais & Justiça*, 15 (45), 63-91. Disponible en: https://doi.org/10.30899/dfj.v15i45.1219.

Cotino, L. (2022). Quien, cómo y qué regular (o no regular) frente a la desinformación. *Teoría y Realidad Constitucional*, 49, 199-238. Disponible en: https://doi.org/10.5944/trc.49.2022.33849.

Degli-Esposti, S. (2023). *La ética de la inteligencia artificial*. Madrid: Consejo Superior de Investigaciones Científicas.

DiResta, R. (2022). Algorithms, Affordances and Agency. En C. Lee Bollinger y R. Geoffrey Stone (eds.). Social Media, Freedom of Speech, and The Future of our Democracy (pp. 121-138). NY: Oxford University Press. Disponible en: https://doi.org/10.1093/oso/9780197621080.003.0008.

DiResta, R. (2024). *Invisible Rulers: The People who Turn Lies into Reality*. NY: Public Affairs.

Douek, E. (2022). The Siren Call of Content Moderation Formalism. En C. Lee Bollinger y R. Geoffrey Stone (eds.). *Social Media, Freedom of Speech, and The Future of our Democracy* (pp. 139-156). NY: Oxford University Press. Disponible en: https://doi.org/10.1093/oso/9780197621080.003.0009.

Ebers, M. (2024). *Avatars and the Protection of Digital Identities in the Metaverse*. Metaverse UA Research Paper, 3. Disponible en: https://is.gd/35sq3J.

Elvira Perales, A. (2023). ¿Quién es Periodista? *Teoría y Realidad Constitucional*, 52, 209-231. Disponible en: https://doi.org/10.5944/trc.52.2023.39015.

Epifanova, A. (2020). *Deciphering Russia's Sovereign Internet Law: Tightening Control and Accelerating the Splinternet. DGAP Analysis, 2*. Berlin: Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V.

Fernández Carballo-Calero, P. (2021). *La propiedad intelectual de las obras creadas por inteligencia artificial*. Navarra: Aranzadi.

Fisher, M. (2023). *A máquina do caos. Como as redes sociais reprogramaram nossa mente e nosso mundo*. São Paulo: Todavia.

García Mahamut, R. y Rallo Lombarte, A. (2015). *Hacia un nuevo derecho europeo de protección de datos*. Valencia: Tirant lo Blanch.

Goldsmith, J. y Wu, T. (2008). *Who Controls the Internet?: Illusions of a Borderless World*. NY: Oxford University Press. Disponible en: https://doi.org/10.1108/sd.2007.05623kae.001.

Harari, Y. N. (2024). *Nexus: A Brief History of Information Networks from the Stone Age to AI*. NY: Penguin Random House LLC.

Hasen, R. L. (2022). *Cheap Speech: How Disinformation Poisons Our Politics — And How To Cure It*. New Haven: Yale University Press. Disponible en: https://doi.org/10.12987/9780300265255.

Haupt, C. E. (2021). Regulating Speech Online: Free Speech Values in Constitutional Frames. *Washington University Law Review*, 99, 751-786.

Herz, M. y Molnar, P. (2012). *The Content and Context of Hate Speech: Rethinking Regulation and Responses*. Cambridge. UK: Cambridge University Press. Disponible en: https://doi.org/10.1017/CBO9781139042871.

Higueras, I. (1995). *Desantes, J. M. et al. Derecho de la información II. Los mensajes informativos*. Madrid: Ed. Colex. Disponible en: https://doi.org/10.15581/003.8.37485.

Johnson, D. R. y Post, D. (1996). Law and Borders. The Rise of Law in Cyberspace. *Standford Law Review*, 48, 1367-1402. Disponible en: https://doi.org/10.2307/1229390.

Kahn, R. A. (2018). Rethinking the Context of Hate Speech Regulation, 14. *First Amendment Law Review*, 200-238.

Kaminski, M. E. (2019). Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability. *Southern California Law Review*, 92, 1529-1615. Disponible en: https://doi.org/10.2139/ssrn.3351404.

Leiner Barry, M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G. y Wolff, S. (1997). A brief history of the internet. *Communications of the ACM*, 40 (2),102-108. Disponible en: https://doi.org/10.1145/253671.253741.

Lemley, M. A. (2021). The splinternet. *Duke Law Journal*, 70 (6), 1397-1428.

Lessig, L. (1996a). The Zones of Cyberspace. *Stanford Law Review*, 48 (5), 1403-1411. Disponible en: https://doi.org/10.2307/1229391.

Lessig, L., (1996b). Reading the Constitution in Cyberspace. *Emory L. J.*, 45, 869-904. Disponible en: https://doi.org/10.2139/ssrn.41681.

Morozov, E. (2018). *Capitalismo Big Tech: ¿Welfare o Nefeudalismo digital?* Madrid: Enclave Libros.

Nachbar, T. (2022). Why We Can't Disconnect Russia From the Internet March. *Blomberg Law*, 14-3-2022. Disponible en: https://is.gd/HkdNSG.

Netanel, N. (2023). Applying Militant Democracy To Defend Against Social Media Harms. *Cardozo Law Review*, 48, 102-189.

Nissembaum, H. (2010). *Privacy in Context.* Stanford: Stanford University Press.

Nugent, N. J. (2023). The Five Internet Rights. *Washington. Law Review*, 98, 527-622.

Pauner Chulvi, C. (2024). La protección de las fuentes periodísticas en la era digital y el impulso regulatorio de la Unión Europea. *Teoría y Realidad Constitucional*, 54, 189-216. Disponible en: https://doi.org/10.5944/trc.54.2024.43312.

Post, D. G. (1996). Governing Cyberspace. *Wayne Law Review*, 43, 155-171.

Presno Linera, M. Á. y Meuwese, A. C. M. (2024). La regulación de la inteligencia artificial en Europa. *Teoría y Realidad Constitucional*, 54, 131-161. Disponible en: https://doi.org/10.5944/trc.54.2024.43310.

Qaissi, H. (2022). Data Brokers: presente y futuro del dato. *Bit*, 31-0¡3-2022. Disponible en: https://is.gd/pBvyGJ.

Riquelme Vázquez, P. (2022). *El contenido esencial de los derechos y libertades: una reinterpretación doctrinal*. Navarra: Aranzadi.

Robles Carrillo, M. (2023). La articulación de la soberanía digital en el marco de la Unión Europea. *Revista de Derecho Comunitario Europeo*, 75, 133-171. Disponible en: https://doi.org/10.18042/cepc/rdce.75.05.

Romano, S., Kerby, N., Schüler, M. y Beraldo, D. (2023). The Impact of Tiktok Policies on Information Flows during Times of war: Evidence of 'Splinternet' and 'Shadow-promotion' in Russia. *The 24th Annual Conference of the Association of Internet Researchers Philadelphia* (18-21 oct.). Philadelphia. Disponible en: https://doi.org/10.5210/spir.v2023i0.13487.

Rubio, R., Alvin, F. F. y Andrade, V. (2024). *Inteligencia artificial y campañas electorales. Disfunciones informativas y amenazas sistémicas de la nueva comunicación política*. Madrid: Centro de Estudios Políticos y Constitucionales.

Sánchez Muñoz, O. (2024). La democracia constitucional en la era digital (a propósito de La Constitución del algoritmo, de Francisco Balaguer Callejón). *Revista Española de Derecho Constitucional*, 131, 373-382.

Singh, S. (2019). Everything in moderation; An Analysis of How Internet Platforms are Using Artificial Intelligence to Moderate User-Generated Content. *New America's Open Tech. Institute*, 1-42.

Simon, H. A. (1971). Designing Organizations for an Information Rich World. En H. Greenberg (ed.). *Computers, Communications, and the Public Interest*. Baltimore: John Hopkins Press.

Starbird, K. (2024). Cómo resistirse a la información errónea de los informes electorales. *SciLine,* 28-8-2024. Disponible en: https://is.gd/fWdAdR.

Strauss, D. A. (2022). Social Media and First Amendment Fault Lines. En C. Lee Bollinger y R. Geoffrey (eds.). *Social Media, Freedom of Speech, and The Future of our Democracy* (pp. 3-16). NY: Oxford University Press. Disponible en: https://doi.org/10.1093/oso/9780197621080.003.0001.

Sulzberg, A. G. (2023). Journalism's Essential Value. *Columbia Journalism Review*, May 15.

Tristante, L. y Teruel, G. (2023). Desinformación y libertad de expresión: el bloqueo europeo de canales rusos ante la invasión de Ucrania a la luz de la Sentencia del Tribunal General (Gran Sala) de 27 de julio de 2022, T-125/22, Rt France C. Consejo de la UE. *Revista de Derecho Público*, 71 (2), 303-329. Disponible en: https://doi.org/10.18543/ed.2936.

Williams, M. (2021). *A ciência do ódio*. Rio de Janeiro: Globo Livros.

Xu, Z. (2024). From algorithmic governance to govern algorithm. *AI & Soc*, 39, 1141-1150. Disponible en: https://doi.org/10.1007/s00146-022-01554-4.