



Revista CIDOB d'Afers Internacionals
ISSN: 1133-6595
ISSN: 2013-035X
publicaciones@cidob.org
Barcelona Centre for International Affairs
España

Colomina Saló, Carme; Pérez-Soler, Susana
Desorden informativo en la UE: construyendo una respuesta normativa
Revista CIDOB d'Afers Internacionals, núm. 131, 2022, Mayo-Septiembre, pp. 141-161
Barcelona Centre for International Affairs
España

DOI: <https://doi.org/10.24241/rcai.2022.131.2.141>

Disponible en: <https://www.redalyc.org/articulo.oa?id=695774517010>

- Cómo citar el artículo
- Número completo
- Más información del artículo
- Página de la revista en [redalyc.org](https://www.redalyc.org)

[redalyc.org](https://www.redalyc.org)

Sistema de Información Científica Redalyc
Red de Revistas Científicas de América Latina y el Caribe, España y Portugal
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso
abierto

Desorden informativo en la Unión Europea: construyendo una respuesta normativa

Information disorder in the European Union: building a regulatory response

Carme Colomina Saló

Investigadora principal, CIDOB; profesora asociada, College of Europe de Brujas, Bélgica.
ccolomina@cidob.org. ORCID: <https://orcid.org/0000-0003-3848-4242>

Susana Pérez-Soler

Doctora en Comunicación Digital y profesora, Universitat Ramon Llull; periodista especializada en periodismo digital, cultura web y redes sociales.
susanaps@blanquerna.url.edu. ORCID: <https://orcid.org/0000-0002-2578-2761>

Cómo citar este artículo: Colomina Saló, Carme y Pérez-Soler, Susana. «Desorden informativo en la UE: construyendo una respuesta normativa». *Revista CIDOB d'Afers Internacionals*, n.º 131 (septiembre de 2022), p. 141-161. DOI: doi.org/10.24241/rcai.2022.131.2.141

Resumen: La desinformación se combate de manera multilateral y desde la multiplicidad de herramientas: plataformas tecnológicas, políticas nacionales, medios de comunicación y plataformas de verificación. A medida que las técnicas desinformativas han ganado en sofisticación y que aumentan también los actores de la disrupción, la Unión Europea (UE) se ha sentido obligada a acelerar un proceso político y regulador que empezó a gestarse en 2015, cuando el Consejo Europeo invitó por primera vez a la Comisión Europea a actuar contra lo que consideraban una amenaza a los procesos democráticos en la UE y en sus estados miembros. Este artículo ofrece un análisis crítico de la evolución de las estrategias de la lucha contra la desinformación en línea en el marco de la UE y las implicaciones que esta voluntad de intervención ha tenido sobre las grandes plataformas digitales que operan en Europa.

Palabras clave: digitalización, UE, desinformación, disrupción, plataformas tecnológicas, regulación

Abstract: Fighting disinformation is a multi-lateral battle that deploys a range of tools: technology platforms, domestic policies, the media and verification platforms. As disinformation techniques have grown more sophisticated and the number of disruptive actors has also risen, the European Union (EU) has felt compelled to accelerate a political and regulatory process that began to take shape in 2015, when the European Council for the first time asked the European Commission to take action against what it considered a threat to democratic processes in the EU and its member states. This paper provides a critical analysis of the evolution of the strategies for fighting online disinformation within the EU framework, and of the implications of this willingness to intervene for the large digital platforms operating in Europe.

Key words: digitalisation, EU, disinformation, disruption, technology platforms, regulation

Internet es hoy un territorio fragmentado. Aquella idea primigenia de un espacio digital convertido en la nueva esfera pública para la comunicación masiva y el empoderamiento colectivo (Castells, 1996) ha dado lugar a una nueva realidad mucho más compleja. La red es un espacio de confrontación geopolítica y desinformación, de choque de relatos y silos de supuestas verdades contrapuestas, que refuerzan la «ciberbalcanización» de las preferencias, según el término que acuñaron en 1997 en un estudio sobre las comunidades electrónicas Van Alstyne y Brynjolfsson (1997). La interconexión digital permite que la información circule a una velocidad mayor que la capacidad humana para procesarla. Esta superabundancia de contenidos, que alimentan la conversación pública en línea, ha cambiado nuestra relación con la información y la veracidad. En este proceso de digitalización de espacios, conocimientos e identidades, las empresas

La red es un espacio de confrontación geopolítica y desinformación, de choque de relatos y silos de supuestas verdades contrapuestas, que refuerzan la «ciberbalcanización» de las preferencias.

tecnológicas de Silicon Valley, como Facebook y Google, están creando problemas nuevos tanto en escala como en naturaleza: se valen de pantallas ubicuas y conectadas a todas horas, dotadas de precisos sistemas de captura, medición, segmentación

y análisis de datos para construir un modelo de negocio dominante basado en la persuasión industrializada (Williams, 2021). Esta «silicolonización del mundo» (Sadin, 2016) desborda las costuras tradicionales de las democracias occidentales, en general, y de la Unión Europea (UE), en particular. Andrew Keen, empresario de Silicon Valley, ya advirtió en 2007, en su libro *The Cult of the Amateur*, que Internet estaba sustituyendo el verdadero conocimiento por la «sabiduría de la turba» (*wisdom of the crowd*), a partir de borrar las fronteras entre hechos y opiniones, y entre los argumentos informados y las especulaciones fatuas. En el contexto de esta sustitución, la verosimilitud ha ido ocupando el puesto de la verdad, como unidad de medida (Kakutani, 2019).

La fuerza de la irrupción de la desinformación en línea ha supuesto la aparición de un «nuevo daño social» (Del Campo, 2021) que se expresa a través de falsedades de distinto tipo, algunas legales y otras ilegales, impactando en el discurso público y la seguridad humana. La desinformación tiene, además, implicaciones de gran alcance para los derechos humanos y las normas democráticas. También disminuye los indicadores más amplios de calidad democrática, perturba la confianza institucional de la ciudadanía, distorsiona las elecciones libres y justas, e incluso fomenta la violencia digital y la represión (Harari, 2018; Peirano, 2019; Innerarity, 2020; Zuboff, 2020). El carácter inherentemente afectivo de las redes sociales ha multiplicado los intercambios persuasivos, los niveles de sentimentalización, y ha impactado en la percepción de legitimidad

de los mediadores tradicionales, modificando la relación del individuo con su representante político, en particular. Asimismo, es difícil regular los efectos de una experiencia tecnológica que se ha vuelto íntima, donde la divisoria clásica entre esfera pública y privada se ha visto difuminada. Se agota la idea de la representación vertical del poder (Arias Maldonado, 2016: 179-183).

Ante tales desafíos, gobiernos e instituciones democráticas ensayan respuestas sociales, políticas y legislativas a un fenómeno en constante evolución. Desde 2015, la UE ha intentado desarrollar un marco propio de principios y soluciones al desafío de la desinformación, demostrando su voluntad de gobernanza. Al respecto, este artículo analiza la evolución normativa y conceptual de dicha estrategia. Para ello, es preciso conocer la aceleración de los distintos niveles de intervención desplegada por las instituciones de la UE desde 2015 hasta hoy, pero, sobre todo, es imprescindible entender que se trata de un desafío en permanente estado de mutación, con origen y solución multifactorial (Seijas, 2020). Así, tras hacer una revisión de la literatura sobre la aproximación de la UE al fenómeno de la desinformación, el artículo evalúa en las distintas secciones cómo las medidas normativas, que en un principio se centraron en el control del contenido, fueron sofisticándose y diversificándose a partir de la necesidad de dar respuesta a la complejidad del desafío.

Evolución conceptual del fenómeno de la desinformación

La *infocracia*, o «régimen de la información» en el mundo digital, que ha teorizado Byung-Chul Han (2022), es una forma de dominio en el que «la información y su procesamiento mediante algoritmos e inteligencia artificial determinan de modo decisivo los procesos sociales, económicos y políticos». La capacidad de alterar la información o los datos, factores decisivos para la obtención del poder, trastoca los procesos democráticos. Aunque el concepto de desinformación es anterior a la era digital y, por tanto, no se adscribe exclusivamente a la revolución que significó la web y su «vientre tecnológico», donde navegamos por un mundo virtual que se disuelve en fragmentos (Baricco, 2019), las herramientas digitales facilitan la distribución masiva y veloz del contenido que se vierte en ella –veraz o no–.

En este contexto, la UE define la desinformación como «información verificable falsa o engañosa que se crea, presenta y difunde con fines de lucro económico o para engañar intencionalmente al público, y que puede causar daño público»

(Comisión Europea, 2018b). Según el informe final del Grupo de Expertos de Alto Nivel sobre las noticias falsas y desinformación en línea (ibídem, 2018a), la producción y promoción de la desinformación puede estar motivada por factores económicos, objetivos de reputación o agendas políticas e ideológicas, y sus efectos pueden verse exacerbados por la forma en que las diferentes audiencias y comunidades reciben, involucran y amplifican dicha desinformación. Cualquiera que tenga una cuenta en redes sociales puede crear y difundir desinformación: gobiernos, empresas, otros grupos de interés o individuos.

Ampliando el foco, la Comisión Europea y la Unesco –la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura– se refieren a tres tipos de desórdenes informativos: la desinformación, la información errónea y la mala información (Wardle y Derakhshan, 2017).

- Desinformación (*disinformation*): información deliberadamente falsa, difundida por motivos económicos, ideológicos o por alguna otra razón. Es el tipo de desinformación que más preocupa a los expertos por su intención deliberada de engañar a la opinión pública.
- Información errónea (*misinformation*): información falsa, pero transmitida con el convencimiento de su veracidad. Aquí se incluyen errores ortográficos y/o tipográficos, datos inexactos o fechas y/o nombres incorrectos.
- Mala información (*mal-information*): información verdadera, pero de ámbito privado o restringido, que se saca a la luz pública con la intención de dañar a una persona, una institución o un país y que, por lo tanto, no debería ser publicada.

Esta clasificación determina la intencionalidad de dañar o sacar rédito como el elemento distintivo entre la desinformación y el contenido falso o erróneo, por lo que define también la voluntad de su carácter disruptivo. El ejecutivo de la UE admite que, además, «la desinformación erosiona la confianza en las instituciones» y daña la democracia «al obstaculizar la capacidad de los ciudadanos para tomar decisiones informadas»¹. También advierte que la desinformación está destinada a polarizar las sociedades democráticas al crear o profundizar las tensiones, así como socavar pilares democráticos como los sistemas electorales. Por su parte, el Parlamento Europeo ve la desinformación como una «presión

1. Comisión Europea. «Tackling online disinformation». *Shaping Europe's digital future* (s/f) (en línea) [Fecha de consulta: 15.10.2021] <https://digital-strategy.ec.europa.eu/en/policies/online-disinformation>

sistemática creciente» sobre las sociedades europeas y su estabilidad electoral². De esta forma, la verdad se ha ido compartimentando en silos distintos que han acabado con la idea de la información como elemento de cohesión e interrelación social (Julibert, 2018). Sin relatos compartidos, la hiperconectividad digital nos conecta solo con aquellos que, desde esta nueva comunidad extraterritorializada, comparten nuestra visión del mundo. Además, las mentiras tienen hasta un 70% de posibilidades más de ser retuiteadas (Vosoughi *et al.*, 2018). Parte de este desequilibrio que amplifica el contenido falso responde a la emocionalidad con que se empaqueta la desinformación, pero también a la arquitectura algorítmica que premia la capacidad de viralización.

Finalmente, la misma Comisión Europea (2018a) desaconseja, en el informe final del Grupo de Expertos de Alto Nivel antes mencionado, referirse al amplio universo de las informaciones falsas o erróneas que circulan en Internet con la manida expresión de *fake news*, que se popularizó con motivo de las elecciones presidenciales de 2016 en Estados Unidos y el referéndum del Brexit celebrado en junio de ese mismo año en el Reino Unido. Para los expertos que han elaborado este informe, liderados

La desinformación tiene implicaciones de gran alcance para los derechos humanos y las normas democráticas: disminuye los indicadores más amplios de calidad democrática, perturba la confianza institucional de la ciudadanía, distorsiona las elecciones libres y justas, e incluso fomenta la violencia digital y la represión.

por la profesora Madeleine De Cock Buning, resulta un término inadecuado para definir el complejo problema de la desinformación porque, como hemos visto, involucra contenido que no es solamente falso, sino también información fabricada de forma errónea o difundida con mala intención. Además, la desinformación comprende prácticas que van más allá de los contenidos con apariencia de *noticia*, como, por ejemplo, los mensajes generados por cuentas automatizadas (*bots*) utilizadas para manipular la opinión pública digital, los vídeos fabricados o manipulados (*deepfake*), la publicidad dirigida, la utilización de plataformas para operaciones de injerencia extranjera, los mensajes en redes sociales y canales de mensajería instantánea, las capturas de pantalla, los memes, etc. También hace referencia al mismo comportamiento digital, que tiene más que ver con la distribución de desinformación que con la producción de esta, y que abarca los comentarios, las comparticiones, los «me gusta», los seguidores,

2. Resolución del Parlamento Europeo, de 23 de noviembre de 2016, sobre la comunicación estratégica de la Unión para contrarrestar la propaganda de terceros en su contra (2016/2030(INI)) (2018/C 224/08).

o cualquier elemento de reacción digital a un contenido. En segundo lugar, el término *fake news* no solo es inadecuado, sino que también es engañoso, porque ha sido apropiado por algunos políticos y sus partidarios, que lo utilizan para desestimar cualquier cobertura o pronunciamiento que encuentren desafiante para sus intereses y, por lo tanto, se ha convertido en un arma arrojadiza con la que actores poderosos pueden interferir en la circulación de información y atacar a los medios de comunicación.

Al analizar los diferentes actores responsables de la desinformación, el grupo de trabajo sobre libertad de expresión y abordaje de la desinformación de la Unesco hace la distinción entre los responsables de la creación del contenido desinformativo y los encargados de su distribución: entre los instigadores (directos o indirectos), que están en el origen de la desinformación, y los agentes (*influencers*, individuos, organizaciones, gobiernos, empresas, instituciones) encargados de difundir las falsedades (Bontcheva y Posetti, 2020). En este contexto, cualquier intento de regulación del fenómeno debería tener en consideración tres vectores distintos: los actores, el contenido y las tácticas de diseminación o comportamientos de la desinformación (Lewandowsky *et al.*, 2020).

Sobreexposición del poder de las plataformas tecnológicas

La principal pieza del sistema de difusión de desinformación son las redes sociales. La historia de estas empresas tecnológicas —que tienen un papel clave en la construcción de la esfera pública digital— comienza en la segunda mitad de los años 2000 con la irrupción de LinkedIn (2003), Facebook (2004), YouTube (2005), Twitter (2006) e Instagram (2008). Las redes sociales proporcionan un entorno inédito para la difusión de información, al combinar dos elementos completamente nuevos: a) la producción de contenidos, que no es ya el fruto de las organizaciones de medios de comunicación, sino de cualquier persona que sube su historia e interactúa con los contenidos producidos por otros, y b) la personalización de los contenidos a los que accede el usuario, que se esbozará en función de los otros a los que sigue y de la publicidad que recibe a partir de sus intereses —tanto los que declara en su perfil como los que la plataforma deduce de su actividad en línea— (Badillo, 2019). El modelo de negocio de estas plataformas en línea se basa, precisamente, en impulsar aquel contenido que genera reacciones, permitiendo a estas plataformas *vender* la atención de los usuarios a los anunciantes. Esta «economía de la atención» (Davenport y Beck, 2002) se

construye algorítmicamente. De la misma manera, los algoritmos son centrales en la difusión del contenido manipulado, ya que pueden ser deliberadamente explotados para la distribución de contenido político polarizante (Flore, 2020).

Durante las elecciones presidenciales estadounidenses de 2016, las tecnológicas se presentaban ante el mundo como simples canales de distribución de contenidos. Sin embargo, la revelación de determinadas campañas de manipulación informativa (véanse Schaedel, 2016 y Subramanian, 2017) y de interferencias rusas sobre el proceso electoral (Mueller, 2019) forzaron a estas plataformas digitales a asumir cierta responsabilidad sobre el contenido que difunden. Desde entonces, han establecido estrategias de moderación de contenidos de manera automatizada y humana, así como sistemas de denuncia para que los usuarios puedan alertar del contenido falso que circula dentro de las plataformas, además de poner límites a la viralidad e ins-

taurar acuerdos con plataformas de verificación. Ahora bien, si la llegada de Trump a la Casa Blanca marcó una nueva consciencia sobre el poder de la construcción narrativa de la posverdad³, su traumática salida se tradujo en una herida reputacional

La principal pieza del sistema de difusión de desinformación son las redes sociales, que proporcionan un entorno inédito, al combinar dos elementos completamente nuevos: la producción y la personalización de los contenidos.

para las plataformas tecnológicas todavía abierta. Después del ataque al Capitolio en Washington, el día 6 de enero de 2021, que terminó con seis víctimas mortales y decenas de heridos, las empresas tecnológicas decidieron eliminar las redes sociales de Donald Trump: sus cuentas de Twitter y Facebook quedaron suspendidas el mismo 6 de enero, mientras millones de ciudadanos de todo el mundo seguían en directo el asalto al corazón de la democracia estadounidense. En menos de 24 horas, estas suspensiones temporales se hicieron permanentes, y Trump se convertía en el primer presidente cancelado en nombre de la democracia. Instagram, Snapchat, Twitch o YouTube también eliminaron sus perfiles. Al mismo tiempo, el debate público se centraba en la responsabilidad de las redes sociales en la polarización política en Estados Unidos.

Fue el colofón de una crisis reputacional para las grandes plataformas tecnológicas que ha ido *in crescendo* y que tiene a Facebook como uno de los máximos exponentes de este declive (Müller y Schulz, 2019). La falta de salvaguardas dentro de la plataforma de Mark Zuckerberg ya quedó en evidencia

3. Aquí entendemos la posverdad como un concepto-lugar común, que engloba desde la falsedad retórica a la decadencia de los hechos objetivos y la verdad racional, científica o académica (Kakutani, 2019).

con la filtración de datos de 87 millones de usuarios de Facebook a Cambridge Analytica en 2018. Más tarde, la publicación de los informes internos de la compañía filtrados a *The Washington Post* y una treintena de medios más por la exabajadora de Facebook, Frances Haugen (Lima, 2021) constataba que la plataforma era plenamente consciente del alcance y el impacto de la desinformación en los sistemas democráticos y, a pesar de ello, no había tomado medidas al respecto. Aunque, como apunta Baricco (2019: 225), «la fuerza de los sistemas nunca está en las oligarquías del vértice» sino en el cambio de paradigma; estas «nuevas élites» tecnológicas han impuesto una nueva forma de estar en el mundo. Las empresas acumulan información sobre sus usuarios –incluso sobre aquellos que no están en sus plataformas– para confeccionar una dieta de contenidos a medida y personalizar su experiencia digital, alterando algorítmicamente la percepción de la realidad. Esta reinterpretación de nuestra relación con el entorno se construye a partir de un conocimiento profundo de la identidad digital de unos usuarios que, sin embargo, desconocen en la mayoría de los casos los métodos y condiciones a partir de los cuales se recogen, analizan y explotan sus datos. La misma desproporción sienten muchos gobiernos democráticos ante el nivel de conocimiento que tienen estas plataformas sobre los intereses, relaciones y comportamientos del individuo-usuario, convertido en producto para el beneficio empresarial, además de ciudadano (Peirano, 2019). Al final, esta asimetría de información se convierte en asimetría de poder en favor de unas plataformas tecnológicas que, a partir de la sobreexposición acumulada durante la aceleración digital impuesta por el confinamiento pandémico, encaran una nueva presión social y política sobre los límites de la supremacía acumulada.

Los gigantes tecnológicos del GAFAM (Google, Amazon, Facebook, Apple y Microsoft), principales exponentes del capitalismo de plataforma que han construido su modelo global a partir de la desregulación estadounidense, son la punta de lanza de lo que Shosana Zuboff (2020: 52-55) llama «capitalismo de vigilancia», el cual define como «un nuevo orden económico que reclama para sí la experiencia humana como materia prima gratuita aprovechable para una serie de prácticas comerciales ocultas de extracción, predicción y ventas». La concentración de poder digital genera, por lo tanto, desigualdad digital. Así es como un sistema nacido para redistribuir el poder ha acabado distribuyendo sobre todo posibilidades (Baricco, 2019), creando a cambio inmensas concentraciones de poder que se ubican en espacios «diferentes a los del siglo xx, pero no parecen ser menos impenetrables». Voces más pesimistas como la de Yuval Noah Harari (2018) advierten de los peligros de crear «dictaduras digitales», construidas con macrodatos, para concentrar el poder en manos de una élite minúscula y condenar a una mayoría a la irrelevancia.

Con todos estos antecedentes, el marco normativo desplegado por la UE busca mitigar los vacíos legales actuales, al tiempo que intenta frenar las medidas unilaterales que algunas de estas plataformas han adoptado recientemente sin que la justicia se hubiera pronunciado aún, sin diálogo ni supervisión –como ocurrió con la expulsión del presidente Trump de las redes sociales–. La canciller alemana, Angela Merkel, ya alertó en ese momento del enorme poder de las plataformas tecnológicas en detrimento de la jurisprudencia de los estados. Es por ello por lo que la UE ha ido desarrollando un marco propio para la regulación de la esfera digital, donde se protejan los derechos fundamentales de las personas; así, pone el foco en las empresas tecnológicas exigiéndoles apertura, transparencia y seguridad.

Aceleración regulatoria de la UE

El proceso regulador en la UE empezó a gestarse en 2015, cuando el Consejo Europeo invitó por primera vez a la Comisión Europea a actuar contra lo que consideraban una amenaza a los procesos democráticos en la Unión y en sus estados miembros. Sin embargo, la percepción de riesgo que podía suponer en aquel momento la desinformación estaba completamente mediada por el conflicto en Ucrania⁴, y los distintos niveles de entendimiento político entre los gobiernos de los distintos estados miembros de la UE y la Federación Rusa. La desinformación se entendía entonces únicamente como una amenaza exterior de la que algunos estados miembros se sentían completamente alejados, lo que dibujaba una Europa de distintas velocidades ante la desinformación, especialmente desde un punto de vista legislativo (Magallón, 2019). Este contexto determinará que una de las primeras acciones directamente vinculadas a la detección de desinformación que se desplegará en Bruselas sea la creación, en 2015, de una unidad de comunicación estratégica, dentro del Servicio Europeo de Acción Exterior, para la identificación de contenido desinformativo sobre la UE con origen en medios de comunicación y plataformas rusas.

En el año 2016 se añade una nueva dimensión al desafío. El referéndum del Brexit puso de manifiesto que decisiones de máxima importancia para el futuro de la UE, como la separación de uno de sus estados miembros (Reino Unido), podían verse condicionadas por campañas de desinformación apoyadas en las tecnologías más sofisticadas (Bastos y Mercea, 2019). Fuera del territorio de la UE, otros ejem-

4. En 2014 se produjo la anexión rusa de Crimea y el inicio de la guerra del Donbás.

plos, como la mencionada victoria de Donald Trump a la presidencia de Estados Unidos, alertaron sobre el alcance de ciertas campañas de desinformación en la política, además de apuntar directamente a la capacidad disruptiva patrocinada desde Rusia (Mueller, 2019). Con el horizonte de las elecciones al Parlamento Europeo previstas para 2019, la respuesta en el seno de la Unión entró en fase de aceleración.

Por un lado, el Informe del Grupo de Expertos de Alto Nivel sobre las noticias falsas y la desinformación en línea sentó las bases conceptuales del fenómeno (Comisión Europea, 2018a); por el otro, a finales de 2018, la Comisión presentó también el Código de Buenas Prácticas en materia de Desinformación (Monti 2020). Este código, de carácter voluntario, es el primer mecanismo autorregulador acordado entre las instituciones europeas, los representantes de las grandes plataformas en línea y de redes sociales, así como

El proceso regulador en la UE empezó a gestarse en 2015, cuando el Consejo Europeo invitó por primera vez a la Comisión Europea a actuar contra lo que consideraban una amenaza a los procesos democráticos en la Unión y en sus estados miembros.

de la industria publicitaria. En este instrumento, que podríamos considerar de derecho blando porque se establece de forma voluntaria, se reconoce el papel de cada uno de estos diferentes actores en la capacidad de diseminación de la desinformación y su impacto en un amplio espectro de usuarios. En este

sentido, el código rompe con la coartada de intermediación aséptica a la que se aferraron durante años las grandes plataformas digitales; pero también se convierte, desde el punto de vista de la responsabilidad sobre el contenido, en una externalización en favor de empresas privadas del poder de regular el discurso público en línea, con el impacto político y social que ello supone.

Cualquier restricción impuesta a la diseminación de contenido inevitablemente interfiere con el derecho a recibir y compartir información (Kuczerawy, 2019). Sin embargo, una tras otra, las grandes plataformas acceden a la corresponsabilidad que reclama la UE. Aquel mismo año 2018, Facebook, Google y Twitter, Mozilla y representantes de la industria publicitaria suscribieron el código. Microsoft se unió en 2019 y, un año más tarde, lo hizo TikTok. Si, en un primer momento, corresponsabilizar a las plataformas tecnológicas fue un paso decisivo para despojar a las grandes redes sociales de su supuesto argumento de ser meras autopistas para la circulación de una información sobre la cual no sentían ninguna incumbencia u obligación, la aceleración en el proceso de digitalización e *infodemia*⁵ vividos duran-

5. Entendida como la avalancha de desinformación registrada durante la pandemia de la COVID-19.

te la pandemia de la COVID-19 obligan a la UE a dar un paso más: para prevenir y combatir la desinformación resulta imprescindible que los algoritmos que utilizan las plataformas tecnológicas, tanto para distribuir los contenidos como para clasificarlos, sean transparentes.

En junio de 2022, la Comisión Europea presentó una nueva actualización de este Código de Buenas Prácticas en materia de Desinformación⁶. Significativamente, la efectividad del nuevo texto todavía depende de la voluntariedad de las empresas en el cumplimiento de una ampliada lista de requisitos, entre los cuales se incluye brindar mayor acceso a los datos por parte de investigadores externos, proporcionar desgloses detallados país por país sobre cómo circula la desinformación y reducir los beneficios económicos de las noticias falsas. La Comisión opta, así, por seguir apostando por la corregulación a través de un mecanismo voluntario, en lugar de aprobar nuevas reglas vinculantes que pudiesen propiciar una eliminación excesiva de contenido. Se trata de una decisión meditada, a partir de las contradicciones vividas en los años anteriores. El hecho de alentar a actuar contra contenido considerado «dañino», en lugar de «ilegal», dificulta que la supresión de cierta desinformación sea una restricción fácilmente justificable en el contexto de la libertad de expresión. Consciente de ello, la Comisión opta por evitar un enfoque paternalista (Harrison, 2021), enfatizando los méritos de la corregulación con las plataformas de redes sociales y empoderando a los usuarios para reconocer la desinformación. Sin embargo, este enfoque también genera dudas, ya que, a medida que estas plataformas tecnológicas —convertidas en *guardianas* del contenido— han ido aumentando su grado de compromiso con las políticas de eliminación de contenido no ilegal, la UE ha constatado también cómo arreciaban las críticas, entre el activismo y el mundo académico, a una «privatización de la censura» (Monti, 2020) por parte de gobiernos e instituciones de la UE, porque ello implica una delegación de poder a actores privados.

La transparencia y la rendición de cuentas en relación con las acciones curatoriales son esenciales para proteger la libertad de expresión. El relator especial de Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y expresión ha pedido reiteradamente la alineación de las políticas de las plataformas digitales sobre moderación de contenidos con los estándares de libertad de expresión (Naciones Unidas, 2018). Esta evolución ha acabado generando un nuevo e incómodo escenario en la estrategia europea de lucha contra la desinformación, especialmente de proporcionalidad y de protección efectiva de derechos fundamentales (Kuczerawy, 2019). Al fin y al cabo, el impacto de la mentira en los sistemas democráticos puede ser do-

6. Véase: https://ec.europa.eu/commission/presscorner/detail/es/qanda_22_3665

ble: por un lado, puede erosionar la confianza, polarizar e incluso distorsionar el libre desarrollo de procesos electorales; por otro, si la eliminación de una mentira dañina se ejerce de manera desproporcionada e incluso arbitraria, el resultado puede impactar en el ejercicio de las libertades individuales y colectivas (García Morales, 2020). Ante este dilema, las instituciones europeas han ido ganando conciencia de que el desafío que plantea la desinformación no proviene solo de su contenido, sino también de cómo se distribuye y se promociona en las redes sociales, es decir, de las estrategias y técnicas para maximizar la capacidad de influencia de dicho contenido.

En los últimos años, se han popularizado las campañas de *astroturfing*, es decir, conversaciones en redes sociales generadas por cuentas automatizadas para favorecer a un partido político, atacar a rivales o magnificar algunos temas para colocarlos

En junio de 2022, la Comisión Europea presentó una nueva actualización del Código de Buenas Prácticas en materia de Desinformación. Significativamente, el texto sigue apostando por la correulación a través de un mecanismo voluntario de las empresas.

en la agenda mediática. En la esfera pública digital operan *bots* (cuentas de redes o programas informáticos que efectúan automáticamente tareas reiterativas), *trols* (usuarios, con identidad desconocida, que pretenden generar polémica en línea) y cuentas mercenarias. Se calcula que aproximadamente el 15% de las cuentas activas

en Twitter, por ejemplo, son *bots*, es decir, no pertenecen a personas reales, sino que son automáticas (véase Confessore *et al.*, 2018). A pesar de que es difícil conocer la dimensión de la desinformación porque funciona como parte de una economía clandestina y adopta distintas formas, solo en 2021, Facebook afirmó haber eliminado 52 redes de influencia que operaron de manera coordinada en 34 países para dirigir o corromper el debate público por objetivos estratégicos⁷.

En este contexto, el Plan de Acción para la Democracia Europea –la agenda de la Comisión Europea para fortalecer la resiliencia de las democracias de la UE– que se presentó en diciembre de 2020 (Comisión Europea, 2020a), amplía el concepto y las estrategias de lucha contra la desinformación para abordar también las «operaciones de influencia de la información» y la «interferencia extranjera en el espacio de la información». Ambos conceptos abarcan los esfuerzos coordinados para influir en una audiencia objetiva por medios engañosos, involucrando en algunos casos un

7. Véase: «Recapping Our 2021 Coordinated Inauthentic Behaviour Enforcements». Meta (20 de enero de 2022) (en línea) [Fecha de consulta: 18.02.2022] <https://about.fb.com/news/2022/01/december-2021-coordinated-inauthentic-behavior-report/>

«actor estatal extranjero» o sus «agentes». Además, ese mismo año, y con la misma voluntad de reforzar las herramientas civiles para la detección de la desinformación, la UE puso en marcha el Observatorio Europeo de Medios Digitales (EDMO, por sus siglas en inglés)⁸, que sirve como centro de conexión para que los verificadores de datos y los académicos colaboren entre sí, al tiempo que los alienta a vincularse activamente con organizaciones de medios de comunicación y expertos en alfabetización mediática a fin de brindar apoyo a los responsables de la formulación de políticas. Todo ello ayuda a coordinar las acciones en la lucha contra la desinformación. Las actividades del EDMO se basan en cinco líneas estratégicas para luchar contra la desinformación de manera multilateral: a) mapear y apoyar a las organizaciones de verificación de datos en Europa; b) apoyar y coordinar actividades de investigación sobre desinformación a nivel europeo; c) crear un portal público que proporcione a los profesionales de los medios de comunicación, los profesores y los ciudadanos información y materiales destinados a impulsar la alfabetización mediática, d) diseñar un marco para garantizar el acceso seguro y protegido de la privacidad a los datos de las plataformas, y e) brindar apoyo a las autoridades públicas en el seguimiento de las medidas implementadas por las plataformas en línea para limitar la propagación y el impacto de la desinformación.

Así, la diversificación de herramientas ha ido de la mano de una diversificación de enfoques. En línea con la aproximación defendida por el grupo de trabajo sobre libertad de expresión y abordaje de la desinformación de la Unesco, el objetivo de la UE es reforzar no solo la detección del contenido, sino también la capacidad de actuación sobre la distribución de dicho contenido y las tácticas automatizadas que amplifican su poder de penetración en la conversación pública y en los procesos individuales de formación de opiniones y valores.

La Ley de Servicios Digitales y el «efecto Bruselas»

Toda esta aceleración de medidas e instrumentos dio un salto cualitativo con la aprobación del paquete legislativo de Servicios Digitales, compuesto por la Ley de Servicios Digitales (DSA, por sus siglas en inglés) y la Ley de Mercados

8. European Digital Media Observatory (EDMO) (en línea) [Fecha de consulta: 18.02.2022] <https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory>

Digitales (DMA, por sus siglas en inglés). Como la misma Comisión había reconocido en sus primeros documentos internos sobre una futura DSA, el «mosaico de normas nacionales» emergentes sobre la moderación de contenido planteaba la necesidad de crear un nuevo «marco [legislativo] general para los servicios digitales en línea» (Comisión Europea, 2019).

La DSA, presentada por la Comisión Europea a finales de 2020 y aprobada en abril de 2022, es la principal herramienta y la única de carácter regulatorio *fuerte* de la UE (Comisión Europea, 2020b). Persigue combatir la desinformación desde la transparencia sobre la arquitectura e implementación de los algoritmos que determinan lo que los usuarios ven –los llamados «sistemas de recomendación» de las plataformas tecnológicas–, además de aspirar a la trazabilidad de las campañas de promoción de esos contenidos, es decir, sobre quién patrocina

Toda la aceleración de medidas e instrumentos contra la desinformación dio un salto cualitativo con la aprobación, por parte del Parlamento Europeo, del paquete legislativo de Servicios Digitales, compuesto por la Ley de Servicios Digitales (DSA) y la Ley de Mercados Digitales (DMA).

los anuncios que ven los usuarios. La DSA también corresponsabiliza a las empresas tecnológicas de la propagación de la desinformación y las involucra en la detección de las mentiras. Sin embargo, el texto señala que las tecnológicas no son responsables de los contenidos ilegales que se comparten y solo deben eliminarlos cuando un juez así lo establezca. El

marco legislativo de la UE quiere que lo que sea ilegal en el ámbito analógico lo sea también en el digital, mediante la imposición de la transparencia total hacia las plataformas tecnológicas, pero dejando en manos de los tribunales de justicia de cada Estado miembro la eliminación de los contenidos, con el fin de evitar que las empresas tecnológicas tengan un papel de censoras.

Por su parte, la DMA agrupa en un mismo texto legislativo las distintas normas que la UE había impuesto hasta ahora para evitar las prácticas monopolísticas de los gigantes digitales. Con ella se prohibirán prácticas como impedir que los usuarios desinstalen aplicaciones preinstaladas, y se exigirán medidas de interoperabilidad para eliminar ecosistemas cerrados y facilitar que los consumidores puedan cambiar de plataforma si así lo desean. Pero, además, la legislación incluye un elemento sancionador –inexistente hasta el momento– de hasta el 6% de la facturación mundial de estas empresas en caso de una primera infracción y hasta el 20% en caso de reincidencia. En el ámbito de la gobernanza, la DSA y la DMA suponen también la superación del modelo de autorregulación aplicado hasta el momento. Pero, sobre todo, refuerzan el carácter de «poder normativo» sobre el cual la UE construye su legitimidad y su aportación al orden global (Whitman, 2011).

La UE ha estado durante mucho tiempo a la vanguardia de la regulación de la esfera digital. El precedente más claro se remonta a la década de los noventa del siglo pasado, con el consenso surgido en la UE para considerar la privacidad de los datos como un derecho fundamental, consagrado en el Tratado de Funcionamiento de la UE en 2007 (Newman, 2008). Sin embargo, la pieza legislativa clave en este terreno llegó una década más tarde, con la Comisión Junker (2014-2019). El Reglamento General de Protección de Datos (RGPD), en 2016, que reemplazaba a la Directiva de privacidad de datos, consolidó los derechos de los ciudadanos europeos sobre sus datos, limitando las cantidades que se pueden recopilar y exigiendo que se procesen de forma segura, temporal y transparente, además de añadir nuevas obligaciones como el «derecho al olvido», entre otras. Ambas propuestas legislativas, tanto el RGPD como la DSA, tienen en común una aproximación al desafío digital claramente «centrado en el consumidor» (Harrison, 2021), que ejemplifica el posicionamiento de la UE ante una competición tecnológica que, para los grandes actores globales, tiene un fuerte componente geopolítico y securitario (Hoffman *et al.*, 2020).

La DSA y la DMA refuerzan el carácter de «poder normativo» sobre el cual la UE construye su legitimidad y su aportación al orden global, el llamado «efecto Bruselas»: el impacto extraterritorial de las legislaciones de la UE, las normas y valores europeos.

Sin embargo, como ya ocurrió con el RGPD, el paquete regulador de los servicios digitales puede contribuir al llamado «efecto Bruselas» (Bradford, 2020): el impacto extraterritorial de las legislaciones de la UE, las normas y valores europeos. Así como el RGPD acabó influyendo en las prácticas y los límites en el uso de datos de los usuarios también a nivel también extracomunitario (Gstrein y Zwitter, 2021), las acciones normativas de la UE en el campo de la desinformación están demostrando cosechar su propio impacto más allá de la Unión. La consecuencia más clara ha sido la asunción de responsabilidades por parte de las grandes plataformas digitales globales sobre el contenido compartido en línea. Un posicionamiento inexistente antes de la firma del Código de prácticas de la desinformación (2018) o el Código de conducta voluntario impulsado por la Comisión Europea en 2016 para combatir el discurso de odio ilegal en línea (Jourová, 2016). Pero el impacto de la DSA y la DMA van mucho más allá: no solo pretenden dar forma al espacio digital europeo, tanto económica como políticamente, sino que, a la vez, ofrecen un marco de regulación del mercado. Esta voluntad de gobernanza del espacio de la UE tiene consecuencias directas sobre el poder de las grandes empresas tecnológicas; un poder construido a través de la extraterritorialidad y la desregulación.

Conclusiones

Los expertos reconocen que la UE se ha movido más rápido de lo previsto para delinear y aplicar soluciones operativas contra la desinformación (Polyakova y Fried, 2019). La cronología del proceso de construcción de un marco de gobernanza en la UE refleja claramente la aceleración regulatoria que se impone a partir de 2018; primero, por los temores a una disrupción de contenido falso que pudiese alterar las elecciones al Parlamento Europeo de 2019 y, más tarde, por la constatación del creciente desequilibrio de derechos y oportunidades que genera el proceso de digitalización.

Desde 2018, la UE ha diversificado recursos y objetivos, y ha primado la coordinación con otros actores, desde las plataformas tecnológicas a las organizaciones de verificación. Todos los recursos empleados en esta línea, desde la creación del EDMO hasta el Código de Buenas Prácticas o el Plan de Acción para la Democracia Europea para fortalecer la resiliencia de los procesos electorales, son tácticas que acompañan, complementan y aligeran la respuesta reguladora comunitaria. Sin embargo, la intensificación y diversificación de medidas adoptadas hasta el presente demuestran que la capacidad de actuación de las instituciones europeas no incide de igual manera en todos los aspectos de la desinformación. Si tenemos en cuenta tanto el abordaje de Bontcheva y Posetti (2020) para la Unesco —que distingue entre los instigadores que están en el origen de la desinformación y los agentes encargados de distribuirla—, como el trabajo de Lewandowsky *et al.* (2020) para la UE —que especifica que cualquier intento de regulación debe tener en cuenta tanto a los actores, como el contenido desinformativo, las tácticas de diseminación y los efectos que causan—, vemos que las acciones de la UE se han centrado especialmente en el control del contenido y ahora intenta reforzar los límites a su capacidad de difusión.

Sin embargo, en el actual contexto, es difícil trazar el origen de los contenidos falsos que se diseminan de manera coordinada y automatizada. Los obstáculos para acotar el problema en origen son evidentes: primero, porque la producción o instigación de dichos contenidos puede iniciarse fuera del territorio comunitario; segundo, porque la libertad de expresión que protege el derecho a la libertad de información de los ciudadanos, ampara a los creadores y propulsores de mentiras.

En definitiva, la Ley de Servicios Digitales (DSA) y la Ley de Mercado Digital (DMA) son propuestas legislativas innovadoras, que reflejan las ambiciones de la UE de construir soberanía a través de la regulación de su espacio digital. Pero, además de desplegar una respuesta regulatoria a todas luces necesaria, Europa necesita ahondar en el fortalecimiento de las conexiones entre los distintos actores para atajar la desinformación sin dañar el derecho a la libertad de expresión, ni ser acusada de censora.

Referencias bibliográficas

- Álvaro, Sandra. «La esfera pública en la era de la hipermediación algorítmica: noticias falsas, desinformación y la mercantilización de la conducta». *Hipertext.net, Revista Académica sobre Documentación Digital y Comunicación Interactiva* n.º 17 (2018), p. 74-82.
- Arias Maldonado, Manuel. *La democracia sentimental. Política y emociones en el siglo XXI*. Barcelona: Página Indómita, 2016.
- Badillo, Ángel. «La sociedad de la desinformación: propaganda, «fake news» y la nueva geopolítica de la información». *Real Instituto Elcano*, Documento de trabajo, n.º 8 (2019) [Fecha de consulta: 14.02.2022] <https://www.realinstitutoelcano.org/documento-de-trabajo/la-sociedad-de-la-desinformacion-propaganda-fake-news-y-la-nueva-geopolitica-de-la-informacion/>
- Baricco, Alessandro. *The Game*. Barcelona: Anagrama, 2019.
- Bastos, Marco y Mercea, Dan. «The Brexit Botnet and User-generated Hyperpartisan News». *Social Science Computer Review*, vol. 37, n.º 1 (2019), p. 38-54.
- Bontcheva, Kalina y Posetti, Julie (eds.). «Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression». *UNESCO Broadband Commission Report*, (septiembre de 2020) (en línea) <https://en.unesco.org/publications/balanceact>
- Bradford, Anu. *The Brussels Effect: how the European Union rules the world*. Nueva York: Oxford University Press, 2020.
- Castells, Manuel. *The Rise of Network Society. The Information Age: Economy, Society and Culture* (vol.1). Cambridge, MA: Blackwell, 1996.
- Comisión Europea. «A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation». *UE Directorate-General for Communications Networks, Content and Technology*, (enero 2018a) (en línea) <https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en>
- Comisión Europea. «Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Action Plan against Disinformation », JOIN(2018) 36 final (diciembre 2018b).
- Comisión Europea. «DGx Proposed Priorities Paper». *Politico.eu*, (agosto de 2019) (en línea [Fecha de consulta: 15.08.2022] https://www.politico.eu/wp-content/uploads/2019/08/clean_definite2.pdf
- Comisión Europea. «Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan». COM (2020) 790 final (diciembre de 2020a).

- Comisión Europea. «Proposal for a Regulation of The European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC». COM/2020/825 final. (diciembre de 2020b)
- Confessore, Nicholas; Dance, Gabriel J. X.; Harris, Richard, y Hansen, Mark. «The Follower Factory». *The New York Times*, (27 de enero de 2018) (en línea) [Fecha de consulta: 18.02.2022] <https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html>
- Davenport, Thomas H. y Beck, John C. *La economía de la atención*. Barcelona: Paidós, 2002.
- Del Campo, Agustina. «Disinformation is not Simply a Content Moderation Issue». En: Feldstein, Steven (ed.). *Issues on the Frontlines of Technology and Politics*. Washington, DC: Carnegie Endowment for International Peace, 2021, p. 23-24.
- Flore, Massimo. «Understanding Citizens' vulnerabilities: from Disinformation to Hostile Narratives». *JRC Publications Repository*, (2020) (en línea) <http://dx.doi.org/10.2760/271224>
- García Morales, Verónica Yazmín. «Donde habitan las mentiras: libertades de expresión e información en tiempos de odio e hiperinformación». *Revista CIDOB d'Afers Internacionals*, n.º 124 (2020), p. 25-47.
- Graves, Lucas y Cherubini, Fererica. «The rise of Fact-Checking Sites in Europe». *Informe del Reuters Institute*, (2016) (en línea) <https://reutersinstitute.politics.ox.ac.uk/our-research/rise-fact-checking-sites-europe>
- Gstrein, Oskar J. y Zwitter Andrej J. «Extraterritorial application of the GDPR: promoting European values or power?». *Internet Policy Review*, vol. 10, n.º 3 (2021) (en línea) <https://doi.org/10.14763/2021.3.1576>
- Han, Byung-Chul. *Infocracia. La digitalización y la crisis de la democracia*. Barcelona: Penguin Random House, 2022.
- Harari, Yuval Noah. *21 Lecciones para el Siglo XXI*. Barcelona: Penguin Random House, 2018.
- Harrison, Ruairí. «Tackling Disinformation in Times of Crises: The European Commission's Response to the Covid-19 Infodemic and the Feasibility of a Consumer-centric solution». *Utrecht Law Review*, vol. 17, n.º 3 (2021), p.18-33.
- Hoffman, Stacie; Bradshaw, Samantha y Taylor Emily. «Networks and Geopolitics: How great power rivalries infected 5G». *Oxford Information Labs*, report, (22 de agosto de 2019) (en línea) <https://oxil.uk/publications/geopolitics-of-5g/>
- Innerarity, Daniel. *Una teoría de la democracia compleja. Gobernar en el siglo XXI*. Barcelona: Galaxia Gutenberg, 2020.
- IFCN-International Fact-Checking Network. «Verified signatories of the IFCN code of principles». *Poynter Institute*, (2019) (en línea) [Fecha de consulta:

- 14.02.2022] <https://ifcncodeofprinciples.poynter.org/signatories>
- Jourová, Vera. «Code of Conduct on countering illegal hate speech online: First results on implementation». *Factsheet Directorate-General for Justice and Consumers*, (diciembre de 2016) (en línea) [Fecha de consulta: 01.09.2022] http://www.sisumma.com/wp-content/uploads/2016/12/factsheet-code-conduct-8_40573.pdf
- Julibert, Joan. *El poder de la mentida*. Barcelona: Edicions Saldonar, 2018.
- Kakutani, Michiko. *La muerte de la verdad*. Barcelona: Galaxia Gutenberg, 2019.
- Keen, Andrew. *The Cult of the Amateur*. Nueva York: Doubleday/Currency, 2007.
- Kuczerawy, Aleksandra. «Fighting online disinformation: did the EU Code of Practice forget about freedom of expression?». En: Terzis, Gegios; Kloza, Darjusz; Kuźelewska, Elbieta y Trottier, Daniel (eds.). *Disinformation and Digital Media as a Challenge for Democracy*. Cambridge: Intersentia, 2019, p. 291-308.
- Lewandowsky, Stephan; Smillie, Laura; Garcia, David; Hertwig, Ralph; Weatherall, Jim; Egidy, Stefanie; Robertson, Ronald E.; O'connor, Caillin; Kozyreva, Anastasia; Lorenz-Spreen, Philipp; Blaschke, Yannic y Leiser, Mark. «Technology and Democracy: Understanding the influence of online technologies on political behaviour and decision-making, EUR 30422 EN». *JRC Publications Repository*, (2020) (en línea) <http://dx.doi.org/10.2760/709177>
- Lima, Cristiano. «A whistleblower power: Key takeaways from the Facebook papers». *The Washington Post*, (26 de octubre de 2021) (en línea) [Fecha de consulta: 30.08.2022] https://www.washingtonpost.com/technology/2021/10/25/what-are-the-facebook-papers/?utm_campaign=wp_main&utm_source=twitter&utm_medium=social
- Magallón Rosa, Raúl. «La (no) regulación de la desinformación en la Unión Europea. Una perspectiva comparada». *Revista de Derecho Político UNED*, n.º 106 (2019), p. 319-347.
- Monti, Matteo. «The EU Code of Practice on Disinformation and the Risk of the Privatisation of Censorship». En: Giusti, Serena y Piras, Elisa (eds.). *Democracy and Fake News*. Routledge, 2020, p. 214-225.
- Mueller, Robert S. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, DC: US Government Publishing Office, 2019 (en línea) [Fecha de consulta: 21.02.2022] <https://www.govinfo.gov/features/mueller-report>
- Müller, Philipp y Schulz, Anne. «Facebook or Fakebook? How users' perception of 'fake news' are related to their evaluation and verification of news on Facebook». *Studies in Communication and Media*, vol. 8, n.º 4 (2019), p. 547-559.

- Naciones Unidas. «UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms». UN Doc A/73/348 (29 de agosto de 2018).
- Newman, Abraham. *Protectors of Privacy: regulating personal data in the Global Economy*, Nueva York: Cornell University Press, 2008.
- Paul, Christopher y Matthews, Miriam. «The Russian “Firehose of Falsehood” Propaganda Model». *Rand Corporation*, (2016) (en línea) [Fecha de consulta: 8/02/2022] <https://www.rand.org/pubs/perspectives/PE198.html>
- Peirano, Marta. *El enemigo conoce el sistema: Manipulación de ideas, personas e influencias después de la economía de la atención*. Barcelona: Debate, 2019.
- Polyakova, Alina y Fried, Daniel. «Democratic Defense Against Disinformation 2.0». *Atlantic Center*, (13 de junio de 2019) (online) [Fecha de consulta: 18.02.2022] <https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation-2-0/>
- Sadin, Éric. *La silicolonisation du monde*. París: L’Échappée, 2016.
- Schaedel, Sydney. «Did the pope endorse Trump?». *FactCheck.org*, (24 de octubre de 2016) (en línea) [Fecha consulta: 17.02.2022] <https://www.factcheck.org/2016/10/did-the-pope-endorse-trump/>
- Seijas, Raquel. «Las soluciones europeas a la desinformación y su riesgo de impacto en los derechos fundamentales». *Revista de los Estudios de Derecho y Ciencia Política*, n.º 31 (2020), p. 1-14 (en línea) [Fecha de consulta: 13.02.2022] <https://doi.org/10.7238/idp.v0i31.3205>
- Snyder, Timothy. *El camino hacia la no libertad*. Barcelona: Galaxia Gutenberg, 2018.
- Stella, Massimo; Ferrara, Emilio y De Domenico, Manlio. «Bots increase exposure to negative and inflammatory content in online social systems». *Proceedings of the National Academy of Sciences*, vol. 115, n.º 49 (2018), p. 12.435-12.440 (en línea) <https://doi.org/10.1073/pnas.1803470115>
- Subramanian, Samanth. «Inside the Macedonian fake-news complex». *Wired*, (15 de febrero de 2017) (en línea) [Fecha de consulta: 17.02.2022] <https://www.wired.com/2017/02/veles-macedonia-fake-news/>
- Timberg, Craig; Dwoskin, Elizabeth y Albergotti, Reed. «Inside Facebook, Jan. 6 violence fueled anger, regret over missed warning signs». *Washington Post*, (22 de octubre de 2022) (en línea) [Fecha de consulta: 14.02.2022] <https://www.washingtonpost.com/technology/2021/10/22/jan-6-capitol-riot-facebook/>
- Van Alstyne, Marshall; Brynjolfsson, Erik. «Electronic Communities: Global Village or Cyberbalkans?». *Proceedings of the International Conference on In-*

- formation Systems*, (1997) (en línea) <https://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=3089CBAA3A27D3299F0854B4B3DB5E84?doi=10.1.1.72.3676&rep=rep1&type=pdf>
- Vosoughi, Soroush; Roy Deb y Aral, Sinan. «The spread of true and false news online». *Science*, vol. 359, n.º 6.380 (2018), p. 1.146-1.151.
- Wardle, Claire, y Derakhshan, Hossein. «Information Disorder: Toward an interdisciplinary framework for research and policy making». *Council of Europe report DGI*, n.º 09 (2017) (en línea) <https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html>
- Whitman, Richard (ed.). *Normative Power Europe: Empirical and Theoretical Perspectives*. Londres: Palgrave Macmillan, 2011.
- Williams, J. *Clics contra la humanidad. Libertad y resistencia en la era de la distracción tecnológica*. Barcelona: Gatopardo Ediciones, 2021.
- World Economic Forum. «The Global Risk Report 2021. 16th Edition». WEF, (2021) (online) [Fecha de consulta: 18.02.2022] <https://www.weforum.org/reports/the-global-risks-report-2021/>
- Zuboff, Shosana. *La era del capitalismo de la vigilancia*. Barcelona: Paidós, 2020.



Núm. 209
vol. XXXVI
15 €

POLÍTICA EXTERIOR

septiembre/octubre de 2022 • www.politicaexterior.com



HISTORIA

A vueltas con el pasado

Margaret MacMillan | Lynn Hunt | Kristina Spohr | Antonio Muñoz Molina



9 788488 025623



9 770213 685004

00209