III.
DERECHO PÚBLICO EUROPEO

EL REGLAMENTO EUROPEO DE SERVICIOS DIGITALES Y LA DEFENSA DE LA DEMOCRACIA

ÁNGEL BARREDO ARTIGUEZ

SUMARIO

Fecha recepción: 29.06.2024
Fecha aceptación: 17.12.2024

EL REGLAMENTO EUROPEO DE SERVICIOS DIGITALES Y LA DEFENSA DE LA DEMOCRACIA

ÁNGEL BARREDO ARTIGUEZ[1]

Investigador predoctoral en la Universidad del País Vasco UPV/EHU

I. INTRODUCCIÓN

La salvaguarda de unas elecciones democráticas no se reduce sólo al correcto escrutinio de los votos o a la garantía de un uso adecuado de los espacios públicos por parte de los candidatos. Las compañías digitales desempeñan un papel fundamental en las elecciones y durante el desarrollo de las campañas electorales. Las plataformas de redes sociales se han convertido en espacios centrales para los procesos democráticos y, en muchos casos, han sustituido a los medios de comunicación tradicionales. Muchos políticos comunican sus mensajes principalmente a través de sus perfiles en redes y, en ese sentido, pueden ser utilizadas como unas herramientas valiosas, pero también albergan potenciales riesgos que pueden vulnerar el derecho a unas elecciones libres y justas.

Consciente de esta delicada situación, el nuevo Reglamento de Servicios Digitales de la Unión Europea pretende actualizar el marco jurídico que regula la actuación de las compañías que prestan servicios intermediarios en línea para hacer frente a los nuevos retos que presentan su diseño y funcionamiento. Para ello, se establecen una serie de potenciales riesgos sistémicos que las grandes compañías deberán tener en cuenta a la hora de diseñar sus servicios. Uno de estos riesgos se refiere a los efectos negativos que puedan tener sobre el discurso cívico, los procesos electorales y la seguridad pública. Por ello, se hace necesaria una delimitación

[1] Este artículo es una extensión de una comunicación presentada en el Congreso de la Asociación de Constitucionalistas de España, celebrado en Valladolid los días 7 y 8 de marzo de 2024. Se trata de un trabajo que se enmarca dentro de las labores realizadas por el grupo de Investigación IT-1663-22 financiado por el Gobierno Vasco. Correo electrónico: angel.barredo@ehu.eus. Investigador predoctoral en la Universidad del País Vasco UPV/EHU, Facultad de Ciencias Sociales y de la Comunicación, Barrio de Sarriena, s/n, 48940, Leioa, Bizkaia. código orcid: https://orcid.org/0009-0008-3445-500X.

de dichos términos que permita identificar los riesgos asociados a cada uno y las posibles medidas de atenuación.

II. EL REGLAMENTO DE SERVICIOS DIGITALES

El objetivo del Reglamento (UE) 2022/2065 relativo a un mercado único de servicios digitales — Reglamento de Servicios Digitales o DSA por sus siglas en inglés— es contribuir al correcto funcionamiento del mercado interior de servicios intermediarios estableciendo normas armonizadas aplicables en todos los Estados miembros. Para ello, pretende crear un entorno en línea seguro, predecible y fiable abordando la difusión de contenidos ilícitos, y los riesgos que para la sociedad pueda generar la difusión de desinformación y demás contenidos. Todo ello, además, tratando de facilitar la innovación y protegiendo efectivamente los derechos fundamentales amparados por la Carta[2]. A lo largo del articulado del texto puede comprobarse cómo se intentan conjugar dos elementos que, en ocasiones, y sobre todo en el ámbito digital, suelen encontrarse enfrentados.

Por un lado, se intenta asegurar un espacio suficiente a la innovación, tratando que la regulación no implique el establecimiento de barreras excesivas que puedan lastrar el progreso en el entorno en línea. Se trata de una preocupación legítima por parte de las instituciones de la Unión que, conscientes de la importancia de tener un sector tecnológico lo suficientemente desarrollado, no quieren arriesgarse a que éste pueda verse obstaculizado por una excesiva regulación que desincentive la innovación. Algo que dejaría a Europa muy por detrás de los avances que puedan darse en Estados Unidos o en China — los dos grandes competidores en materia digital a los que se enfrenta la UE—.

Por otro lado, se trata de proteger los derechos que están reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea y que pueden quedar amenazados en un entorno en línea salvaje y carente de cualquier tipo de regulación[3]. Pues como se comprobará, no son pocos los casos que atestiguan el inmenso poder con el que cuentan las compañías digitales, y la capacidad que tienen a la hora de vulnerar los derechos más elementales de sus usuarios, así como de condicionar el correcto desarrollo de los procesos democráticos.

El objeto de la regulación de este nuevo reglamento son los conocidos como "servicios intermediarios", que vienen siendo prestados por dos tipos de compañías:

[2] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). Considerando (9). https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81573

[3] Francesc Bracero "La UE mete en cintura el 'salvaje oeste' digital". La Vanguardia. 20/01/2022. Fecha de consulta 13/02/2024. https://www.lavanguardia.com/tecnologia/20220120/8001480/ley-servicios-digitales-google-facebook-internet.html

(1) Las plataformas en línea: que prestan un servicio de alojamiento de datos, y que, a petición de un destinatario del servicio, almacena y difunde información al público, y (2) los motores de búsqueda en línea cuyas interfaces permite a los usuarios introducir consultas para hacer búsquedas de, en principio, todos los sitios web[4]. De ahora en adelante me referiré a ambos tipos indiferentemente como "compañías digitales" o "grandes plataformas" salvo en los supuestos en los que necesariamente deban diferenciarse.

Los últimos años del siglo veinte trajeron consigo el desarrollo exponencial de internet y el nacimiento de las primeras compañías digitales. Se trataba de un sector prometedor que no había desplegado aún todo su potencial y la sociedad carecía de información suficiente para prever los riesgos asociados a la acumulación de poder por parte de estas compañías. Unas multinacionales que, además, actuaban en un mundo cada vez más globalizado en el que la ruptura del nexo Estado-nación-mercado[5] abría la puerta a un espacio económico determinado por una mano invisible global transformando el alcance del concepto clásico de soberanía estatal[6], y reduciendo el espacio de la política a su mínima expresión[7]. En ese contexto, las democracias constitucionales de ambas orillas del Atlántico —Estados Unidos y la Unión Europea—, adoptaron una posición liberal de intervención mínima, autolimitando su capacidad regulatoria a la vez que eximían a los servicios intermediarios que se estaban creando de toda responsabilidad. Una posición que reflejaba tanto las insuficiencias regulatorias de las últimas décadas del pasado siglo, como el inicial "ciberoptimismo" hacia las potencialidades de la nueva sociedad digital de la información[8].

La regulación europea existente hasta la aprobación de la DSA venía contenida en la Directiva 2000/31/CE sobre Comercio Electrónico en cuya sección 4ª —artículos 12 a 15— se establecía un ínfimo régimen de responsabilidad por el cual se hacía extremadamente difícil responsabilizar a las compañías de servicios intermediarios

[4] Para una definición más exhaustiva de los prestadores de dichos servicios y del tipo de servicio en línea véase el artículo 3 DSA.

[5] TAJADURA TEJADA, J. (2004). "¿El ocaso de Westfalia? Reflexiones en torno a la crisis del constitucionalismo en el contexto de la mundialización". *Revista de Estudios Políticos* (nueva época), nº 123, enero-marzo. pp. 323-324. En la misma línea

[6] La crisis de la soberanía estatal en sus dos dimensiones –interna y externa– como consecuencia de la globalización, ha sido puesta de manifiesto en; TORRES DEL MORAL, A. (2012) "Del Estado absoluto al supranacional e internacionalmente integrado". *Revista de Derecho Constitucional Europeo*. Año 9. Nº 18. Julio-diciembre. pp. 27 y 28; y DE VERGOTTINI, G. (2015) "La persistente soberanía". *Teoría y Realidad Constitucional.* UNED. N.º 36. pp. 81 y 82.

[7] Sobre la reducción del espacio de la política y las relaciones entre el mercado cosmopolita y el Estado; DE VEGA GARCÍA, P. (1998) "Mundialización y Derecho Constitucional: La crisis del principio democrático en el constitucionalismo actual". *Revista de Estudios Políticos* (Nueva Época), nº 100. Abril-junio. pp 15 a 17.

[8] DE GREGORIO, G. (2022). "Digital Constitutionalism across the Atlantic". *Global Constitutionalism,* nº 11 (2). p. 301.

por el contenido compartido por sus usuarios[9]. Es decir, en la mayoría de los casos, las plataformas, consideradas como meras intermediarias, no podían ser demandadas por los usos indebidos o actividades ilícitas que llevasen a cabo sus usuarios —por ejemplo, difusión de discursos de odio o venta de productos ilegales—. Se trataba de un marco regulador que, en líneas generales, venía a reflejar la normativa federal estadounidense contenida en la Sección 230 de la Ley de Decencia de las Comunicaciones de 1996[10]. Una regulación que, centrada en los discursos difamatorios y su posible censura por las propias compañías, intentaba conseguir un equilibrio entre la decencia que debía regir las comunicaciones en línea y el derecho constitucional a la libertad de expresión[11].

La DSA tratará de actualizar el marco jurídico que establecía la directiva europea en la medida en que los servicios de la sociedad de la información, y especialmente los servicios intermediarios, han cambiado sustancialmente en estas dos últimas décadas. Las compañías que operan en la red funcionan mediante el procesamiento de ingentes cantidades de datos de diversa índole —que van desde el mero uso que se hace del dispositivo, hasta conocer los gustos e inquietudes personales—, y que, al ponerlos en relación, obtienen información con valor añadido. Esta técnica o práctica de recopilación y manejo de datos es conocida como *Big Data* o "macrodatos"[12]. Como reconoce González de la Garza, se trata de un instrumento técnico que confiere a su poseedor un poder absoluto, anónimo y constante que permite penetrar en lo más recóndito de la intimidad de los usuarios y averiguar todo sobre ellos sin que éstos sean siquiera conscientes de ello. Una facultad con la que no hubieran podido ni soñar los regímenes más autoritarios del pasado siglo[13].

---

[9] Directiva 2000/31/CE, de 8 de junio de 2000, (Directiva sobre el comercio electrónico). https://www.boe.es/buscar/doc.php?id=DOUE-L-2000-81295

[10] Para una exposición de las ventajas y beneficios de dicha regulación –y sobre los posibles riesgos– en la conformación y desarrollo de un Internet libre: KOSSEFF, F. (2019) *The Twenty-Six Words That Created The Internet*. Cornell University Press. pp. 207 y ss.

[11] La disposición norteamericana tenía como objetivo principal armonizar las contradictorias respuestas jurisprudenciales que se estaban dando en los casos de responsabilidad por difamaciones en internet, y que trataban de subsumir a los prestadores de servicios en línea en alguna de las categorías clásicas conformadas en los casos relativos a la libertad de expresión –editores, distribuidores o meros transportistas–, pero sin mucho éxito. EHRLICH P. (2002). "Communication Decency Act §230". *Berkeley Technology Law Journal,* Vol. 17. pp. 403-406.

[12] "El Big Data supone la obtención y análisis constante de ingentes cantidades de datos, incluidos personales, que provienen de diferentes fuentes y que son objeto de un tratamiento automatizado por parte de avanzadas técnicas computacionales y algoritmos matemáticos" MARTÍN JIMÉNEZ, F.J. (2024). "Big Data: Riesgos y soluciones desde el Derecho y desde los principios". *Revista de Derecho Político,* nº 119, enero-abril, p. 219.

[13] GONZÁLEZ DE LA GARZA, L.M. (2018). "La crisis de la democracia representativa. Nuevas relaciones políticas entre democracia, populismo virtual, poderes privados y tecnocracia en la era de la propaganda electoral cognitiva virtual, el *microtargeting* y el *big data*". *Revista de Derecho Político,* nº 103, septiembre-diciembre, pp. 272-273.

Sonados casos como el de Cambridge Analytica[14] en 2016 concretizaron un temor que venía advirtiéndose años antes: los riesgos que para el Estado de Derecho y la democracia podían suponer determinados actores privados[15]. En la medida en que estas compañías regulan el comportamiento y las decisiones de sus usuarios en el proceso comunicativo en línea, pueden ser situadas dentro de la categoría de "poderes privados"[16]. Un hecho que demuestra no sólo su capacidad para vulnerar derechos fundamentales sino también la necesidad de revisar una regulación que se ha tornado insuficiente, y que debe redirigirse hacia una mayor responsabilidad de las plataformas[17]. Por ello, desde la aprobación en 2016 del Reglamento general de protección de datos[18], hasta la reciente normativa en materia de mercados digitales (DMA)[19], la propia DSA y el Reglamento de Inteligencia Artificial[20], puede hablarse de un cambio regulatorio en la Unión Europea tendente a establecer un mayor control sobre las compañías que prestan servicios intermediarios en línea para proteger los valores democráticos sobre los que se asienta el entramado comunitario y los sistemas constitucionales de los Estados miembros.

III. LAS GRANDES COMPAÑÍAS DIGITALES Y LOS RIESGOS SISTÉMICOS

En los últimos años han surgido una serie de compañías digitales de muy gran tamaño que actúan como espacios semipúblicos para el intercambio de información y para el comercio en línea que plantean riesgos especiales desde el punto de vista de los derechos de los usuarios. La DSA realiza una diferenciación en el régimen de responsabilidad de las compañías diferenciándolas en dos grupos; por un lado, las compañías en general y por otro, las plataformas en línea y motores de búsqueda de muy gran tamaño — aquellas cuyo número de destinatarios activos exceda de 45 millones de usuarios, o del 10% de la población de la Unión[21]—.

---

[14] BBC MUNDO. Redacción. 20 de marzo de 2018. Actualizado el 17 de febrero de 2018. https://www.bbc.com/mundo/noticias-43472797. Fecha de consulta: 27 de septiembre de 2023.

[15] Informe sobre el Estado de Derecho adoptado por la Comisión de Venecia en su 86ª sesión plenaria (25-26 de marzo de 2011), p. 18. https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2011)003rev-spa.

[16] VILLAVERDE MENÉNDEZ, I. (2020) *Los poderes salvajes: ciberespacio y responsabilidad por contenidos difamatorios.* Madrid. Marcial Pons. Pp. 39 y 40.

[17] CORREDOIRA, L. (2024) "Democracia y desinformación. Respuestas regulatorias de la Unión Europea para el fortalecimiento de la democracia y cambios de rumbo del paquete de servicios digitales" en SERRANO MAÍLLO, I y CORREDOIRA, L. (eds.) *Democracia y desinformación: nuevas formas de polarización, discursos de odio y campañas en redes. Respuestas regulatorias de Europa y América Latina.* Madrid. Dykinson. pp. 272 y ss.

[18] Reglamento (UE) 2016/679, de 27 de abril de 2016, (Reglamento de Protección de Datos).

[19] Reglamento (UE) 2022/, de 14 de septiembre de 2022, (Reglamento de Mercados Digitales).

[20] Reglamento (UE) 2024/1689, de 13 de junio de 2024, (Reglamento de Inteligencia Artificial).

[21] Artículo 33 DSA. Puede consultarse la lista de las compañías designadas como "plataformas en línea y motores de búsqueda de muy gran tamaño", así como la información sobre los primeros

Este segundo grupo de compañías está obligado a la observancia de las disposiciones de carácter general aplicables a todos los prestadores de servicios intermediarios en línea, además de a otras específicas como, por ejemplo, el sometimiento anual a auditorías independientes o al abono de una tasa de supervisión[22]. No obstante, la DSA deja meridianamente claro en su artículo 8 — en la misma línea que el artículo 15.1 de la Directiva del 2000— que no se establece una obligación general de supervisión ni de colaboración que implique que las compañías deban realizar una búsqueda activa de posibles actividades ilícitas y la identificación de aquellos que las llevan a cabo. Una matización del todo fundamental, que como se comprobará, reduce el régimen de responsabilidad a la comprobación de que sus diseños no promuevan e incrementen los denominados como "riesgos sistémicos". Por lo tanto, en lo relativo a posibles contenidos ilegales e infracciones que sus usuarios puedan cometer frente a terceros, las compañías de servicios intermediarios mantienen la exención de responsabilidad o inmunidad, sujeta a ciertos condicionamientos, que establecía la regulación anterior[23].

La obligación de mayor importancia a la que quedan sometidas es a "la detección, análisis y evaluación con diligencia de cualquier riesgo sistémico en la Unión que se derive del diseño o del funcionamiento de su servicio y los sistemas relacionados con este, incluidos los sistemas algorítmicos, o del uso que se haga de sus servicios"[24].

Las compañías digitales de muy gran tamaño pueden influir en gran medida en la seguridad en línea, en la opinión y el discurso públicos, así como en el comercio en línea. Sus interfaces se diseñan con el objetivo de favorecer a sus modelos de negocio, basados en la obtención de beneficios mediante la publicidad[25], y pueden causar inquietud en la sociedad en su conjunto. Por ello, según reconoce el legislador comunitario, resulta necesaria una regulación que sea capaz de detectar y reducir de manera eficaz los riesgos y los perjuicios sociales que puedan generar.

A la hora de calificar los riesgos como "sistémicos" el Reglamento tuvo en cuenta la posición de intermediación en los flujos de información que ocupan estas compañías y el rol que juegan en la amplificación y conformación de la opinión y discurso públicos. Para ello, la evaluación se debe centrar en la escala que este tipo de riesgos pueden llegar a alcanzar, y en la posibilidad de extenderse más allá de los usuarios de sus servicios. Por tanto, un riesgo será considerado como sistémico cuando pueda perjudicar a individuos a gran escala o a sistemas esenciales para la gobernanza y el

procedimientos abiertos contra TikTok, Meta, X y AliExpress por posibles violaciones de las disposiciones de la DSA, en el siguiente enlace: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses. Última consulta noviembre de 2024.

[22] Artículos 37 y 43 DSA respectivamente.

[23] BARRERO ORTEGA, A. (2021). "Responsabilidad de los intermediarios de internet en el derecho de la UE". *Revista Española de Derecho Constitucional,* nº 123, pp. 116 y ss.

[24] Artículo 34 DSA.

[25] BALAGUER CALLEJÓN, F. (2022). *La Constitución del algoritmo*, Zaragoza, Fundación Manuel Giménez Abad. p. 72.

buen funcionamiento de la sociedad. Para lo cual, la cantidad de usuarios sirve como indicador tanto del número de personas que podrían verse afectadas por algún daño, como del potencial impacto sobre los sistemas públicos necesarios para el buen funcionamiento de la sociedad y la economía[26].

Cuando un riesgo sea considerado como sistémico podrá pertenecer a una de estas dos categorías[27]:

1. Riesgos que tienen un amplio impacto en los sistemas: Cuando el contenido y la conducta se da en varios servicios digitales; cuando los riesgos afectan a una serie de derechos fundamentales interdependientes, ya sea por el tamaño e impacto de un proveedor de servicios digitales, o por la importancia de la actividad que desarrolla el operador en concreto.
2. Riesgos que son causados o exacerbados por los sistemas: El riesgo puede aparecer, por ejemplo, porque la estructura o el sistema expone a un gran número de usuarios a cierto contenido sin que éstos lo demanden intencionadamente. También pueden ser riesgos colaterales que aparecen cuando se ponen en funcionamiento otras medidas de control como, por ejemplo, el caso de los sistemas de moderación de contenidos de las propias plataformas que, en muchas ocasiones, vulneran el derecho a la libertad de expresión.

De esta forma, la DSA impone a las compañías digitales de muy gran tamaño la obligación de evaluar los riesgos sistémicos que entraña el diseño, funcionamiento y uso de sus servicios, así como los posibles usos indebidos que lleven a cabo los usuarios de estos servicios[28]. Para ello, deberán adoptar las medidas de reducción de riesgos que resulten más adecuadas y respetuosas con los derechos fundamentales[29]. En este sentido, el Reglamento prevé la existencia de cuatro categorías de riesgos sistémicos relacionados con: (a) la difusión de contenidos ilícitos, (b) efectos sobre el ejercicio de los derechos fundamentales, (c) discurso cívico, procesos electorales y seguridad pública, y d) salud pública, menores y violencia de género[30]:

[26] MICOVA, S. y CALEF, A. (2023). "Elements for Effective Systemic Risk Assessment under the DSA". *Center on Regulation in Europe (CERRE).* Report. July. pp. 13-15.

[27] PIELEMEIER, J. y SULLIVAN, D. (2023). "Implementing risk assessments under the Digital Service Act". *Digital Trust and Safety Partnership,* Discussion Summary. Junio. p. 4

[28] Deberán realizar informes propios y someterse a auditorias independientes. Los primeros informes publicados durante el primer año de vigencia del Reglamento pueden consultarse en el siguiente enlace: https://digital-strategy.ec.europa.eu/en/policies/dsa-brings-transparency

[29] Considerando (79) DSA.

[30] Considerandos (80 a 83) y artículo 34.1 DSA.

IV. LA DEFENSA DE LA DEMOCRACIA

Como se acaba de comprobar, el artículo 34 reproduce los riesgos sistémicos enumerados en los considerandos, y su apartado primero, letra (c) establece como riesgo sistémico "los efectos reales o negativos sobre el discurso cívico y los procesos electorales, así como sobre la seguridad pública". Una regulación que puede traducirse como una obligación que se les impone a las grandes compañías tecnológicas para proteger la integridad de los sistemas democráticos de los Estados miembros. Para ello, se toma en consideración como presupuestos básicos de un correcto funcionamiento democrático: un *discurso cívico* respetuoso y auténtico, un *proceso electoral* garantista y libre, y un sistema que asegure la *seguridad pública*. Siendo la democracia uno de los valores fundamentales de la Unión Europea[31], el destacado interés por su efectiva protección se encuentra más que justificado.

Por ello, los siguientes apartados se centrarán en delimitar los términos "discurso cívico", "proceso electoral" y "seguridad pública", para tratar de identificar algunos de los potenciales riesgos a los que se enfrenta cada uno de ellos en el entorno digital.

A) la protección del discurso cívico

El Reglamento busca proteger el discurso cívico tratando de conformar un espacio en línea donde personas autónomas que aspiren a informarse y formarse ideas, así como compartir sus conocimientos y opiniones puedan hacerlo con todas las garantías y el respeto suficiente. En consecuencia, el discurso cívico es entendido como un método a través del cual grupos de personas contribuyen, mediante su libertad de expresión y opinión, a conformar un discurso público plural y respetuoso, un espacio necesario y fundamental en cualquier régimen democrático que se precie[32].

Para la existencia de una democracia funcional es fundamental que la gente hable entre sí y comparta sus ideas sobre política y asuntos públicos. Participar en discusiones públicas de carácter político ayuda a las personas a adquirir conocimientos, les permite enseñar o difundir información a otras y puede ser tan importante para la comprensión de las noticias como la propia exposición a éstas. El debate político también informa a la gente sobre las formas de participar e influye en su elección de

[31] Tratado de la Unión Europea. C 83/13. Diario Oficial de la Unión Europea. En cuyo artículo dos se establece que "La Unión se fundamenta en los valores de respeto de la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a minoría…"

[32] CALABRESE, S. y REICH, O. (2024). "Identifying, Analyzing, Assessing and Mitigating potential negative effects on civic discourse and electoral processes: a minimum menu of risks very large online platforms should take heed of". *European Partnership for Democracy*, January. P. 12. En este interesante informe los autores presentan ciertos riesgos tomando en consideración los que consideran como requisitos de un discurso adecuado.

voto. Debatir sobre política o actualidad, y los desacuerdos inherentes a este intercambio son partes esenciales de cualquier democracia[33].

Los espacios para que los ciudadanos se relacionen entre sí y se produzcan esos intercambios de opinión y discusiones públicas son fundamentales, y en la actualidad, las plataformas en línea tienen la oportunidad de ofrecer estos espacios. La naturaleza única de Internet, unida a los fenómenos psicológicos y de comunicación que afectan a los usuarios en línea, influyen enormemente en la calidad de las interacciones que se dan en estas plataformas. El anonimato, la desinhibición y la adopción de costumbres antisociales pueden hacer que el discurso en línea carezca de civismo. Sin embargo, las investigaciones que se están desarrollando en la actualidad parecen indicar que el diseño estratégico de las plataformas y sus sistemas de funcionamiento pueden allanar el camino hacia un diálogo más cívico[34]. No obstante, las plataformas parecen optar por opciones de diseño menos honestas y comprometidas con dichos valores[35].

El civismo siempre ha sido considerado un requisito para el discurso democrático y ha venido siendo definido frecuentemente como una suerte de educación y cortesía general, un "comportamiento respetuoso del ciudadano con las normas de convivencia pública"[36], una cualidad que se valora como un indicador positivo para el correcto funcionamiento de una sociedad. Las conversaciones sobre el significado de ciudadanía, democracia y discurso público resaltan como virtud esencial el civismo, cuya falta conlleva implicaciones perjudiciales para un sistema democrático[37].

1. Amenazas para un discurso abierto y plural

Los principales riesgos que se pueden dar en cuanto a la accesibilidad e inclusividad del discurso derivan de la posibilidad de que, las plataformas, en su condición de empresas privadas —y, por lo tanto, propietarias del servicio— decidan no permitir el acceso a sus interfaces a algún usuario o grupo concreto. Se trata de la posición conocida como *"gatekeeper"* o guardianes, que tradicionalmente la doctrina ha venido a distinguir en dos grandes tipos: los que controlan el acceso a la información, y los

[33] LEAVITT, P. y PEACOCK, C. (2014). "Civility, Engagement, and Online Discourse: a Review of Literature". *National Institute for Civic Discourse*, The University of Arizona. August 4. p. 1

[34] LEAVITT, P. y PEACOCK, C. (2014). Op. cit. p. 6.

[35] Frances Haugen, exempleada del gigante tecnológico Facebook –ahora Meta–, sorprendió al mundo cuando en 2021 reconoció ante el Senado estadounidense que la compañía había decidido intencionadamente implantar un sistema algorítmico que primaba los intereses comerciales sobre la salud y seguridad públicas. Una decisión que, si bien podía haber sido del todo diferente, terminó por dar como resultado un sistema que exacerbaba la división, el extremismo y la polarización, afectado gravemente a la salud mental de los jóvenes y al correcto funcionamiento de la democracia norteamericana. Statement of Frances Haugen October 4, 2021. Disponible en línea: https://www.commerce.senate.gov/services/files/FC8A558E-824E-4914-BEDB-3A7B1190BD49.

[36] "Civismo", Diccionario de la Real Academia de la Lengua Española.

[37] PAPACHARISSI, Z. (2004). "Democracy online: Civility, Politeness, and the Democratic Potential of Online Discussion Groups". *New Media and Society,* Vol 6(2). p. 260

que tienen un papel facilitador mediante el control de los servicios intermediarios que son necesarios para vincular a los usuarios con el contenido, para mediar entre los diferentes actores de la cadena de información, o para producir, transportar y distribuir contenidos[38]. Por ejemplo, una red social mantiene un control sobre el acceso que los anunciantes en línea tienen a sus usuarios, de igual manera que un motor de búsqueda controla el acceso de los usuarios a contenidos web mediante el uso de una clasificación algorítmica que prioriza unos contenidos sobre otros.

Se trata de sujetos que tienen una posición privilegiada para dirigir el acceso de los usuarios a servicios o aplicaciones concretas, al mismo tiempo que tienen la posibilidad de aprovecharse de esos mismos clientes para, con los datos que estos originan con el uso de las aplicaciones, ofrecer a las empresas anunciadoras en línea un servicio cada vez más variado y sofisticado[39].

Con ello, se constata la falsedad de la idea que sostiene que las redes sociales son espacios donde los usuarios interactúan libremente y en los que la plataforma se limita a una mera intermediación tecnológicamente neutral. Existen decisiones de diseño que condicionan toda la actividad que se desarrolla, además del uso de algoritmos cuya influencia en el proceso comunicativo resulta decisiva para determinar el contenido que acaban consumiendo los usuarios[40].

Una de las técnicas de mayor incidencia para una participación libre la constituye la conocida como "exclusión oculta". Se trata de una actividad que viene expresamente reconocida en la DSA[41] y que se refiere a un tipo engañoso de exclusión de perfiles en foros web por el cual el usuario mantiene la impresión de que aún puede publicar, a pesar de que realmente su contenido ya no es visible para el resto de usuarios[42]. El término también abarca otro tipo de vetos que no se comunican al usuario como la exclusión de listas de difusión o la no promoción intencionada de contenido[43]. Se trata de una actividad de censura encubierta que puede generar consecuencias negativas en el ámbito del discurso. En la misma línea, la propia plataforma puede ejercer activamente una desproporcionada curación algorítmica o moderación de contenidos,

[38] HELBERGER, N., KLEINEN-VON KÖNIGSLÖW, K., y VAN DER NOLL, R. (2015). "Regulating the New Information Intermediaries as Gatekeepers of Information Diversity". *Info,* VOL. 17, Nº6. p. 52. Disponible en línea: https://www.ivir.nl/publicaties/download/1618.pdf.

[39] ALEXIADIS, P. y DE STREEL, A. (2020). "Designing an EU Intervention Standard for Digital Platforms". *EUI Working Paper RSCAS 2020/14.* Robert Schuman Centre for Advanced Studies, Florence School of Regulation. European University Institute. Disponible en línea: https://cadmus.eui.eu/handle/1814/66307. p. 5.

[40] TERUEL LOZANO, G. (2023). "Libertad de expresión, censura y pluralismo en las redes sociales: algoritmos y el nuevo paradigma regulatorio europeo", en BALAGUER CALLEJÓN, F., y COTINO HUESO, L. (Coord.), *Derecho Público de la Inteligencia artificial*. Zaragoza. Fundación Giménez Abad. pp. 186-187

[41] Considerando (55) DSA.

[42] Para conocer sus posibles incidencias en el compromiso cívico: CALABRESE, S. y REICH, O. (2024). Op. Cit. pp. 27-28.

[43] LEERSSEN, P. (2023). "An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation". *Computer Law and Security Review,* Vol. 48. Abril. p. 2.

que efectivamente suponga una actividad censora privada[44]. Medidas que pueden degradar o silenciar por completo determinadas voces y que se alejan del inicial ideal democrático y participativo que parecían prometer este tipo de compañías digitales —sobre todo las redes sociales— durante los primeros años desde su nacimiento.

Otra de las amenazas para la pluralidad del discurso en línea se deriva de la capacidad que tienen las plataformas de generar, de manera consciente y deliberada, espacios de autoafirmación y exclusión que "refuerzan las posiciones particulares cerrando cualquier compromiso con lo diferente"[45]. Conocidas por la doctrina como "*eco chambers"* o cámaras de eco, pueden conducir a la fragmentación del discurso público al dividir a los "sectores sociales en auténticas burbujas que desconocen y niegan la verdad de los otros, en un proceso continuo de reafirmación de las propias convicciones"[46], pero cuya efectiva influencia en el discurso es debatida[47].

2. Amenazas para un discurso centrado en la verdad

El uso de información alejada de la realidad no es un fenómeno nuevo, pero si se ha visto ampliamente acrecentado en la nueva esfera de comunicación digital. Un espacio comunicativo horizontal donde los usuarios pueden ser al mismo tiempo consumidores y generadores de información. Entre este contenido destacan las "*fake news"* o noticias falsas y la *posverdad*[48] en las que los elementos subjetivos personales y las emociones, desplazan a los hechos objetivos y los hechos comprobados, para la formación de la

[44] Sobre la censura privada de las compañías digitales y jurisprudencia norteamericana: VÁZQUEZ ALONSO, V.(2020) "Twitter no es un foro público pero el perfil de Trump sí lo es. Sobre la censura privada *de* y *en* las plataformas digitales en los EE.UU." *Estudios de Deusto.* Vol. 68/1. Enero-junio.pp. 475-508. Un debate en torno al establecimiento de una mayor responsabilidad de los intermediarios por el contenido de terceros y la supuesta "censura previa vicarial" que ello puede implicar puede encontrarse en VILLAVERDE MENÉNDEZ, I. (2020). Op. Cit. pp. 96 y ss.

[45] COTINO HUESO, L. (2013) "La selección y personalización de noticias por el usuario de nuevas tecnologías" en CORREDOIRA, L. y COTINO HUESO, L (dirs.), *Libertad de expresión e información en Internet: amenazas y protección de los derechos fundamentales.* Madrid. Centro de Estudios Políticos y Constitucionales. p. 46.

[46] BALAGUER CALLEJÓN, F (2022). Op. Cit. p. 77.

[47] BARBERÁ, P. (2020). "Social Media, Echo Chambers, and Political Polarization", en PERSILY, N and TUCKER, J.A. *Social Media and Democracy.* Cambridge University Press. pp 34 a 55. El autor afirma que los usuarios de redes sociales no tienen una capacidad absoluta para decidir los contenidos que consumen ya que se encuentran expuestos a contenidos que aparecen de manera accidental y que mucho del contenido que aparece es compartido por los que él denomina "enlaces frágiles" – antiguos conocidos, compañeros de trabajo, etc.– lo que se traduce, necesariamente, en una exposición a contenido ideológicamente diverso.

[48] Tras realizar un análisis sobre la "verdad", Rubio Núñez considera la "posverdad" como la suma de un contenido falso o engañoso, y su distribución masiva a través de canales tecnológicos y sus consecuencias. RUBIO NÚÑEZ, R. (2018). "Los efectos de la posverdad en la democracia". *Revista de Derecho Político.* UNED. N.º 103. Septiembre-diciembre. p. 203.

opinión pública y la toma de decisiones[49]. Se trata de un contenido que formalmente imita a las noticias emitidas por los medios tradicionales pero cuyos creadores —individuos u organizaciones— carecen de los sistemas editoriales necesarios para garantizar su exactitud y veracidad y que, junto a la desinformación, tienen como finalidad engañar a la gente[50]. Las noticias falsas alcanzan a un mayor número de usuarios que aquellas que ofrecen una información veraz, y de todas las categorías de noticias falsas, las de contenido político mantienen una dinámica de difusión mucho más acelerada que el resto, haciéndose más virales y llegando a mucha más gente[51].

Si bien es cierto que el cambio tecnológico ha propiciado un acceso y democratización de la información sin precedentes en la historia, también lo es la cada vez mayor dificultad para comprobar la autenticidad de las noticias y contenidos vertidos en la red. La generación de estas noticias totalmente alejadas de la verdad pone de manifiesto la erosión del ideal de compromiso con los hechos reales y el discurso informado que debería contribuir a la formación de la opinión pública y servir como mecanismo de control democrático[52]. Una situación que ha puesto de relieve la imperante necesidad de promover una educación o "alfabetización mediática que permita a las nuevas generaciones saber decodificar lo que leen"[53] e intentar, en la medida de lo posible, distinguir entre lo que es verdad y lo que no.

B) La protección de los procesos electorales

En un sistema democrático, la esencia del proceso electoral consiste en que los ciudadanos puedan expresar su voluntad política mediante la participación libre y efectiva en unas elecciones que les permita la elección de sus representantes. Dicha participación queda formalmente regulada por medio de un conjunto de normas e instituciones que conforman el sistema electoral. El papel que juegan estas reglas es facilitar y posibilitar la participación, así como limitarla y condicionarla a la observancia de una serie de principios y garantías que se consideran indispensables en un régimen constitucional[54]. No obstante, y a pesar de tratar de configurarse como un sistema que posibilite la mayor y más fiel representación de la voluntad popular, con frecuencia dichas reglas aumentan la influencia de ciertos grupos, mientras debilitan

[49] SERRA CRISTÓBAL, R. (2021) "De falsedades, mentiras y otras técnicas que faltan a la verdad para influir en la opinión pública". *Teoría y Realidad* Constitucional, núm.47. pp. 203-204.

[50] LAZER, M.J.D *et al.,* (2018). "The Science of Fake News". *Science,* 359, p. 1094

[51] VOSOUGHI *et al.,* (2018). "The Spread of True and False News Online". *Science,* 359, p. 1148.

[52] PAUNER CHULVI, C. (2018) "Noticias falsas y libertad de expresión e información. El control de los contenidos informáticos en la red". *Teoría y Realidad Constitucional.* UNED. Núm. 41. p. 299

[53] FERNÁNDEZ-GARCÍA, N. (2017) "*Fake News:* una oportunidad para la alfabetización mediática". *Nueva Sociedad,* nº 269, mayo-junio. p. 68.

[54] VALLÈS, J.M. (1990). "Proceso electoral, comportamiento electoral y sistema político". *Revista del Centro de Estudios Constitucionales,* nº 5. Enero-marzo. p. 189.

la de otros. Una tendencia que se ha visto acrecentada por la irrupción de las plataformas digitales y las nuevas formas de entender la comunicación política que han traído consigo. Estas compañías han revolucionado la forma de difundir y expresar la opinión, de consumir información e incluso la manera de hacer publicidad. Todos estos cambios tienen un impacto directo en el desarrollo de los procesos electorales, como, por ejemplo, en el diseño de las campañas y de la publicidad política[55] y en las estrategias de captación del voto.

Resulta necesario resaltar que no todas las consecuencias de la irrupción de las compañías digitales han sido negativas, entre otros, y como ya han sido adelantados, podrían destacarse los efectos positivos que incluyen una mayor democratización del espacio público. Desde los primeros años de Internet, parte de la doctrina, como el profesor Manuel Castells, predijo que el sistema de comunicación digital revolucionaría el panorama de la comunicación al fragmentar el monopolio informativo sustentado por los grandes medios de comunicación tradicionales, dando paso a una autonomía sin precedentes de los sujetos comunicadores para comunicarse en sentido amplio y de forma no jerarquizada[56]. Se daría voz a individuos y grupos antes silenciados por esos mismos medios que hacían las veces de intermediarios y censores. Se admitía así, como una de las potencialidades de internet, su capacidad para "fomentar, facilitar y engrandecer la participación política de los ciudadanos"[57].

En la actualidad, y con la perspectiva que brinda el paso del tiempo, resulta evidente que las diferentes plataformas digitales ofrecen una pluralidad de medios —blogs, páginas web, enlaces, noticieros digitales…— que han facilitado la aparición de múltiples discursos anteriormente ausentes, facilitando la visibilización de nuevos movimientos sociales que han sido capaces de condicionar la agenda pública[58]. Ello se debe a la capacidad que tienen las redes sociales para compensar la desventaja que, frente a grupos organizados como empresas, sindicatos y asociaciones, tienen colectivos menos disciplinados a la hora de coordinar una reivindicación o una protesta en la esfera pública[59]. La irrupción en las elecciones europeas de junio del español Alvise Pérez y del youtuber chipriota Fidias, demuestra la capacidad que tienen este tipo de perfiles famosos en redes sociales —juntos acumulan unos cuatro millones de seguidores— para condicionar, tanto para bien como para mal, la agenda pública sin apenas protagonismo en los medios tradicionales.

---

[55] Una preocupación que ha encontrado acomodo normativo en el Reglamento (UE) 2024/900 sobre transparencia y segmentación en la publicidad política.

[56] CASTELLS, M. (2009) *Comunicación y poder.* Madrid. Alianza Editorial. pp. 188-189.

[57] RUBIO NÚÑEZ, R (2000) "Internet en la participación política". *Revista de Estudios Políticos* (Nueva Época). Nº 109. Julio-septiembre. p. 291

[58] RESINA DE LA FUENTE, J. (2010). "Ciberpolítica, redes sociales y nuevas movilizaciones en España: el impacto digital en los procesos de deliberación y participación ciudadana". *Mediaciones Sociales. Revista de Ciencias Sociales y de la Comunicación,* nº7, segundo semestre de 2010, pp. 143-169. Universidad Complutense de Madrid. pp. 150-151.

[59] SHIRKY, C. (2011). "The Political Power of Social Media: Technology, The Public Sphere, and Political Change". *Foreign Affairs,* Vol. 9, nº1, enero-febrero. p. 35.

1. Amenazas para una libre conformación de la voluntad política

Como ya se ha mencionado, los complejos sistemas algorítmicos utilizados por las compañías digitales son capaces de elaborar perfiles muy precisos recabando los datos y la información que los usuarios van generando a medida que utilizan sus servicios. Sobre estos perfiles se cimenta toda la estructura publicitaria en la que se basa su modelo de negocio. Disponer de esta ingente cantidad de información dota a las compañías de una capacidad sin precedentes para detectar posibles consumidores y segmentar el mercado con precisión.

De esta forma, los datos pueden ser útiles para que empresas publicitarias oferten con precisión sus productos a potenciales clientes, o para que conozcan con precisión hábitos de consumo y preferencias, pudiendo así diseñar estrategias de mercado más eficientes. Sin embargo, y para lo que aquí nos interesa, también pueden ser utilizados para dirigir, con extrema precisión, publicidad electoral a grupos concretos de la población. Conocer las preferencias ideológicas, los gustos e inquietudes de las personas permite realizar una campaña mucho más personalizada hacia, por ejemplo, un potencial grupo de votantes indecisos. Estas acciones son las que se conocen como "*microtargeting*" y pueden derivar, en sus versiones más extremas, en campañas de publicidad política personalizada que pretenda influir en el sentido del voto del ciudadano de una manera subliminal, apelando directamente a sus inquietudes o miedos sin que el destinatario sea capaz de reconocer que el contenido concreto que se le presenta ha sido deliberadamente seleccionado para influir en su conducta política[60].

La DSA, consciente de los riesgos que esta práctica puede entrañar, limita el uso de técnicas de segmentación para la presentación de anuncios que se basen en la elaboración de perfiles utilizando los considerados como "datos personales de carácter especial"[61]. Esta categoría de datos especiales viene reconocida en el Reglamento General de Protección de Datos[62], entre los que destacan aquellos relativos a la salud, la ideología, las concepciones filosóficas o la orientación sexual de las personas usuarias del servicio. No obstante, casos de *microtargeting* electoral como el de Cambridge Analytica, o el llevado a cabo durante la campaña del BREXIT, reflejan la necesidad de que se realice un control efectivo sobre el cumplimiento de dichas disposiciones.

Los algoritmos de estas compañías son los que dictan lo que los usuarios visualizan y de qué manera, por lo que pueden ser fácilmente manipulados para restringir o priorizar determinados contenidos. Además, lo normal es que los usuarios no sean conscientes de que se han tomado decisiones en su lugar sobre lo que acaban consumiendo y que éstas limitan su exposición a ciertos contenidos de manera

[60] HOWDLE, G. (2023). "Microtargeting, Dogwhistles and Deliberative Democracy". *Topoi,* nº 42, pp. 446 y 447.

[61] Considerando (69) DSA.

[62] Art. 9.1. del Reglamento (UE) 2016/679 (Reglamento general de protección de datos).

intencionada. Ello puede llevar a la creencia errónea de que lo que se presenta se hace de manera neutral y que cubre los diversos puntos de vista existentes[63].

Del mismo modo que los algoritmos pueden programarse para ejecutar una determinada tarea —como detectar los gustos y preferencias de los usuarios—, podrían ser configurados para, por ejemplo, enviar información sesgada a grupos poblacionales sensibles o pendientes de determinados temas o noticias concretas[64]. Se trata de una técnica conocida como "*dogwhistle*" o "silbato para perros" consistente en promocionar de manera intencionada mensajes que contengan ciertas palabras clave y que puedan ser atribuibles a determinada opción política. Otra forma de influir de forma menos aparente en la promoción de ciertos actores políticos podría darse mediante una política permisiva con la utilización de *bots*[65] y cuentas falsas que interactuando de forma masiva denotan una falsa impresión de popularidad, lo que puede influir en la percepción que sobre ciertos candidatos puedan formarse los usuarios.

Se trata de un riesgo que viene a desmentir la creencia en la supuesta neutralidad de los prestadores de servicios digitales mostrando el poder real y efectivo del que disponen estas compañías para tomar partido por la opción política que mayor sintonía muestre con sus propios intereses comerciales y servirles de altavoz.

2. Amenazas derivadas de injerencias de terceros

Las posibles injerencias en los procesos electorales nacionales por parte de terceros— ya sean estos gobiernos extranjeros o grupos de interés privados— han sido uno de los pilares sobre los que se ha centrado el debate público sobre la seguridad digital de las elecciones. El Parlamento Europeo ha recomendado a los Estados miembros que cataloguen la injerencia extranjera en línea, incluida la desinformación, como una amenaza a la seguridad nacional y transfronteriza, a la vez que hace un llamamiento para el establecimiento de medidas que atenúen las posibles consecuencias que pueden ser ocasionadas por esta práctica[66]. Este tipo de interferencia puede ejecutarse utilizando métodos que van desde los ciberataques a la infraestructura electoral

[63] PRESNO LINERA, M.A. (2022). *Derechos Fundamentales e Inteligencia Artificial*. Madrid. Fundación Manuel Giménez Abad. Marcial Pons. pp. 57 y 58.

[64] ABA-CATOIRA, A. (2020) "Los desórdenes informativos en un sistema de comunicación democrático". *Revista de Derecho Político.* UNED. N.º 109. Septiembre-diciembre. p. 126

[65] Se define el término *"bot"* – abreviatura de robot– como una cuenta de redes sociales predominantemente controlada por un programa informático y no por un usuario humano. Si bien es cierto que dicha definición es inherentemente neutral sobre la intencionalidad detrás de la creación y utilización de los *bots* , las investigaciones realizadas apuntan a un mayor uso malintencionado que legítimo de los mismos. FERRARA, E. (2020). "Bots, elections, and social media: a brief overview", en K. Shu et al. (eds.) *Disinformation, Misinformation, and Fake News in Social Media: Emerging Research Challenges and Opportunities*. Springer. p. 97.

[66] Resolución del Parlamento Europeo 2022/2075(INI), de 1 de junio de 2023, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, en particular la desinformación. P9_TA(2023)0219. punto (11) y ss. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0219_ES.pdf.

del Estado, hasta la producción de campañas de desinformación masivas y la financiación ilegal de candidatos concretos[67].

Muchas de estas actividades se llevan a cabo por las ya mencionadas cuentas *"bot",* perfiles de redes sociales que simulan ser usuarios humanos desde las que se realiza una coordinación para distribuir contenido incendiario y falso a determinados grupos radicales, o para tratar de generar campañas de desinformación e incluso ataques directos como insultos y amenazas a determinados usuarios[68]. Este tipo de injerencias externas representa uno de los desafíos más importantes para las estructuras democráticas de los Estados miembros de la Unión Europea. En este contexto, Robles Carrillo, señala que, entre otras cuestiones, la percepción de que Europa se ha visto perjudicada en términos geopolíticos por las grandes compañías digitales, tanto estadounidenses como chinas, ha abierto el debate en torno a la articulación de una propuesta de soberanía digital europea que sitúe al continente en una autonomía estratégica frente a terceros y en defensa de sus valores democráticos[69].

Como ya se ha mencionado, el desarrollo de esta soberanía digital refleja la competición entre diferentes modelos: Estados Unidos, China y la Unión Europea. Cada uno de ellos entiende la digitalización como un negocio en Estados Unidos, un instrumento de poder en China y una esfera en la que deben perseguirse valores sociales y democráticos en Europa[70]. Es dentro de esta lógica de modelos diferenciados en la que la DSA positiviza los principios democráticos europeos al sistematizar los riesgos que puede implicar la influencia de potencias extranjeras —o incluso de las propias compañías digitales— sobre la política nacional y la gobernanza democrática interna. Una amenaza que, pudiendo derivar en ataques cibernéticos a infraestructuras tecnológicas vitales del Estado, podría incluirse en el siguiente apartado relativo a la seguridad pública

C) La protección de la seguridad pública

Siguiendo a Freixes y Remotti[71], la seguridad pública puede entenderse, por un lado, como el interés de la colectividad en que se adopten medidas preventivas

[67] CALABRESE, S. y REICH, O. (2024). Op. Cit. p. 38.

[68] KLÜBER, J. et al. (2021). "The 2021 German Federal Election on Social Media: An Analysis of Systemic Electoral Risks Created by Twitter and Facebook Based on the Proposed EU Digital Service Act". Report for the WU Vienna University of Economics and Business. Agosto. p. 47.

[69] ROBLES CARRILLO, M. (2023). "La articulación de la soberanía digital en el marco de la Unión Europea". *Revista de Derecho Comunitario Europeo,* nº 75, p. 151.

[70] INNERARITY, D. (2023) "European Digital Sovereignty", en BONGARDT, A. and TORRES, F. (eds), *The political economy of Europe's future and identity: integration in crisis mode*, Florence, European University Institute. p. 289

[71] FREIXES SANJUAN, T y REMOTTI CARBONELL, J.C. (1995) "La configuración constitucional de la seguridad ciudadana". *Revista de Estudios Políticos* (Nueva Época). Núm. 87. Enero-marzo. Entre las páginas 149 y 153, los autores realizan una investigación en torno a la delimitación del concepto "seguridad pública" en la Constitución española de 1978.

tendentes a evitar situaciones de peligro o riesgo de desastres y calamidades. Por otro, como el interés por asegurar el correcto funcionamiento de los entes públicos, la seguridad jurídica, y la protección de bienes o del patrimonio público. Al mismo tiempo, señalan, deben existir instrumentos suficientes y adecuados para hacer frente a las situaciones que puedan poner en peligro dichos intereses[72]. De suerte que puede afirmarse que, materialmente, "la seguridad pública tiene como objeto la protección de personas y bienes y el mantenimiento de la tranquilidad y el orden ciudadano"[73], para conseguir así, un equilibrio entre las normas y los derechos y libertades. Con relación a dicha definición, la DSA vincula la defensa de la seguridad pública con la salud pública[74], y la configura como uno de los hechos que pueden justificar el establecimiento de medidas de urgencia como respuesta a crisis que den lugar a circunstancias extraordinarias que amenacen la seguridad de la Unión[75].

En un Estado democrático, la garantía de los derechos fundamentales está estrechamente vinculada con la seguridad pública. Esto se debe a que los derechos y libertades únicamente podrán ser eficazmente ejercidos si el orden y la paz social están garantizados, permitiendo que los ciudadanos vivan en armonía[76], con confianza en las instituciones y con la seguridad de que sus derechos individuales son —y serán— respetados por el resto de la comunidad. Es cierto que muchas de las amenazas previamente analizadas pueden llegar a constituir un riesgo para la paz social, sin embargo, pueden señalarse ciertas actividades cuyo objetivo y resultado directo implica la generación de enfrentamientos y altercados que alteran la convivencia pacífica de la sociedad, y que justifican la inclusión de la seguridad pública junto a los riesgos para el discurso cívico y los procesos electorales, como riesgos que afectan al sistema democrático.

1. Amenazas para el mantenimiento del orden público y la paz social

Como en el caso del discurso cívico, las campañas de desinformación afectan directamente a la seguridad pública, al configurarse como auténticas amenazas para los Estados democráticos. Pues, como se refleja en la Estrategia se Seguridad Nacional de 2021[77], estas actividades buscan polarizar la sociedad y minar la confianza ciudadana

[72] Ibidem. p. 152.

[73] RIDAURA MARTÍNEZ, M.J. (2014) "La seguridad ciudadana como función del Estado". *Estudios de Deusto*. Vol. 62/2. Bilbao. Julio-diciembre. p. 333.

[74] Considerando (91) DSA.

[75] Artículo 36 DSA. Tales crisis suponen una amenaza para la seguridad estatal y pueden derivar de: conflictos armados, actos de terrorismo, catástrofes naturales, pandemias y amenazas transfronterizas.

[76] MARTÍNEZ ATIENZA, G. (2018) *Políticas de seguridad pública y privada*. Ediciones Experiencia. Barcelona. pp. 4 y 5.

[77] Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021.

en las instituciones democráticas, y con ello de los propios procesos electorales, mediante la propagación de un contenido distorsionado de la realidad.

En este sentido, puede darse el supuesto en el que aquellos candidatos que hayan perdido las elecciones, así como sus partidarios, se dediquen a difundir alegaciones indocumentadas sobre un supuesto fraude electoral, como por ejemplo durante el proceso de escrutinio, tratando así de justificar la derrota electoral. Todas estas acciones tienen el objetivo de deslegitimar las elecciones democráticas y movilizar a parte del electorado para la realización de protestas electorales que pueden acabar en disturbios y serios enfrentamientos con las fuerzas y cuerpos de seguridad u otros ciudadanos[78]. Un riesgo real que pudo ser corroborado durante el asalto al Capitolio estadounidense en 2021[79], y durante la toma de las principales instituciones federales en Brasilia en 2023[80]. Ambos casos promovidos y alentados desde cuestas de redes sociales alegando un supuesto fraude electoral, socavando la confianza ciudadana en las instituciones democráticas.

Ese tipo de actividades tiende a generar, a su vez, un efecto disruptivo en la sociedad exacerbando la polarización. La exposición selectiva a determinados contenidos, las perspectivas aisladas de la información que se consume, y las ya mencionadas cámaras de eco, dificultan el reconocimiento y el respeto de opiniones diferentes. El modelo de negocio basado en la obtención de datos para su posterior comercialización con fines publicitarios precisa que los usuarios permanezcan el mayor tiempo posible en las plataformas. En la medida en que los contenidos extremistas y las opiniones más incendiarias son capaces de producir mayor número de interacciones, los algoritmos tienden a promocionan este tipo de mensajes frente al resto[81].

La sustitución de los discursos sosegados por posiciones más extremas puede comprobarse en la generalización de los discursos de odio. Este tipo de contenido suele dirigirse a la estigmatización y criminalización de ciertos colectivos vulnerables para generar un efecto de odio hacia los mismos o crear una situación de confusión e histeria social tergiversando la realidad o exagerando la magnitud de una

[78] KLÜBER, J. Op. cit. pp. 43-44.

[79] Existía un temor a que pudiera repetirse un episodio similar en caso de que la candidata Kamala Harris ganase las elecciones frente a Trump por un escaso margen. Ya que el republicano advirtió en sus redes sociales de que los demócratas únicamente podrían vencer haciendo trampas. Andrew Prokop. "*The crisis that could ensue if Harris wins narrowly. How far would Trump and his supporters go to try and flip the outcome?"*. VOX. 30/10/2024

[80] Un hecho que ha llevado al expresidente Jair Bolsonaro a ser acusado por la policía federal de un intento de golde de Estado y de abolición del Estado de Derecho. Naiara Galarraga *"La policía acusa formalmente a Bolsonaro, a dos generales y a 34 personas más de intento de golpe de Estado en Brasil"*. El País. 21/11/2024.

[81] BALAGUER CALLEJÓN, F. (2023) "La Constitución del algoritmo. El difícil encaje de la Constitución analógica en el mundo digital" en BALAGUER CALLEJÓN, F. y COTINO HUESO, L. (Coord.), *Derecho Público de la Inteligencia artificial*. Zaragoza. Fundación Giménez Abad. p 47..

preocupación o problema social[82]. Todo ello afecta a la seguridad pública ya que, en muchas ocasiones, estas actividades se traducen en un estallido de violencia en el mundo analógico.

D) Medidas de reducción de riesgos

El artículo 34.2 del Reglamento establece que al realizar las evaluaciones de los potenciales riesgos sistémicos, las grandes plataformas deberán de tener en cuenta la manera en la que influyen los siguientes factores: el diseño de sus sistemas de recomendación y de cualquier otro sistemas algorítmico; sus sistemas de moderación de contenidos, las condiciones generales aplicables y su ejecución; los sistemas de selección y presentación de anuncios, así como las prácticas del prestador relacionadas con los datos. Con base en dichos factores, el artículo 35.1 identifica potenciales medidas atenuantes: adaptar el diseño, las características o el funcionamiento de sus servicios; adaptar sus términos y condiciones; adaptar los procesos de moderación de contenidos y sus sistemas algorítmicos; la adopción de medidas de concienciación; la puesta en marcha de ajustes de cooperación con los alertadores fiables; etc. En relación con la seguridad pública, el artículo 36 prevé la posibilidad de que la Comisión, previa recomendación de la Junta de servicios digitales, exija de forma preceptiva el establecimiento de las medidas previstas en el artículo 35 —entre otras— cuando se produzcan circunstancias extraordinarias que supongan una grave amenaza para la seguridad o la salud pública.

Más allá de la posible configuración de nuevos tipos delictivos[83], la defensa de la democracia requiere la puesta en práctica de herramientas educativas que promuevan una ciudadanía responsable y posibiliten la adquisición de una cohesión e identidad común, que permita una convivencia respetuosa en la diversidad[84]. Una educación que, dirigida preferentemente a los nativos digitales, tenga como finalidad concienciar sobre los riesgos que conlleva el uso acrítico de este tipo de plataformas digitales para el correcto desarrollo de las democracias, además de informarles sobre sus derechos y deberes como usuarios[85]. Para ello, las medidas deberían centrarse en dar a

[82] NUEVO-LÓPEZ, A., et al. (2023). "Bulos, redes sociales, derechos, seguridad y salud pública: dos casos de estudio relacionados". *Revista de Ciencias de la Comunicación e Información.* Vol. 28. Los autores realizan un interesante estudio sobre el rol de las redes sociales a la hora de amplificar ciertos bulos relacionados con las agresiones sexuales y las infecciones relacionadas con la viruela del mono.

[83] Por ejemplo, Marchal González propone la posibilidad de configurar un "delito de desinformación": MARCHAL GONZÁLEZ, A.N. (2023). "La necesidad de un nuevo tipo delictivo: La desinformación como una amenaza para el orden público". *Boletín Criminológico*. N.º 219. pp. 27 y ss.

[84] VIDAL PRADO, C. (2022). "La educación cívica como herramienta para construir y fortalecer la democracia y el Estado de derecho". *Revista General de Derecho Público Comparado,* nº32, diciembre. pp. 13 y 28.

[85] JARAMILLO, O (2013). "El futuro de la vida pública y privada en las redes sociales" en CORREDOIRA, L. y COTINO HUESO, L (dirs.). Op. Cit. p. 410.

conocer los peligros inherentes al uso malintencionado de estos servicios como, por ejemplo, las cámaras de eco, el funcionamiento no neutral de los algoritmos, las injerencias extranjeras y los sesgos de confirmación[86]. Todo ello debe hacerse desde las propias plataformas[87], pero con la necesaria colaboración de los alertadores fiables[88] —condición que deberá de ser otorgada a las entidades que cumplan los requisitos y por el procedimiento previsto en el art. 22—, y de las instituciones públicas de los Estados miembros.

Una de las cuestiones que no se abordan en el Reglamento y que podría resultar de gran relevancia, no sólo en la cuestión de los riesgos democráticos sino para todos los sistemas en general, es la posibilidad de que las grandes plataformas y los motores de búsqueda de gran tamaño interrumpieran o incluso cesaran la prestación de sus servicios. Ello en la medida en que miles de empresas dependen en cierta forma de las plataformas digitales para la comunicación con sus clientes. Igualmente, los servicios que prestan estas compañías son cruciales para las campañas de numerosos candidatos políticos y partidos, sobre todo para aquellos partidos pequeños o de nivel local a los que resulta muy difícil llegar a los medios de tirada nacional.

Junto a la esfera privada, la pandemia del Covid-19 puso de manifiesto la dependencia que tienen los gobiernos de este tipo de plataformas a la hora de hacer frente a crisis nacionales; no sólo para llegar a un gran parte de la población, sino por el papel prominente que tuvieron las plataformas para fiscalizar la información y determinar qué fuentes podían considerarse fiables y cuáles no[89]. Una posición de subordinación que para ciertas voces críticas refleja la insuficiencia de la regulación propuesta por la DSA, que al intentar establecer un régimen mayor de responsabilidad por las posibles consecuencias del diseño de sus interfaces, coloca a las compañías en un auténtica posición de dominio de la comunicación en línea, como verdaderas soberanas del discurso y del poder de opinión en el mundo digital[90]. Una idea que ha llevado a parte de la doctrina a defender una regulación que, más allá de centrarse

[86] Resolución del Parlamento Europeo 2022/2075(INI), de 1 de junio de 2023, Op. Cit. puntos (17) y (20).

[87] La herramienta DSA "Whistleblower Tool" permite a las personas con información privilegiada –como los propios trabajadores– realizar denuncias anónimas sobre posibles prácticas nocivas: https://digital-services-act-whistleblower.integrityline.app/

[88] Además de los mecanismos de notificación y acción ya existentes en anteriores disposiciones, centrales en el esquema de exención de responsabilidad de las grandes compañías digitales, la DSA codifica la figura de los alertadores fiables. Estos deberán ser entidades que posean conocimientos y competencias específicas para detectar, identificar y notificar contenidos ilícitos, así como independientes de las plataformas. Una regulación que, sin embargo, no llega a ser suficiente y perpetua el modelo de negocio de las plataformas y que, sin una mayor concreción y control, quedan al servicio de las estructuras de poder ya existentes. CETINA PRESUEL, R. (2024). "Alertadores fiables: de su codificación en el reglamento de servicios digitales a la necesidad de atender a sus limitaciones" en SERRANO MAÍLLO, I y CORREDOIRA, L. (Edis.). Op. Cit. pp. 258 y ss.

[89] HELBERGER, N. (2020). "The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power". *Digital Journalism,* nº8 (6), p. 848.

[90] HELBERGER, N. (2020). Op. cit. pp. 847-849.

en los posibles usos malintencionados que se haga de los servicios ofertados por estas compañías, otorgue a los diseños algorítmicos la consideración de infraestructuras esenciales[91] y les aplique el marco regulatorio de compañías que prestan servicios de interés público, adaptándolo a las circunstancias del mundo digital.

Debido a la naturaleza de estos riesgos muchos deberán abordarse desde una lógica de coordinación entre las diferentes compañías digitales y los Estados, pues en muchos casos, las causas que originan estos riegos se dan en más de una plataforma a la vez o se contagian de una a otra, en la medida en que éstas forman un entramado ecosistema de nivel global. Por ello, y en relación con el resto de los riesgos sistémicos, la DSA establece, como garantía de su propia eficacia y ejecución, la obligación de crear en cada Estado miembro una autoridad competente como "coordinador de servicios digitales"[92] —encargada de la supervisión de los prestadores de servicios intermediarios y de la aplicación del Reglamento— y una "Junta Europea de Servicios Digitales" que integre a los Coordinadores nacionales y sirva de asistencia a la Comisión[93]. En caso de incumplimiento reiterado también se prevé un disuasorio régimen sancionatorio[94].

V. CONCLUSIONES

La limitación del poder en una democracia constitucional debe, en su sentido más elemental, tratar de garantizar que las reglas del juego democrático y el proceso electoral sean respetadas por todos los actores participantes, y que las elecciones se desarrollen de manera limpia y garantista. Si no se observan esas condiciones mínimas, no podría asegurarse la convivencia social, ni tampoco la resolución pacífica de controversias, y el aparato institucional sobre el que se erige el régimen democrático quedaría dañado de manera irreparable. El surgimiento en las últimas décadas de grandes conglomerados digitales de carácter multinacional ha puesto de manifiesto

[91] SIMONS, J., y GHOSH, D. (2020). "Utilities for Democracy: Why and How the Algorithmic Infrastructure of Facebook and Google must be Regulated". *Brookings Institution,* pp. 9 y ss.; GUGGENBERGER, N. (2021). "Essential Platforms". *24 Stanford Technology Law Review, nº 237.* pp. 327 y ss.

[92] En el caso de España la Comisión Nacional de los Mercados y la Competencia (CNMC) ha sido designada por el Ministerio para la Transformación Digital y de la Función Pública como Coordinador de servicios digitales. https://www.cnmc.es/prensa/coordinador-servicios-digitales-20240124.

[93] Artículos 49 y 61 DSA, respectivamente, y cuyo plan de trabajo se ha presentado para los meses de septiembre de 2024 hasta agosto de 2025. Puede comprobarse un resumen de las labores de control realizadas por la Comisión en la web https://transparency.dsa.ec.europa.eu/.

[94] Artículos 52 y 74-79 DSA. La Comisión ha enviado a X las conclusiones preliminares por un supuesto incumplimiento de lo dispuesto por los artículos 25, 39 y 40 (12) de la DSA. En caso de confirmarse, implicaría la aplicación del artículo 52 pudiendo imponer a la plataforma una multa de hasta el 6 % del volumen de negocios total anual mundial. https://ec.europa.eu/commission/presscorner/detail/es/ip_24_3761.

la aparición de unos nuevos jugadores en el tablero democrático. Unos sujetos que, más allá de participar bajo el marco normativo del resto de actores, han actuado bajo una autorregulación que les ha otorgado un papel preponderante y cuyo poder e influencia no puede seguir siendo ignorado.

El reconocimiento por parte del Reglamento de Servicio Digitales del potencial riesgo que puede ocasionar un uso malintencionado de los servicios intermediarios en línea sobre los procesos democráticos es un paso significativo —pero no suficiente— a la hora de intentar proteger las democracias. Las redes sociales no son el reflejo directo de la sociedad y las plataformas no son espacios neutrales en los que "el libre mercado de las ideas" funcione sin interferencias. Los sistemas algorítmicos están diseñados con una lógica de maximizar el tiempo que los usuarios pasan en las plataformas para poder así extraer datos y posteriormente comercializarlos con fines publicitarios. De ello se derivan las interferencias que grupos de usuarios o incluso las propias plataformas pueden generar para distorsionar los contenidos y promocionar o silenciar mensajes concretos.

Los escándalos que se han dado en los últimos años en torno a los procesos electorales en línea han puesto de manifiesto que los esfuerzos actuales por parte de los reguladores públicos, así como de las grandes plataformas, no son suficientes para asegurar unos procesos electorales limpios. Los Estados tienen que tomar plena conciencia sobre las carencias que presentan las regulaciones electorales actuales en lo concerniente a la publicidad y las campañas electorales en el entorno digital. Se debe impulsar una educación que promueva valores cívicos democráticos y donde se advierta de los riesgos inherentes al uso de las nuevas tecnologías. Es preciso, además, reconocer el papel protagonista que pueden llegar a tener las compañías de servicios intermediarios en línea durante las elecciones para poder diseñar instituciones adecuadas que garanticen el desarrollo de un proceso electoral con todas las garantías en la que todos los actores respeten las reglas del juego. Es necesario que los avances tecnológicos promuevan dinámicas que favorezcan la participación ciudadana dentro de una lógica cívica y democrática. Una solución que no puede venir auspiciada por un modelo basado en la autorregulación de los grandes conglomerados tecnológicos, ni en las decisiones tecnocráticas de los grupos de expertos que para éstos trabajan.

El enfoque normativo de la DSA, cuya base jurídica recae en el art. 114 TFUE —relativo al mercado interior—, no parece el más adecuado. Junto al Reglamento General de Protección de Datos, el Reglamento de Mercados Digitales y el Reglamento de Inteligencia Artificial, la DSA se encuadra en un entramado normativo que trata de conjugar la innovación tecnológica con la protección de los derechos fundamentales. Sin embargo, los sujetos destinatarios de las normas son entes privados a los que se impone una serie de obligaciones para garantizar el respeto de ciertos derechos. Una suerte de regulación horizontal de los derechos, una intervención desde la lógica económica del mercado interior que puede llegar a desnaturalizarlos.

Desde lo que se ha entendido por "discurso cívico", "procesos electorales" y "seguridad pública", se ha tratado de identificar una serie de amenazas que, de manera

Revista de Derecho Político
N.º 122, enero-abril, 2025, págs. 295-326
https://doi.org/10.5944/rdp.122.2025.44751

general, pueden afectar al correcto funcionamiento y desarrollo de los sistemas democráticos, y que abarcan temas como las injerencias de terceros Estados, las noticias falsas y la microsegmentación.

La cuestión no radica en decidir si las elecciones democráticas son o no compatibles con las grandes compañías digitales ya que, a pesar de presentar retos sin precedentes a los sistemas electorales, también pueden ser instrumentos democratizadores de los espacios públicos, sirviendo de altavoz a opiniones que hasta ahora eran silenciadas por los medios tradicionales. Lo verdaderamente relevante será determinar si las plataformas y sus reguladores estarán dispuestos a tomarse en serio los riesgos sistémicos en torno a las elecciones y adoptar medidas significativas para atenuarlos. Para ello, no deben limitarse a la realización de pequeños ajustes y cambios en sus sistemas durante las campañas electorales, sino que deben diseñar plataformas más respetuosas con las garantías democráticas y los procesos electorales que vertebran y aseguran nuestra convivencia pacífica y ordenada.

VI. BIBLIOGRAFÍA

Aba-Catoira, A. (2020) "Los desórdenes informativos en un sistema de comunicación democrático". *Revista de Derecho Político.* UNED. N.º 109. Septiembre-diciembre. pp. 119-151. https://revistas.uned.es/index.php/derechopolitico/article/view/29056

Alexiadis, p. y de Streel, A. (2020) "Designing an EU Intervention Standard for Digital Platforms". *EUI Working Paper RSCAS 2020/14.* Robert Schuman Centre for Advanced Studies, Florence School of Regulation. European University Institute. https://cadmus.eui.eu/handle/1814/66307.

Balaguer Callejón, F. (2022). *La Constitución del algoritmo*. Zaragoza. Fundación Manuel Giménez Abad.

— (2023). "La Constitución del algoritmo. El difícil encaje de la Constitución analógica en el mundo digital", en BALAGUER CALLEJÓN, F. y COTINO HUESO, L. (Coord.), *Derecho Público de la Inteligencia artificial*. Zaragoza. Fundación Giménez Abad. pp. 29-56.

Barberá, P. (2020). "Social Media, Echo Chambers, and Political Polarization" en PERSILY, N y TUCKER, J.A. *Social Media and Democracy.* Cambridge University Press.

Barrero Ortega, A. (2021). "Responsabilidad de los intermediarios de internet en el derecho de la UE". *Revista Española de Derecho Constitucional,* nº 123, pp. 107-132. doi: https://doi.org/10.18042/cepc/redc.123.04

Calabrese, S. y Reich, O. (2024). "Identifying, Analysing, Assessing and Mitigating potential negative effects on civic discourse and electoral processes: a minimum menu of risks very large online platforms should take heed of". *European Partnership for Democracy*. January. https://www.liberties.eu/f/mpdgy5

Castells, M. (2009). *Comunicación y poder,* Madrid, Alianza Editorial.

Cetina Presuel, R. (2024). "Alertadores fiables: de su codificación en el reglamento de servicios digitales a la necesidad de atender a sus limitaciones" en SERRANO MAÍLLO, I y CORREDOIRA, L. (eds.) *Democracia y desinformación: nuevas formas de polarización, discursos de odio y campañas en redes. Respuestas regulatorias de Europa y América Latina.* Madrid. Dykinson. pp. 251-266.

Corredoira, L. (2024) "Democracia y desinformación. Respuestas regulatorias de la Unión Europea para el fortalecimiento de la democracia y cambios de rumbo del paquete de servicios digitales" en en SERRANO MAÍLLO, I y CORREDOIRA, L. (eds.) *Democracia y desinformación: nuevas formas de polarización, discursos de odio y campañas en redes. Respuestas regulatorias de Europa y América Latina.* Madrid. Dykinson. pp. 267-293.

Cotino Hueso, L. (2013) "La selección y personalización de noticias por el usuario de nuevas tecnologías" en CORREDOIRA, L. y COTINO HUESO, L (dirs.), *Libertad de expresión e información en Internet: amenazas y protección de los derechos fundamentales.* Madrid. Centro de Estudios Políticos y Constitucionales. pp. 41-56.

de Gregorio, G. (2022). "Digital Constitutionalism across the Atlantic". *Global Constitutionalism,* nº 11 (2) pp. 279-324.

de Vega García, P. (1998) "Mundialización y Derecho Constitucional: La crisis del principio democrático en el constitucionalismo actual". *Revista de Estudios Políticos* (Nueva Época), nº 100. Abril-junio. pp. 13-56. https://www.cepc.gob.es/sites/default/files/2021-12/17154repne100015.pdf

de Vergottini, G. (2015) "La persistente soberanía". *Teoría y Realidad Constitucional.* UNED. Nº 36. pp. 67-91. https://revistas.uned.es/index.php/TRC/article/view/16079

Ehrlich P. (2002). "Communication Decency Act §230". *Berkeley Technology Law Journal.* Vol. 17. pp. 401-420. DOI: https://doi.org/10.15779/Z384X12.

Fernández-García, N. (2017). "*Fake News:* una oportunidad para la alfabetización mediática". *Nueva Sociedad,* Nº 269, mayo-junio. pp 66-77.

Ferrara, E. (2020). "Bots, elections, and social media: a brief overview", en K. Shu et al. (eds.), *Disinformation, Misinformation, and Fake News in Social Media: Emerging Research Challenges and Opportunities*. Springer. pp. 95-114. Disponible en línea: https://link.springer.com/chapter/10.1007/978-3-030-42699-6_6.

Freixes Sanjuan, T y Remotti Carbonell, J.C. (1995) "La configuración constitucional de la seguridad ciudadana". *Revista de Estudios Políticos* (Nueva Época). Núm. 87. Enero-marzo. pp. 141-162.

González de la Garza, L.M. (2018). "La crisis de la democracia representativa. Nuevas relaciones políticas entre democracia, populismo virtual, poderes privados y tecnocracia en la era de la propaganda electoral cognitiva virtual, el *microtargeting* y el *big data*". *Revista de Derecho Político,* nº 103, septiembre-diciembre, págs. 257-302. https://revistas.uned.es/index.php/derechopolitico/article/view/23203

Guggenberger, N. (2021). "Essential Platforms". *24 Stanford Technology Law Review,* nº 237. pp. 237-343. https://law.stanford.edu/publications/essential-platforms/

Helberger, N., Kleinen-Von Königslöw, K., y VAN DER NOLL, R. (2015). "Regulating the New Information Intermediaries as Gatekeepers of Information Diversity". *Info,* VOL. 17, Nº6. pp. 50-71. https://www.ivir.nl/publicaties/download/1618.pdf.

— (2020). "The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power". *Digital Journalism,* VOL. 8, nº6, p.842-854. https://doi.org/10.1080/21670811.2020.1773888

Howdle, G. (2023). "Microtargeting, Dogwhistles and Deliberative Democracy". *Topoi,* nº 42, pp. 445-458. https://doi.org/10.1007/s11245-023-09889-3.

Innerarity, D. (2023). "European Digital Sovereignty", en BONGARDT, A. and TORRES, F. (eds), *The political economy of Europe's future and identity : integration in crisis mode*, Florencia, European University Institute, pp. 286-292 - https://hdl.handle.net/1814/76293.

Jaramillo, O (2013). "El futuro de la vida pública y privada en las redes sociales" en CORREDOIRA, L. y COTINO HUESO, L (dirs.), *Libertad de expresión e información en Internet: amenazas y protección de los derechos fundamentales.* Madrid. Centro de Estudios Políticos y Constitucionales. pp. 395-413.

Klüber, J. et al. (2021). "The 2021 German Federal Election on Social Media: An Analysis of Systemic Electoral Risks Created by Twitter and Facebook Based on the Proposed EU Digital Service Act". Report for the WU Vienna University of Economics and Business. Agosto. https://www.sustainablecomputing.eu/wp-content/uploads/2021/10/DE_Elections_Report_Final_17.pdf

Kosseff, F. (2019) *The Twenty-Six Words That Created The Internet*. Cornell University Press.

Lazer, M.J.D *et al.,* (2018). "The Science of Fake News". *Science,* nº 359, pp. 1094-1096. DOI:10.1126/science.aao2998.

Leavitt, P. y Peacock, C. (2014). "Civility, Engagement, and Online Discourse: a Review of Literature". *National Institute for Civic Discourse*, The University of Arizona. August 4.

Leerssen, P. (2023). "An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation". *Computer Law and Security Review,* Vol. 48. Abril. https://www.sciencedirect.com/science/article/pii/S0267364923000018

Marchal González, A.N. (2023). "La necesidad de un nuevo tipo delictivo: La desinformación como una amenaza para el orden público". *Boletín Criminológico*. N.º 219. pp. 1-39.

Martínez Atienza, G. (2018). *Políticas de seguridad pública y privada*. Ediciones Experiencia. Barcelona. Libro electrónico.

Martín Jiménez, F.J. (2024). "Big Data: Riesgos y soluciones desde el Derecho y desde los principios". *Revista de Derecho Político,* nº 119, enero-abril, págs. 215-249. https://revistas.uned.es/index.php/derechopolitico/article/view/40416

Micova, S. y Calef, A. (2023). "Elements for Effective Systemic Risk Assessment under the DSA". *Center on Regulation in Europe* (CERRE), Report. July. https://cerre.eu/wp-content/uploads/2023/07/CERRE-DSA-Systemic-Risk-Report.pdf

Nuevo-López, A., López-Martínez, F., y DELGADO PEÑA, J.J. (2023). "Bulos, redes sociales, derechos, seguridad y salud pública: dos casos de estudio relacionados". *Revista de Ciencias de la Comunicación e Información.* Vol. 28. pp. 120-147.

Papacharissi, Z. (2004). "Democracy online: Civility, Politeness, and the Democratic Potential of Online Discussion Groups". *New Media and Society*, Vol 6(2). pp. 259-283.

Pauner Chulvi, C. (2018). "Noticias falsas y libertad de expresión e información. El control de los contenidos informáticos en la red". *Teoría y Realidad Constitucional.* UNED. Núm. 41. pp. 297-318.

Pielemeier, J. y Sullivan, D. (2023). "Implementing risk assessments under the Digital Service Act". *Digital Trust and Safety Partnership*, Discussion Summary. Junio.

Presno Linera, M.A. (2022). *Derechos Fundamentales e Inteligencia Artificial*, Madrid Fundación Manuel Giménez Abad, Marcial Pons.

Resina de la Fuente, J. (2010). "Ciberpolítica, redes sociales y nuevas movilizaciones en España: el impacto digital en los procesos de deliberación y participación ciudadana". *Mediaciones Sociales. Revista de Ciencias Sociales y de la Comunicación,* nº7, segundo semestre, pp. 143-169. Universidad Complutense de Madrid. https://produccioncientifica.ucm.es/documentos/5d399a19299952068445e98e

Ridaura Martínez, M.J. (2014) "La seguridad ciudadana como función del Estado". *Estudios de Deusto*. Vol. 62/2. Bilbao. Julio-diciembre. pp. 319-346. https://revista-estudios.revistas.deusto.es/article/view/259

Robles Carrillo, M. (2023). "La articulación de la soberanía digital en el marco de la Unión Europea". *Revista de Derecho Comunitario Europeo,* nº 75, pp. 133-171. https://www.cepc.gob.es/sites/default/files/2023-10/40196rdce7505robles-carrillo.pdf

Rubio Núñez, R (2000). "Internet en la participación política". *Revista de Estudios Políticos* (Nueva Época), nº 109, Julio-septiembre, pp. 285-302. https://webs.ucm.es/centros/cont/descargas/documento3949.pdf

— Rubio Núñez, R. (2018). "Los efectos de la posverdad en la democracia". *Revista de Derecho Político.* UNED. N.º 103. Septiembre-diciembre. pp. 191-228. https://revistas.uned.es/index.php/derechopolitico/article/view/23201

Serra Cristóbal, R. (2021) "De falsedades, mentiras y otras técnicas que faltan a la verdad para influir en la opinión pública". *Teoría y Realidad Constitucional*, núm.47. pp. 199-235. https://revistas.uned.es/index.php/TRC/article/view/30712

SHIRKY, C. (2011). "The Political Power of Social Media: Technology, The Public Sphere, and Political Change". *Foreign Affairs,* Vol. 9, nº1, enero-febrero. pp. 28-41. https://www.jstor.org/stable/25800379

Simons, J., y Ghosh, D. (2020). "Utilities for Democracy: Why and How the Algorithmic Infrastructure of Facebook and Google must be Regulated". *Brookings Institution,* pp. 1-28. https://www.brookings.edu/wp-content/uploads/2020/08/Simons-Ghosh_Utilities-for-Democracy_PDF.pdf

Tajadura Tejada, J. (2004). "¿El ocaso de Westfalia? Reflexiones en torno a la crisis del constitucionalismo en el contexto de la mundialización". *Revista de Estudios Políticos* (nueva época), nº 123, enero-marzo. pp. 315-349.

Teruel Lozano, G. (2023). "Libertad de expresión, censura y pluralismo en las redes sociales: algoritmos y el nuevo paradigma regulatorio europeo", en BALAGUER CALLEJÓN, F., y COTINO HUESO, L. (Coord.), *Derecho Público de la Inteligencia artificial*. Zaragoza. Fundación Giménez Abad. pp. 181-222.

Torres del Moral, A. (2012) "Del Estado absoluto al supranacional e internacionalmente integrado". *Revista de Derecho Constitucional Europeo*. Año 9. Nº 18. Julio-diciembre. pp. 19-41. https://www.ugr.es/~redce/REDCE18/articulos/01_TORRES_MORAL.htm

Vallès, J.M. (1990). "Proceso electoral, comportamiento electoral y sistema político". *Revista del Centro de Estudios Constitucionales,* nº 5, enero-marzo. https://www.cepc.gob.es/sites/default/files/2021-12/35348rcec05187.pdf

Vázquez Alonso, V. (2020). "Twitter no es un foro público pero el perfil de Trump sí lo es. Sobre la censura privada *de* y *en* las plataformas digitales en los EE.UU." *Estudios de Deusto.* Vol. 68/1. Enero-junio.pp. 475-508. https://revista-estudios.revistas.deusto.es/article/view/1832

Vidal Prado, C. (2022). "La educación cívica como herramienta para construir y fortalecer la democracia y el Estado de derecho". *Revista General de Derecho Público Comparado,* nº32, diciembre. https://portalcientifico.uned.es/documentos/63d0849ff0be5d2a9f2da349

Villaverde Menéndez, I. (2020). *Los poderes salvajes: ciberespacio y responsabilidad por contenidos difamatorios.* Madrid. Marcial Pons.

Vosoughi *et al.,* (2018). "The Spread of True and False News Online". *Science, nº* 359, pp. 1146-1151. https://www.science.org/doi/full/10.1126/science.aap9559

Title
The European Digital Service Act and the defence of Democracy

Summary

I. Introduction. II. The Digital Service Act. III. Large digital companies and systemic risks. IV. Defending democracy. a) Protecting civic discourse, b) Protecting electoral processes, c) Protecting public security, d) Risk reduction measures. V. Conclusions. VI. Bibliography.

Resumen

El mes de febrero de 2024 comenzó la aplicación, en toda su extensión, del Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). Una disposición que tiene como objetivo actualizar el marco jurídico que regula la actuación de las compañías que prestan servicios intermediarios en línea en todos los Estados miembros de la Unión.
La actualidad del Reglamento ha despertado un gran interés en la doctrina sobre la adecuación del régimen de responsabilidad diseñado, y su comparación con el régimen anterior, así como el abordado en diferentes países —sobre todo Estados Unidos—. No obstante, resulta necesario analizar la nueva disposición desde la problemática que plantea el control del poder privado y sus posibles incidencias en un régimen democrático constitucional. La aparición de nuevas empresas multinacionales de enorme influencia cuyos servicios resultan, en muchos casos, esenciales —tanto desde el punto de vista comercial como democrático— ha puesto de manifiesto la necesidad de reformular el mínimo régimen de responsabilidad que les venía siendo aplicable. El Reglamento de Servicios Digitales prevé la posibilidad de que el diseño, uso y funcionamiento de los servicios intermediarios en línea pueda entrañar una serie de riesgos sistémicos que afecten a los regímenes constitucionales de los Estados miembros. Unos riesgos que el legislador europeo agrupa en torno a cuatro categorías.
En esa línea, el presente artículo analiza el tercero de dichos riesgos sistémicos, concretamente, el contenido en el artículo 34.1 apartado (c), relativo a "cualquier efecto negativo real o previsibles sobre el discurso cívico y los procesos electorales, así como sobre la seguridad pública".
Para ello, la investigación realiza, en un primer lugar, (II) un análisis general del propio Reglamento, seguido de (III) una presentación de las grandes compañías como categoría autónoma y de los riesgos sistémicos que establece la Unión. El tercer apartado (IV) se centra en la defensa de la democracia subsumida en el tercero de los riesgos, analizando los conceptos de "discurso cívico", "proceso electoral" y "seguridad pública", para tratar de identificar algunos de los potenciales riesgos a los que se enfrenta cada uno de ellos en el entorno digital y las medidas de atenuación que brinda el Reglamento. Un estudio que conduce a una serie de (V) conclusiones

entre las que destaca la idea de que, si bien es cierto que los esfuerzos acometidos por la nueva regulación apuntan en buena dirección, será precisa la colaboración de las propias compañías y un férreo control por parte de las autoridades nacionales que garanticen su observancia.

Abstract

In February 2024, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (the Digital Services Act) entered into application in its entirety. This provision aims to update the legal framework governing the activities of companies providing online intermediary services in all EU Member States.

The topicality of the Regulation has aroused great interest in the doctrine on the adequacy of the liability regime designed, and its comparison with the previous regime, as well as that of different countries —especially the United States—. However, it is necessary to analyse the new provision from the perspective of the problems posed by the control of private power and its possible effects on a constitutional democratic regime. The emergence of new highly influential multinational companies whose services are, in many cases, essential — both commercially and democratically — has highlighted the need to reformulate the minimal liability regime that had been applicable to them. The Digital Services Act foresees the possibility that the design, use and operation of online intermediary services may entail a number of systemic risks affecting Member States' constitutional regimes. These risks are grouped by the European legislator into four categories.

This article analyses the third of these systemic risks, specifically, that contained in Article 34.1 (c), relating to "any actual or foreseeable negative effects on civic discourse and electoral processes, and public security".

To this end, the research first provides (I) a general analysis of the DSA itself, followed by (II) a presentation of large companies as an autonomous category and of the systemic risks established by the EU. The third section (III) focuses on the defence of democracy subsumed under the third of the risks, analysing the concepts of "civic discourse" and "electoral process", in an attempt to identify some of the potential risks faced by each of them in the digital environment, and the mitigation measures provided by the DSA. This study leads to a series of (IV) conclusions, including the idea that, although it is true that the efforts undertaken by the new regulation point in the right direction, the collaboration of the companies themselves and a strict control by the national authorities to ensure compliance, will be necessary.

Palabras clave

Reglamento de Servicios Digitales; Riesgos sistémicos; Democracia; Discurso cívico; Procesos electorales.

Keywords

Digital Services Act; Systemic risks; Democracy; Civic discourse; Electoral processes.