

Control de la desinformación en Europa a la luz de la Ley de Servicios Digitales de la UE (DSA) (1)

Monitoring disinformation in Europe under the EU Digital Services Act (DSA)

La desinformación viene siendo uno de los retos a los que se enfrentan nuestras democracias hoy en día, pues, entre otras cosas, las campañas de desinformación pretenden la construcción de un relato público interesado y no veraz. Estas campañas se difunden especialmente a través de las grandes plataformas digitales y su colaboración se vuelve necesaria para luchar contra el fenómeno de la desinformación. Este trabajo analiza como la nueva Ley de Servicios Digitales (DSA) viene a crear un nuevo paradigma sobre la regulación de la actuación de dichas plataformas y los contenidos que en ellas se almacenan o transmiten. Se analiza el papel que la ley europea otorga a las diferentes plataformas digitales en lo que refiere a la moderación de contenidos susceptibles de generar desinformación. Asimismo, se pone de manifiesto los riesgos que a su vez genera el tratar de eliminar del debate público determinadas ideas porque se entienda que son falsas o tergiversadas.

Ley de Servicios Digitales, DSA, moderación de contenidos, contenidos digitales, desinformación, noticias falsas, bulos, debate público, opinión pública, discurso público, monitorización de contenidos digitales, plataformas digitales.

Disinformation is one of the challenges facing our democracies nowadays. Among other things, disinformation campaigns aim to construct a self-serving and untruthful public narrative. These campaigns are spreading especially through large digital platforms and their collaboration is necessary to fight against the phenomenon of disinformation. This paper analyses how the new Digital Services Act (DSA) creates a new paradigm for regulating the actions of these platforms and the content stored or transmitted on them. It analyses the role that the European law gives to the different digital platforms with regard to the moderation of contents that generate disinformation. It also highlights the risks involved in trying to remove certain ideas from public debate because they are understood to be false.

Digital Services Act, DSA, content moderation, digital content, disinformation, fake news, hoaxes, public debate, public opinion, public narrative, digital content monitoring, digital platforms.



Rosario Serra Cristóbal (2)

Catedrática de Derecho Constitucional

Universitat de València

1. EL DEBATE PÚBLICO EN LA RED. CONTROLAR EL DISCURSO

A mitad de octubre de 2023, la Comisión Europea anunció que iniciaba investigaciones sobre desinformación en las redes sociales propiedad de X (anteriormente Twitter), Meta (Facebook e Instagram) y TikTok relacionada con contenidos relativos a la guerra que enfrenta a Israel con Hamás en la Franja de Gaza. Y, el 18 de diciembre de ese año la Comisión finalmente comunicó que se abría un procedimiento formal contra X por posibles incumplimientos de las exigencias de la normativa europea de servicios digitales (3).

Esta no es más que una de las consecuencias prácticas de la aplicación del nuevo Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales, conocido como Ley de Servicios Digitales o DSA, por sus siglas en inglés, y que entró en vigor el 25 de agosto de 2023 para las grandes plataformas y el 24 de febrero de 2024 para el resto. La compañía X aseguró que había borrado cientos de cuentas vinculadas a Hamás, pero se mostró reacia a un exceso de moderación de contenidos, indicando que un buen sistema para evitar la desinformación y la manipulación era colocar avisos y notas públicas tras las publicaciones, además de «limitar las interacciones» de ese contenido a través de la alteración del algoritmo. A su parecer, estas acciones «están destinadas a limitar el alcance de la publicación mientras se mantiene la capacidad del público para verla y discutirla» (4).

Sin duda, se abren interesantes interrogantes. La DSA establece un nuevo modelo de regulación de los contenidos que circulan en la red a través de las plataformas digitales. Busca proteger a los usuarios de los contenidos ilegales, la desinformación y la publicidad engañosa, para lo que establece una serie de requisitos de diligencia a estas plataformas, que van desde la eliminación de

contenidos de desinformación o ilícitos a la necesidad de adoptar medidas preventivas contra la circulación de tales contenidos o el cumplimiento de reglas de transparencia (5) en cuanto a sus algoritmos, prácticas comerciales o el impacto de sus actuaciones (6) . Nos encontramos ante un nuevo paradigma en la Unión Europea sobre la regulación de la actuación de las plataformas digitales que ofrecen servicios en la Unión y los contenidos que se almacenan o distribuyen en las mismas.

Como decíamos, el caso de la circulación de relatos sobre el terrible conflicto en Gaza en las plataformas no ha hecho más que abrir el debate acerca de la responsabilidad de las compañías digitales respecto de los contenidos digitales, las facultades de la UE para ordenar o controlar actuaciones de estas empresas respecto de los mismos o sobre qué medidas son las óptimas para garantizar la seguridad y la ausencia de desinformación en la red, entre otras. Pero, sobre todo, uno de los grandes interrogantes en torno al cual ya se había debatido es, en definitiva, las consecuencias que todo ello puede tener sobre el control del discurso público, esto es, como esa moderación de contenidos (7) puede influir en la conformación del relato colectivo. Porque las campañas de desinformación no suelen limitarse a la difusión de noticias falsas sin más, sino que normalmente pretenden la construcción de un relato público interesado y no veraz.

No es la primera vez que la UE adopta medidas limitadoras de la circulación de contenidos informativos por considerar el carácter desinformador de los mismos

No es la primera vez que la UE adopta medidas limitadoras de la circulación de contenidos informativos por considerar el carácter desinformador de los mismos. Antes de que la DSA entrara en vigor, durante la pandemia por Covid-19, ya se establecieron restricciones para evitar la difusión de bulos. Y, posteriormente, en 2022, como respuesta a las noticias falsas difundidas por el Gobierno ruso en las cadenas *Sputnik* y *Russia Today* y la manipulación informativa sobre las razones de la invasión de Ucrania o la difusión de datos falsos sobre dicha campaña bélica, los países de la UE acordaron en el Consejo de la UE el cierre de las emisiones de estas cadenas rusas en su territorio, alegando que estaban siendo utilizados como instrumentos de desinformación (8) . A continuación, Google y YouTube anunciaron que procederían de igual modo. Esa medida sin precedentes suscitó críticas por lo que el hecho de la cancelación de un medio de comunicación supone para la misma democracia.

En el fondo late la realidad de determinar qué ideas o informaciones pueden circular por las redes y llegar a millones de usuarios y cuáles deben quedar proscritas por ilegales o por producir desinformación. Recordemos que el flujo de opiniones y contra opiniones contribuyen a la construcción de una opinión pública diversa sobre aquellas cuestiones que interesan a todos (9) . Sin las libertades de expresión e información no cabe una participación ciudadana libre e informada que permita conformar una opinión pública con una mínima calidad (10) . Para que esa generación de

opinión pública cumpla con los estándares que la democracia exige es necesario que la misma esté conformada sobre unos mínimos conocimientos de los hechos acaecidos, de las opciones/alternativas que existen, por muy radicales que estas puedan sonar, de las consecuencias de las diferentes opciones, etc., porque la democracia se asienta sobre un debate público, plural e informado. Esta libre circulación de la información en redes favorece una «opinión pública libre».

Lo lamentable es que, aunque los medios digitales ofrecen más oportunidades de acceder a la información y de difundir ideas, llegando a muchísima más gente que lo hacían los medios tradicionales, su uso también ha traído resultados perversos. Y es que, como ya advirtiera el Tribunal Europeo de Derechos Humanos, «la posibilidad de que los individuos se expresen en internet constituye una herramienta sin precedentes para el ejercicio de la libertad de expresión. Se trata de un hecho indiscutible. Sin embargo, las ventajas de este medio van acompañadas de una serie de riesgos. Contenidos claramente ilícitos, incluido el difamatorio, odioso o violento, pueden difundirse como nunca antes por todo el mundo en cuestión de segundos, y a veces permanecer en línea durante mucho tiempo» (asunto *Times Newspapers Ltd. c. Reino Unido*, 2009, FJ 27). A lo que habría que añadir el riesgo aún mayor que la red supone para la difusión de bulos y los daños que ello puede generar a las personas y al normal funcionamiento de la democracia.

Por un lado, esa enorme capacidad de difusión y amplificación de contenidos que circulan a través de las redes ha sido aprovechada para analizar, mediante algoritmos, el consumo de noticias de la población, haciendo uso del rastro digital que los usuarios dejan en internet sobre sus gustos, tendencias, intereses, etcétera, y condicionando la información que cada cual recibe, haciéndoles llegar mensajes que confirman sus opiniones preexistentes y retroalimentando sus posiciones ideológicas (11). En todo caso, esta forma de actuar de las plataformas digitales, de alimentar el *feed* de los usuarios, ha venido a ser regulado de forma distinta desde la entrada en vigor de la DSA, pues este no podrá ser solo personalizado. Algunas plataformas ya lo han desplegado, como X, Facebook, Instagram o TikTok, ofreciendo un espacio con mensajes no personalizados ordenados cronológicamente, minorando ese efecto de retroalimentar el *feed* de cada usuario solo con la información que le gusta.

Y, por otro lado, esta tecnología digital ha sido usada, como decíamos, para desinformar (al igual que para expandir otros mensajes perniciosos como los xenófobos o discriminadores). La desinformación ha encontrado en el mundo digital un campo abonado para hacer crecer los mensajes que faltan a la verdad mediante el uso de herramientas como los *spammers* (12) u otro tipo de técnicas de comunicación digital. En internet se ha observado una tendencia al alza en el uso de las técnicas de la mentira o la ficción por parte de cualquier persona o entidad, pero, especialmente por determinados líderes, partidos o movimientos políticos que libran una batalla por controlar la percepción de la opinión pública sobre el poder, los hechos o las necesidades del pueblo; buscan adueñarse del relato público: puede ser el relato sobre el origen o la gestión de la pandemia (13), los resultados de unas elecciones, la crisis climática (14), la justificación de una guerra, la responsabilidad de cualquier problema social u otras cuestiones, lo importante es influir en el parecer de la ciudadanía. Y esos contenidos falsos pueden acabar conduciendo: a la radicalización y polarización de la ciudadanía (15); a condicionar unos resultados electorales; a la discriminación u

odio hacia determinados colectivos o ciudadanos; a generar falsos prejuicios hacia determinadas medidas sanitarias, sociales o económicas (16) ; al desgaste o exaltación de la imagen de un personaje público o un grupo político; al rechazo de determinados productos en el mercado, etc.

La propia seguridad interna de un Estado puede verse afectada. Como recordaba Cristina Pauner (17) , las campañas masivas de desinformación han sido utilizadas por agentes externos para sembrar la desconfianza y crear tensiones sociales en diversos Estados, en muchas ocasiones minando la credibilidad del discurso oficial, intentando influir en procesos electorales (18) o desestabilizando instituciones. Piénsese en la campaña de desinformación que fue orquestada desde las filas del partido republicano, alimentada con los mensajes falsos emitidos por la cuenta personal de Donald Trump, y que condujo al asalto violento al Capitolio estadounidense en enero de 2021.

Como decíamos al comienzo, el terrible ataque terrorista de Hamás y la descomunal y desproporcionada reacción de Israel en territorio palestino han vuelto a poner de manifiesto la capacidad que la (des)información tiene de influir en el imaginario colectivo, condicionando o potenciando el sentimiento colectivo de cualquier persona sobre las actuaciones de unos y otros. El conflicto entre Israel y Hamas ha demostrado de nuevo cómo las redes pueden ayudar a escribir una historia u otra.

Ese poder de la información (y la desinformación) en las redes seguirá siendo utilizado con fines interesados en una y mil coyunturas. De hecho, se planteaba Harari cómo esa capacidad de las redes y el uso de la inteligencia artificial puede influir en las elecciones estadounidenses de 2024 (19) . Todos sabemos que la información desempeña un papel vital en la construcción de relatos. El sentir de la opinión pública y lo que quedará escrito en el imaginario colectivo viene condicionado por lo que se transmite públicamente. Y las redes constituyen ese nuevo espacio donde se monta la narrativa de lo que sucede.

Controlar todo ello es tremendamente complejo por los riesgos que a su vez genera la eliminación del debate público de determinadas ideas porque se entienda que son falsas o tergiversadas. No hemos de perder de vista que con la moderación de contenidos que la normativa europea regula se corre el riesgo de perjudicar a uno de los elementos básicos de la democracia: el libre flujo de ideas y hechos noticiables del que hablábamos más arriba. La propia DSA es consciente de ello, por lo que tendremos que ser cautos.

2. LA DESINFORMACIÓN VIGILADA DESDE HACE AÑOS EN EUROPA

Por las razones expuestas, desde hace años, la desinformación viene siendo vigilada con honda preocupación. De ahí que tanto Gobiernos como instituciones supranacionales (entre ellas la Unión Europea) estén en alerta y hayan adoptado medidas para luchar contra ella.

Sin duda, para abordar la nueva regulación de la DSA en lo que refiere al control de contenidos desinformadores que circulan en las plataformas digitales, es necesario hacer un repaso, aunque sea somero, de cómo ha sido abordado el fenómeno de la desinformación en estos años.

2.1. La lucha contra la desinformación desde el ámbito estatal

2.1.1. Los planes estatales de seguridad. El caso de España

El desorden informativo al que nos referimos fue percibido como algo tan preocupante, que muchos estados europeos se apresuraron a incluir la desinformación en sus planes de seguridad. En el caso de España, el Informe Anual de Seguridad Nacional de España de 2019 señalaba que «especial mención merecen las amenazas híbridas, uno de cuyos componentes es la desinformación, que mediante la manipulación de la información a través de Internet y las redes sociales provoca la polarización y radicalización de la ciudadanía». Se definía, por tanto, la desinformación como un ingrediente de las amenazas híbridas. Ahondando en esa realidad, la Estrategia de Seguridad Nacional de 2021 incluyó por primera vez las campañas de desinformación como uno de los retos que desafían a España, porque, tal como se indica en la misma, producen inestabilidad, tienen la voluntad de generar confusión y socavar la cohesión social, pretenden erosionar las instituciones o influir en los procesos democráticos y alientan la polarización (20). Y en el Informe Anual de Seguridad Nacional de 2022 volvía a hacerse hincapié en la amenaza que para la seguridad nacional suponen las campañas de desinformación.

Al considerarse la desinformación como reto o como una amenaza para la seguridad nacional, son los cuerpos de seguridad, defensa o inteligencia los que, en la gran mayoría de los Estados, se han encargado de desarrollar programas de prevención, concienciación y control de este tipo de mensajes falsos. Así, por ejemplo, Francia creó en 2021 una unidad permanente dentro de la Secretaría General de Defensa y Seguridad Nacional (21) para analizar y detectar campañas de desinformación e identificar sus fuentes (22). Volviendo al caso de España, desde 2013 se cuenta con un organismo responsable de combatir las noticias falsas, el Consejo Nacional de Ciberseguridad, que fue instituido fundamentalmente para evitar los ciberataques, pero se le encomendó provisionalmente la misión de detectar y contrarrestar las campañas de desinformación. En 2019 se creó la Comisión Permanente contra la desinformación, grupo de trabajo interministerial, dirigido por el Departamento de Seguridad Nacional y creado con el objeto de establecer mecanismos de coordinación permanente entre los diferentes órganos de la Administración. El 30 de octubre de 2020 se dio un paso más adoptándose la Orden ministerial PCM/1030/2020, por la que se publicaba el Procedimiento de actuación contra la desinformación, aprobado por el Consejo de Seguridad Nacional, que refiere a la realización de actuaciones de monitorización y vigilancia (detección, alerta temprana, notificación y análisis) con el objetivo de detectar campañas de desinformación y su análisis ante su posible impacto en la seguridad nacional, así como como para el apoyo en la gestión de situaciones de crisis (como el caso de la Covid-19) donde pudiera haber una afectación derivada de dichas campañas. Sin embargo, se trataba de una orden meramente enunciativa, que hacía un esbozo de la estructura orgánica de actuación frente a la desinformación, sin aludir a una regulación más precisa y sin hacer ninguna referencia a las garantías que, respecto de los derechos a la libertad de expresión, de información, de privacidad o de autodeterminación informativa, deberían adoptarse. No hace falta recordar que lo relativo a esa posible limitación de derechos fundamentales y las garantías que, en su caso, hubiera que establecer, ello debería recogerse en una norma con rango de ley y de carácter orgánico y tendría que atender a las previsiones constitucionales.

2.1.2. Adopción de medidas legislativas para hacer frente al fenómeno de la desinformación

En España se han presentado varias proposiciones no de ley sobre desinformación y noticias falsas de las que se deduce el vínculo con la seguridad, aunque todas ellas han resultado fallidas (23) . Otros Estados sí han alcanzado algún avance legislativo en esta materia, aunque aún la regulación es escasa (24) . Por poner un ejemplo, **Alemania** adoptó la **Ley sobre la mejora de la aplicación de la ley en las redes sociales**, de 1 de septiembre de 2017 (*Netzdurchsetzungsgesetz*, conocida como *NetzDG*), que obliga a borrar determinados contenidos que afecten a derechos fundamentales en un plazo de 24 horas y contempla multas para las redes sociales si se oponen a borrar de sus plataformas mensajes *fake* (al igual que los que inciten al odio). Esta Ley fue reformada por la Ley de 3 de junio de 2021 (*Gesetz zur Änderung des Netzdurchsetzungsgesetzes*), estableciéndose la obligación de las empresas de incluir mecanismos de recurso más garantistas cuando se produzca la moderación de un contenido, al tiempo que incluyó nuevas vías, más allá de las multas, para obligar a las compañías digitales a cumplir con las previsiones de la ley, e igualmente recogió nuevas obligaciones de transparencia para tales empresas.

Francia aprobó la **Ley n.º 2018-1202, de 22 de diciembre de 2018 (conocida como Avia Law)**, que, entre otras cosas, introducía mecanismos para advertir y suspender emisiones de noticias falsas en los prolegómenos o durante un proceso electoral. Está facultad fue atribuida al *Conseil supérieur de l'audiovisuel*. Este podía avisar y obligar a que los medios dejaran de emitir si consideran que estaban bajo órdenes o influencia de un Estado extranjero que estuviera actuando contra los intereses fundamentales de la Nación, en particular mediante la difusión de información falsa. También cualquier partido, candidato o persona podía acudir a un juez especial único en Francia para solicitar que se retirase una información difundida de forma automática on-line que fuese inexacta o engañosa y que pudiera afectar a las elecciones. De todos modos, el Consejo Constitucional Francés en 2020 declaró que la norma presentaba serias dudas de constitucionalidad. En todo caso, el art. L97 del Código Electoral francés ya penalizaba la difusión de información falsa para inducir a los electores a no participar en las elecciones o para tratar de influir de alguna forma en el sentido del voto de los ciudadanos. Aun así, en 2022 un grupo de expertos debatió la posibilidad de establecer legalmente una responsabilidad penal por la diseminación de información falsa online realizada con mala fe y que trajera aparejadas malas consecuencias para individuos o la colectividad (25) .

También en junio de 2018, en el Reino Unido, la Comisión Electoral Británica pidió una mayor transparencia para los votantes con respecto a la práctica de las campañas electorales digitales, haciendo recomendaciones sobre la responsabilidad, el gasto y la transparencia: *Digital campaigning. Increasing transparency for voters* (26) .

Merece igualmente mención la ley austriaca que se aprobó en enero de 2021, la **Ley de plataformas de comunicación, Kommunikationsplattformen-Gesetz (KoPI-G)**, que buscaba controlar contenidos ubicados en los servicios de las plataformas digitales de comunicación, aunque lo cierto es que se centró más en control de mensajes propiamente ilegales, como los que generan discurso del odio, que en el control de la desinformación (27) . De hecho, solo prohíbe la desinformación en contados casos y bajo determinadas circunstancias. Otra muestra de que el objetivo principal de la ley no es el control de la desinformación la encontramos en el hecho de que, para referirse a esta normativa, se utiliza la expresión «hate-speech package» en lugar del término «disinformation law». Lo

interesante es que se trata de una ley que se adoptó teniendo en cuenta las previsiones de la DSA, que acabaría adoptándose un año después. La ley austriaca obliga a los prestadores nacionales y extranjeros de plataformas de comunicación a establecer mecanismos de declaración y verificación de los contenidos potencialmente ilícitos. Precisamente esto fue recurrido por Google Ireland, Meta Platforms Ireland y TikTok, tres plataformas establecidas en Irlanda, que alegaron que la ley austriaca era contraria al Derecho de la Unión, concretamente a la Directiva relativa a los servicios de la sociedad de la información. El Tribunal de Justicia de la UE respondió que aunque es cierto que, en condiciones estrictas y en casos específicos, los Estados miembros distintos del Estado miembro de origen del servicio en cuestión pueden adoptar efectivamente medidas para garantizar el orden público, la protección de la salud pública, la seguridad pública o la protección de los consumidores, esos Estados (Austria) distintos al de origen (Irlanda), no pueden adoptar medidas de carácter general y abstracto aplicables indistintamente a cualquier prestador de una categoría de servicios de la sociedad de la información. Si el Estado miembro de destino (en este caso, Austria) estuviera autorizado a adoptar dichas medidas, se estaría usurpando la competencia reglamentaria del Estado miembro de origen (en este caso, Irlanda). Por otra parte, ello socavaría la confianza mutua entre los Estados miembros y violaría el principio de reconocimiento mutuo. Además, las plataformas afectadas estarían sometidas a legislaciones diferentes, lo que también vulneraría la libre prestación de servicios y, por tanto, el buen funcionamiento del mercado interior (STJUE C-376/22, asunto *Google Ireland y otros*, de 16 de noviembre de 2023).

En todo caso, en la DSA, respecto de esa normativa nacional, señala que «Los Estados miembros no deben adoptar ni mantener otros requisitos nacionales relativos a las materias comprendidas en el ámbito de aplicación del presente Reglamento, a menos que este prevea expresamente tal posibilidad, ya que ello afectaría a la aplicación directa y uniforme de las normas plenamente armonizadas aplicables a los prestadores de servicios intermediarios de conformidad con los objetivos del presente Reglamento. Lo anterior no debe excluir la posibilidad de aplicar otras normas de Derecho nacional aplicables a los prestadores de servicios intermediarios» (Considerando 9), cuando persigan objetivos relativos a la protección del orden público, seguridad pública y la defensa nacional, de los consumidores o persecución del delito o el discurso del odio. Con lo cual, todas estas normas deberán ser revisadas a la luz del nuevo Reglamento europeo.

2.2. La lucha contra la desinformación desde la UE

Lo que es evidente es que la lucha contra la desinformación es una batalla que ha de librarse no solo en cada Estado, sino también en la esfera supranacional, pues este fenómeno utiliza principalmente internet y las redes sociales como vía de difusión, y estas operan ajenas a las fronteras nacionales. Por ello, pronto surgieron iniciativas supranacionales de cooperación y lucha contra la desinformación. En el marco de la UE, esa lucha se ha encauzado a través de varias acciones cuyos primeros hitos fueron: la adopción en 2016 de un *Marco común de lucha contra las amenazas híbridas*, entre las que se encuentra la desinformación; el *Código de buenas prácticas en materia de desinformación* de 2018, —una medida de autorregulación para garantizar una mayor transparencia de las plataformas en línea y mejorar las políticas de estas en materia de desinformación—, y del *Plan de lucha contra la desinformación* también de 2018.

En marzo de 2019, se creó un *Sistema de Alerta Rápida* (RAS) con puntos de contacto nacionales para alertar instantáneamente sobre campañas de desinformación a través de una infraestructura tecnológica específica y para intercambiar información entre los Estados miembros y la Unión. Este Sistema asegura la necesaria coordinación entre los socios europeos y facilita tanto la monitorización de las redes para detectar campañas y acciones de desinformación como, eventualmente, el diseño de respuestas comunes cuando resulte necesario.

En 2000 se aprobó la *Directiva de Comercio Electrónico* (28), estableciendo el marco jurídico fundamental para los servicios en línea en la UE, que establecía requisitos de transparencia e información para los proveedores de servicios en línea y recogía la regla de la irresponsabilidad de los prestadores de servicios digitales por los contenidos en línea que gestionan, mientras no conocieran de su ilicitud, aunque necesitaban eliminarlos o deshabilitar el acceso a los mismos lo más rápido posible una vez que fueran conscientes de su naturaleza ilícita (29).

En 2020 cabría hacer alusión a que la Comisión Europea, en la nueva Estrategia de Seguridad de la Unión 2020-25 (24 de junio de 2020), hacía hincapié en la lucha contra «las campañas de desinformación y la radicalización de la narrativa política» (30).

En junio de 2022 se llevó a cabo una revisión del Código de buenas prácticas para reforzarlo, teniendo en cuenta las enseñanzas extraídas de la desinformación durante la crisis de la Covid-19 y la guerra de agresión de Rusia a Ucrania, —*The Strengthened Code of Practice on Disinformation 2022*—. El *Código reforzado de buenas prácticas contra la desinformación* busca: impedir que los actores que difundan información falsa puedan obtener ingresos publicitarios y garantizar la transparencia sobre los contenidos que difunden publicidad política; asimismo, busca proporcionar una mayor claridad sobre el funcionamiento de los algoritmos y permitir la verificación por terceros; hacer que resulte más fácil para los usuarios encontrar y acceder a fuentes distintas de noticias; introducir medidas para identificar y cerrar cuentas falsas; poner a disposición de los usuarios, investigadores y otros colectivos herramientas de denuncia en caso de hallar noticias falsas (31). En todo caso, no podemos dejar de reconocer que se trata de medidas de *soft law* «para todos los que voluntariamente se hayan adherido», pero no incluye mandatos legislativos imperativos. Así, a este Código se han adherido hasta la actualidad 44 plataformas digitales, entre ellas, Microsoft, TikTok, Google, o Meta, pero, por ejemplo, la red X, aunque inicialmente lo firmó, posteriormente lo abandonó.

Por último, hay que resaltar que ese mismo año 2022, se alcanzó un hito normativo muy significativo, que fue la aprobación de la Ley de Servicios Digitales-DSA (32), citada más arriba y objeto principal de nuestro estudio, y que contiene previsiones más avanzadas, entre otras cosas, en la cuestión de las responsabilidades de los servicios digitales y la protección de los derechos fundamentales de los usuarios en línea frente a contenidos o servicios ilegales o susceptibles de generar desinformación. Esta norma ha venido a hacer una revisión de la Directiva de Comercio electrónico más de 20 años después, teniendo en cuenta los nuevos desafíos y cambios que ha experimentado la realidad digital. Además, ha de subrayarse que se trata de un Reglamento y, por lo tanto, de directa y obligada aplicación.

En resumidas cuentas, la prioridad para la UE ha sido siempre, y más ahora con la DSA, la de establecer un marco uniforme entre todos los Estados en el control de los contenidos digitales. De ahí que el 18 de octubre de 2023 la Comisión Europea adoptara una *Recomendación sobre la lucha contra la desinformación y difusión de contenidos ilegales en el contexto de la DSA y tiempos de conflicto*, invitando a los Estados Miembros a anticipar la cooperación y coordinación de actuaciones para la implementación de la DSA (33).

3. LAS PREVISIONES DE LA DSA EN MATERIA DE DESINFORMACIÓN

El modelo de la UE sobre la responsabilidad de aquellas empresas intermediarias y plataformas prestadoras de servicios digitales por los contenidos que circulan o se almacenan en sus plataformas ha sido la de no exigirles responsabilidad por tales contenidos, excepto que estas tuvieran conocimiento de la existencia de tal ilícito. Por lo tanto, cuando se constata que, por alguna vía, son conocedoras de la existencia de contenidos ilícitos en sus plataformas, surge la obligación de actuar. Así se estableció en la Directiva de Comercio electrónico de 2000 y se ha recogido en la DSA (arts. 4, 5 y 6 DSA).

Esa respuesta ha de ser mucho más tenaz y rápida cuando los contenidos digitales van relacionados con contenidos ilegales, esto es, terroristas, xenófobos, delitos de odio, ciberdelincuencia, abuso y explotación de la infancia, o de protección intelectual, pues junto a estas normas, son de aplicación otras que contienen previsiones muy claras al respecto. Pongamos como ejemplo, el *Código de Conducta para la lucha contra la incitación ilegal al odio en internet* de 2016 o el *Reglamento (UE) 2021/784, del Parlamento Europeo y del Consejo, de 29 de abril de 2021, sobre la lucha contra la difusión de contenidos terroristas en línea*.

Sin embargo, las previsiones normativas respecto de los contenidos que denominamos de desinformación, —la información falsa o errónea—, parecen recoger una responsabilidad un tanto más laxa o atenuada para las plataformas digitales, o al menos un poco más difícil de exigir. De hecho, la DSA en los considerandos refiere reiterada y profusamente al fenómeno de la desinformación, estableciendo las mismas previsiones que cuando se está ante los «contenidos ilícitos», y hace referencia reiterada a las campañas de desinformación y la manipulación de contenidos. Pero luego, en el articulado, no cita expresamente el fenómeno de la desinformación como tal, no utiliza este término, ni habla de bulos o contenidos desinformadores o falsos o cualquier otro tipo de expresión similar. Sí es cierto que cuando alude en el art. 3 a la «moderación de contenidos», habla de «detectar, identificar y actuar contra contenidos ilícitos o información incompatible con sus condiciones generales». Y dice que esa moderación podrá suponer, «por ejemplo, la adopción de medidas que afecten a la disponibilidad, visibilidad, y accesibilidad de dicho contenido ilícito o de dicha información, como la relegación, la desmonetización de la información, el bloqueo de esta o su supresión, o que afecten a la capacidad de los destinatarios del servicio de proporcionar dicha información, como la supresión o suspensión de la cuenta de un destinatario del servicio». También el art. 34 DSA habla de «la amplificación y la difusión potencialmente rápida y amplia de contenido ilícito y de información incompatible con sus condiciones generales».

Por lo tanto, la desinformación hemos de asimilarla a ese tipo de contenidos que circulan o se almacenan en la red y son susceptibles de ser moderados, porque, además de lo que acabamos de indicar, a ello nos conducen claramente los considerandos del Reglamento que definen la intención del legislador comunitario. Así los efectos de la DSA, hay que entender por «contenidos ilícitos» aquellos contrarios a las normas comunitarias o estatales en aplicación del Derecho de la UE, entre ellos los que generen desinformación y con ello contravengan previsiones normativas comunitarias. No pueden considerarse contenidos ilícitos por desinformadores los que sean inocuos (por ejemplo, afirmar que la tierra es plana) o pudieran ampararse dentro de los márgenes de la libertad ideológica.

Lo que hace la DSA es establecer una regulación asimétrica, prevé diferentes tipos de obligación de diligencia respecto de los servicios y los contenidos ilícitos o susceptibles de generar desinformación que se ponen a disposición pública en la Red

Lo que hace la DSA es establecer una regulación asimétrica, prevé diferentes tipos de obligación de diligencia respecto de los servicios y los contenidos ilícitos o susceptibles de generar desinformación que se ponen a disposición pública (34) en la Red, obligaciones que además son de distinto tenor o grado para los servicios de intermediación, los servicios de alojamiento de datos, las plataformas en línea y las plataformas de muy gran tamaño (VLOPs) (35) . Así, aunque la DSA establece requisitos de diligencia desde los sitios web simples hasta a los servicios de infraestructura de internet y plataformas en línea, la mayor parte de las previsiones, especialmente las de mayor calado, van dirigidas a las plataformas en línea, singularmente a las VLOPs.

Las previsiones de la DSA pueden catalogarse sucintamente del siguiente modo:

3.1. Adopción de medidas con carácter coercitivo frente a contenidos ilícitos o de desinformación

Las medidas que con carácter coercitivo han de adoptar todas las empresas digitales a las que refiere el Reglamento son aquellas que consisten básicamente en el cumplimiento de forma inmediata de la orden de retirada o bloqueo de contenidos, suspensión de la prestación o cualquier otra medida que se les dirija por la autoridad judicial o administrativa competente, poniendo así fin a una infracción o impidiéndola, con la obligación adicional de su conservación del contenido por un tiempo determinado (art. 9.1 DSA).

Esos plazos de actuación pueden ser más breves por obligaciones derivadas, como decíamos anteriormente, del *Código reforzado de buenas prácticas contra la desinformación* o del *Código de Conducta para la lucha contra la incitación ilegal al odio en internet* de 2016, o del *Reglamento (UE) 2021/784, del Parlamento Europeo y del Consejo, de 29 de abril de 2021, sobre la lucha contra la difusión de contenidos terroristas en línea*, cuando el bulo que se esté difundiendo en internet pueda generar ese odio o sea un bulo que pueda ser considerado como contenido terrorista (36) .

Una vez cumplido el requerimiento por parte de la autoridad competente estatal o de la UE, los prestadores de servicios de alojamiento de datos informarán sin demora indebida a estas, mediante la plantilla establecida, de que se ha cumplido con la orden de retirada o bloqueo de página web o cualquier otra medida adoptada.

Por otro lado, ha de indicarse que esa obligación de actuar con prontitud de las plataformas digitales, retirando la información que haya almacenado o bloqueando el acceso a ella, surge también cuando el conocimiento del contenido ilícito o susceptible de generar desinformación proviene, no de una orden de una autoridad judicial o administrativa, sino de notificaciones realizadas o denunciadas por terceros (art. 5.1.e DSA). De hecho, el art. 16 de la DSA indica que «los prestadores de servicios de alojamiento de datos establecerán mecanismos que permitan que cualquier persona física o entidad les notifique la presencia en su servicio de elementos de información concretos que esa persona física o entidad considere contenidos ilícitos. Dichos mecanismos serán de fácil acceso y manejo, y permitirán el envío de notificaciones».

También el conocimiento de un contenido de desinformación puede provenir de su propia actividad prospectiva de búsqueda de bulos, esto es, que sean conocidas por los propios sistemas de detección de contenidos falsos que haya puesto en marcha la plataforma digital.

En todos esos casos, el mero conocimiento obliga a adoptar medidas coercitivas sobre los usuarios como protección general frente al uso indebido de las plataformas. Asimismo, deben suspender, durante un período razonable y después de una advertencia previa, la prestación de servicios a los destinatarios del servicio que proporcione con frecuencia contenidos manifiestamente ilícitos (art. 23.1 DSA). Por lo tanto, no basta con la mera transmisión puntual o anecdótica de un ilícito o hecho falso para entender que se está haciendo un uso indebido de la plataforma.

En todos los supuestos, para que se produzca la comunicación entre las autoridades judiciales o administrativas, de la UE o de los Estados, que permita la transmisión de las órdenes de moderación de contenidos o la adopción de cualquier medida a este respecto, se establece la obligación de las plataformas digitales de designar un Jefe de cumplimiento de la DSA o persona de contacto de las mismas con las autoridades de los Estados miembros, la Comisión Europea, el Consejo de Servicios Digitales y los destinatarios de los servicios que ofrezcan.

3.2. La notificación a la autoridad correspondiente de contenidos desinformadores

Con el fin de prevenir menoscabo a intereses particulares o generales, la DSA también prevé el establecimiento de cauces para que se pueda alertar a las autoridades de la existencia de contenidos ilícitos o de desinformación y puedan adoptarse las respuestas pertinentes, una obligación que va dirigida especialmente a los servicios de alojamiento, plataformas en línea y VLOPs, y no a los servicios intermediarios.

Existe así el deber de informar a las autoridades competentes (o al punto de contacto del Estado miembro de la Unión en que tengan su establecimiento principal o su representante legal) y, en su caso, a Europol cuando detecten contenidos ilícitos, especialmente cuando sean susceptibles de

constituir un delito (art. 18 DSA). En todo caso, atendiendo a la estricta literalidad de la DSA, resulta complicado determinar si existe esa obligación, o cuándo, de alertar a las autoridades del efecto desinformador de determinados contenidos, porque ello no queda reflejado de forma clara en la DSA y porque no siempre es fácil determinar el carácter desinformador de una noticia. Sobre esta idea volveremos más adelante.

3.3. La entrega de información o datos

Asimismo, las plataformas pueden estar obligadas a la entrega de información específica sobre uno o varios destinatarios individuales del servicio digital, orden que ha de ser dictada por la autoridad administrativa o judicial que hayan determinado los propios Estados o las propias de la UE (art. 10 DSA).

En la misma línea, el art 40 DSA obliga a los prestadores en línea de muy gran tamaño —VLOPs— o de motores de búsqueda en línea de muy gran tamaño —VLOSEs— a proporcionar datos al coordinador de servicios digitales de establecimiento o a la Comisión para hacer el seguimiento del cumplimiento del Reglamento y evaluarlo. Esa solicitud ha de hacerse de forma motivada y en un período razonable, especificado en la misma el acceso a los datos concretos que sean necesarios. Aunque el precepto subraya que los coordinadores de Servicios digitales y la Comisión utilizarán los datos teniendo en cuenta los derechos de los titulares de los mismos en lo que respecta a la protección de datos personales, la protección de la información confidencial y el mantenimiento de la seguridad del servicio, los riesgos de que estos derechos e intereses puedan ser dañados por esa cesión de datos es evidente.

3.4. Las actuaciones de carácter preventivo/prospectivo

3.4.1. Monitorización y búsqueda activa de contenidos susceptibles de generar desinformación

La DSA empieza indicando que «no se impondrá a los prestadores de servicios intermediarios ninguna obligación general de monitorizar la información que transmitan o almacenen, ni de buscar activamente hechos o circunstancias que indiquen la existencia de actividades ilícitas» (art. 8 DSA). Efectivamente, esa ha sido la regla general, pero ello no ha impedido, como decíamos anteriormente, que muchas empresas digitales, desde hace años, vengán adoptando voluntariamente actuaciones dirigidas a moderar los contenidos que circulan o se almacenan en sus plataformas. La misma DSA en el art. 7 refiere a esas investigaciones/controles realizados por iniciativa propia por las plataformas digitales, que tienen por objetivo detectar y retirar contenidos ilícitos o bloquear el acceso a ellos u otras medidas.

En concreto, el control sobre la desinformación ha sido una práctica llevada a cabo por las propias grandes corporaciones digitales de forma voluntaria, que han ido adoptando mecanismos para hacer un filtrado de noticias falsas a través de equipos de evaluadores o *fact-checkers* independientes (37) y eliminar o establecer una etiqueta de «posible *fake*» para aquellos mensajes que manifiestamente falten a la verdad. Este camino se emprendió en 2018 cuando Facebook, Google, Microsoft, Mozilla, Twitter y siete asociaciones comerciales europeas firmaron el *Código de buenas prácticas contra la desinformación*, al que nos referíamos más arriba. Igualmente, se han abierto sitios web que buscan detectar y hacer públicos bulos que circulan por las redes (*Maldita.es*, *Newtral*, *EFE Verifica*,

#StopBulos, Snopes, la Buloteca, Hoaxy, CazaHoax, FactCheck.org, ...).

Tenemos muchos ejemplos de este tipo de actuación voluntaria prospectiva llevada a término por grandes compañías de servicios digitales, pero alguna de estas actuaciones ha tenido especial repercusión pública e incluso ha recibido más de una crítica. Este es caso, en 2021, de las suspensiones temporales por Twitter de las cuentas de Vox (8 días), de Bolsonaro o del mismo Donald Trump. Sobre los riesgos que conllevan para la misma democracia los controles proactivos de este tipo hablaremos posteriormente.

3.4.2. Evaluar riesgos sistémicos y contribuir a su reducción

Pero, aunque se establezca en la DSA que «no se impondrá a los prestadores de servicios intermediarios ninguna obligación general de monitorizar la información que transmitan o almacenen, ni de buscar activamente hechos o circunstancias que indiquen la existencia de actividades ilícitas» (art. 8 DSA), sí se prevé alguna obligación en ese sentido en determinados casos y exclusivamente para los prestadores de plataformas en línea de muy gran tamaño —VLOPs— y de motores de búsqueda en línea de muy gran tamaño —VLOSEs—. Ciertamente, para ellas la DSA crea la obligación de adoptar ciertas medidas de carácter preventivo. Se trata de obligaciones consistentes en evaluar y contribuir a la reducción de determinados riesgos sistémicos a los que refiere la propia DSA. Esta considera, entre otros, como contenido con riesgo sistémico para la sociedad, el contenido que cree «cualquier efecto negativo real o previsible para el ejercicio de los derechos fundamentales, en particular [...] a la libertad de expresión e información, incluida la libertad y pluralismo de los medios de comunicación [...]» o «cualquier efecto negativo real o previsible sobre el discurso cívico y los procesos electorales, así como sobre la seguridad pública», esto es, que puedan dañar a la democracia, al igual que los que pongan en riesgo la salud pública o la seguridad (art. 34 DSA). Sin visos de duda, las campañas de desinformación constituyen uno de esos contenidos capaces de generar los daños sistémicos que se indican y, por lo tanto, serían susceptibles de ser controladas con ese fin preventivo.

La DSA establece para las plataformas de gran tamaño el deber de «detectar, analizar y evaluar con diligencia 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» (art. 34.1 DSA) o «de la manipulación intencionada de su servicio por la amplificación y la difusión potencialmente rápida y amplia de contenido ilícito y de información incompatible con sus condiciones generales» (art 34.2). Deben centrarse en los elementos que puedan contribuir a los riesgos que se derivan de la circulación de contenidos, **evaluando los riesgos sistémicos** a los que refiere la DSA. Puntualiza asimismo que dichos prestadores de servicios también deben centrarse en la información que no sea ilícita, pero que contribuya a esos riesgos sistémicos.

En concreto, respecto de la desinformación, el considerando 84 de la DSA indica que: «Por consiguiente, dichos prestadores deben dedicar especial atención a cómo se utilizan sus servicios para difundir o amplificar contenidos incorrectos o engañosos, incluida la desinformación. Cuando la amplificación algorítmica de la información contribuya a los riesgos sistémicos, dichos prestadores

deben reflejarlo debidamente en sus evaluaciones de riesgos. [...] Estos riesgos pueden derivarse, por ejemplo, del uso no auténtico del servicio, como la creación de cuentas falsas, el uso de bots o el uso engañoso de un servicio, y otros comportamientos total o parcialmente automatizados, que pueden dar lugar a la difusión rápida y extendida de información al público que sea un contenido ilícito o incompatible con las condiciones generales de una plataforma en línea o un motor de búsqueda en línea y que contribuya a campañas de desinformación».

Igualmente, estas VLOPs deben conservar todos los documentos justificativos relativos a las evaluaciones de riesgos que hayan llevado a cabo, como la información relativa a su preparación, los datos subyacentes y los datos sobre la realización de pruebas de sus sistemas algorítmicos.

Además de detectar y de llevar a cabo la evaluación, la DSA indica que las plataformas de gran tamaño deben desplegar los medios necesarios para **reducir diligentemente los riesgos sistémicos** determinados en las evaluaciones de riesgos, eso sí, respetando los derechos fundamentales (Considerando 86). Cualquier medida con este objeto debe ser eficaz y apropiada para reducir los riesgos sistémicos específicos detectados. Debe ser proporcionada a la capacidad económica del prestador de la plataforma y de la necesidad de evitar restricciones innecesarias al uso de su servicio, teniendo en cuenta los riesgos para los derechos fundamentales, en especial con la libertad de expresión. En concreto, deberán garantizar que «un elemento de información, ya se trate de imagen, audio o vídeo generado o manipulado que se asemeja notablemente a personas, objetos, lugares u otras entidades o sucesos existentes y que puede inducir erróneamente a una persona a pensar que son auténticos o verídicos, se distinga mediante indicaciones destacadas cuando se presente en sus interfaces en línea y, además, proporcionar una funcionalidad fácil de utilizar que permita a los destinatarios del servicio señalar dicha información» (art. 35.2 DSA)

También deben sopesar **medidas de concienciación**, en especial cuando los riesgos estén relacionados con campañas de desinformación (art. 35.1.i).

Por último, hay que indicar que la DSA establece que las VLOPs han de realizar sus evaluaciones de riesgos y diseñar sus medidas de reducción del riesgo contando con la participación de representantes de los destinatarios del servicio, representantes de grupos potencialmente afectados por sus servicios, expertos independientes y organizaciones de la sociedad civil. Deben tratar de integrar dichas consultas en sus metodologías de evaluación de riesgos y de diseño de medidas de reducción, incluidas, en su caso, encuestas, grupos de discusión, mesas redondas y otros métodos de consulta y diseño.

3.4.3. La colaboración en tiempos de crisis

En tiempos de crisis puede ser necesario que los prestadores de servicios en línea de muy gran tamaño —de nuevo las VLOPs y las VLOSEs— adopten con urgencia determinadas medidas excepcionales en relación con los contenidos en línea, además de las que adoptarían en cumplimiento de las obligaciones generales que derivan del Reglamento. A este respecto, debe considerarse que se produce una crisis cuando se producen circunstancias extraordinarias que pueden dar lugar a una amenaza grave para la seguridad pública o la salud pública en la Unión o en partes significativas de la Unión. Estas crisis podrían derivarse, entre otros, de conflictos armados o

actos de terrorismo, ciberataques, catástrofes naturales como terremotos y huracanes, así como las pandemias y otras amenazas transfronterizas graves para la salud pública. Y en todas ellas, la circulación de campañas de desinformación a través de las redes podría agravar aún más la situación de crisis.

En ese tipo de situaciones, la Comisión podría exigir a los prestadores de plataformas en línea de muy gran tamaño y a los prestadores de motores de búsqueda en línea de muy gran tamaño, previa recomendación de la Junta Europea de Servicios Digitales, que inicien urgentemente una respuesta a la crisis. Tal como prevé la DSA, entre las medidas que dichos prestadores pueden considerar aplicar, pueden incluirse, por ejemplo, la adaptación de los procesos de moderación de contenidos y el aumento de los recursos dedicados a la moderación de contenidos, la adopción de medidas de concienciación y la promoción de información fiable. (art. 36 DSA). En todo caso, deben determinarse los requisitos necesarios para entender que se está ante una situación de crisis al objeto de garantizar que dichas medidas se adopten por necesidad justificada, con todas las garantías y duren el tiempo estrictamente necesario.

3.4.4. Participar en códigos de conducta

La DSA también prevé que la Comisión fomentará y facilitará la elaboración de Códigos de conducta voluntarios en el ámbito de la Unión para contribuir a la debida aplicación del Reglamento, invitando a las plataformas a adoptarlos y adherirse a los mismos. Se indica también que, en caso de incumplimiento sistemático de los Códigos de conducta, la Comisión y la Junta de servicios digitales podrán pedir a los signatarios de tales códigos de conducta que adopten las medidas necesarias (art. 45 DSA).

Dice también la DSA que la adhesión de las plataformas de gran tamaño a determinados códigos de conducta (por ejemplo, al *Código reforzado de buenas prácticas en materia de desinformación* o al *Código de conducta para la lucha contra la incitación ilegal al odio en internet*) y su cumplimiento pueden considerarse una medida adecuada para evitar los riesgos que se derivan del mal uso de las plataformas. Incluso añade que, «la negativa de un prestador de una plataforma en línea o de un motor de búsqueda en línea a participar en la aplicación de un código de conducta de esta índole a invitación de la Comisión, sin explicaciones adecuadas, podría tenerse en cuenta, cuando sea pertinente, a la hora de determinar si la plataforma en línea o el motor de búsqueda en línea ha incumplido las obligaciones establecidas en el presente Reglamento» (Considerando 104). Pero en el mismo considerando también advierte que «el mero hecho de participar en un código de conducta determinado y aplicarlo no debe presuponer por sí mismo el cumplimiento del presente Reglamento».

4. LOS RIESGOS Y POSIBLES GARANTÍAS DERIVADOS DE LAS PREVISIONES EN MATERIA DE MODERACIÓN DE CONTENIDOS DIGITALES PREVISTAS POR LA DSA

4.1. La dificultad para cribar los mensajes falsos sin dañar las libertades de expresión e información

Sin duda, uno de los mayores riesgos que la moderación de contenidos digitales puede generar es la extralimitación de las libertades de expresión e información. Así, la DSA reconoce desde sus

primeros considerandos la dificultad respecto de estas libertades que puede derivarse de la aplicación de aquellas medidas que tratan de evitar los daños de la difusión de desinformación u otros contenidos ilícitos. De hecho, en particular, la DSA exige un deber de diligencia a los prestadores de servicios digitales, indicando que «cuando se produzca la retirada o bloqueo del acceso deber llevarse a cabo de manera diligente, objetiva y proporcionada para aplicar y hacer cumplir las restricciones [...] con la debida consideración de los derechos e intereses legítimos de todas las partes implicadas, incluidos los derechos fundamentales de los destinatarios del servicio, como la libertad de expresión, la libertad y el pluralismo de los medios de comunicación y otros derechos y libertades fundamentales amparados por la Carta» (art. 14.4 DSA).

En la misma línea, señala que «el presente Reglamento ha de interpretarse y aplicarse de conformidad con tales derechos fundamentales, incluida la libertad de expresión e información, y la libertad y el pluralismo de los medios de comunicación. En el ejercicio de las competencias establecidas en el presente Reglamento, todas las autoridades públicas implicadas deben alcanzar, en situaciones en las que los derechos fundamentales pertinentes entren en conflicto, un equilibrio justo entre los derechos afectados, de conformidad con el principio de proporcionalidad» (Considerando 153).

Para evitar o minorar ese daño en las libertades de expresión e informativas, tanto a la autoridad estatal o de la UE como a la empresa digital, se le exige que cualquier orden de transmisión de información o de moderación de contenidos (por ejemplo, de borrado de los mismos o cierre de página web) ha de motivarse expresamente, indicarse la razón por la que ese contenido finalmente es considerado susceptible de moderación, informar al titular de tales contenidos desinformadores e identificar el precepto del Derecho de la Unión o del Estado en aplicación del Derecho de la UE se ha infringido (arts. 9.2 y 17 DSA). Se trata de establecer garantías que aseguren que esa moderación de contenidos desinformadores está justificada.

Igualmente, se ha de informar de los mecanismos de recursos susceptibles de ser empleados contra la acción de moderación de contenidos realizada. Asimismo, en su caso, se ha de informar a la persona o entidad afectada de la existencia de mecanismos de resolución extrajudicial, que deben estar previstos siempre en el caso de las VLOPs.

A este respecto, hay que recordar que Facebook-Meta estableció un consejo asesor de contenido compuesto por cuarenta expertos internacionales y fijó como objetivo la defensa de la libertad de expresión (38). El consejo asesor actúa a modo de tribunal internacional de apelación, donde los usuarios e interesados pueden solicitar la revisión de decisiones tomadas por la entidad, cuando puedan haber afectado a los derechos individuales o colectivos de los usuarios.

Además, existe la obligación para las corporaciones digitales de conservar los contenidos moderados por la necesidad de garantizar los medios de prueba pertinentes a la propia compañía digital como al titular de los contenidos en línea retirados o cuyo acceso haya sido bloqueado ante un posible proceso judicial o administrativo, así como para garantizar el restablecimiento de dichos contenidos, en función del resultado de dichos procedimientos.

4.2. La posibilidad de error sobre la verdad o falsedad de un contenido digital

Sin duda, una de las dificultades adicionales cuando se trata de controlar mensajes falsos, es que es más difícil errar con las predicciones o métodos de detección que si se buscan contenidos ilegales como, por ejemplo, los de carácter terrorista o discriminator, especialmente si en el monitoreo se han utilizado exclusivamente algoritmos. Resulta infinitamente más arduo cuando se trata de detectar mensajes de desinformación por la complejidad técnica de encontrar cómo realizar ese filtrado, que no puede ser tan automático como en otros monitoreos. Los expertos se inclinan por defender que el juicio humano, y el establecimiento de paneles de expertos (*fact-checkers*) que realicen las comprobaciones pertinentes, es una herramienta mucho más fiable para controlar las noticias falsas que el recurso a los algoritmos.

De hecho, en los considerandos de la DSA ya se señala que «los prestadores de que se trate deben, por ejemplo, adoptar medidas razonables para garantizar que, cuando se utilicen herramientas automatizadas para llevar a cabo tales actividades, la tecnología de que se trate tenga la fiabilidad suficiente para limitar en la mayor medida posible el porcentaje de errores» (Considerando 26 DSA).

También es posible que el error provenga de quien notifique una falsedad y no se haya realizado la suficiente comprobación. De hecho, la DSA señala que los prestadores de plataformas en línea otorgarán especial prioridad a las notificaciones enviadas por lo que se denominan «alertadores fiables», que son aquellas entidades que hayan sido designadas como tales por el Coordinador de servicios digitales de cada Estado, previa solicitud, que hayan demostrado poseer conocimientos y competencias para detectar, identificar y notificar contenidos ilícitos y no dependan de ningún prestador de plataformas en línea (art. 22 DSA).

Pero, en segundo lugar, lo más complejo es realizar un monitoreo de los contenidos digitales diferenciando lo que son solo medias verdades de las indiscutibles falsedades o mentiras. Es muy complicado realizarlo de una manera neutra y sin caer en el error de eliminar mensajes que son manifestación de la libertad ideológica o de la libertad informativa, o que pueden estar erradas, pero no entrarían dentro del concepto de bulo. La verdad no siempre es fácil reconocerla y, a veces, hasta algunas barbaridades son aceptables en democracia. Por ejemplo, se admiten posiciones negacionistas sobre la existencia del Holocausto cuando encontraríamos infinidad de pruebas históricas acerca de su existencia (39). Y, sobre todo, en gran número de ocasiones, la verdad es distinta dependiendo de quién la argumente, no existiendo una única verdad.

Por todo ello, además de la exigencia de motivación de la moderación de contenidos realizada, la DSA exige una política de transparencia en su política de moderación de contenidos, al indicar que las empresas digitales deberán informar a los usuarios sobre cualesquiera políticas, procedimientos, medidas y herramientas empleados para moderar los contenidos, incluidas la toma de decisiones mediante algoritmos y la revisión humana, así como sobre las normas de procedimiento de su sistema interno de gestión de reclamaciones. (art. 14 DSA). Y deben publicar esta información de un modo que resulte claro y accesible.

4.3. El riesgo de convertir a las plataformas de servicios electrónicos en controladores del debate

público

Pese a que en los considerandos de la DSA se indica, respecto de los prestadores de servicios digitales, que «nada de lo dispuesto en el presente Reglamento debe interpretarse como la imposición de una obligación general de monitorización o de una búsqueda activa de hechos general, o una obligación general de que los prestadores adopten medidas proactivas en relación con contenidos ilícitos» (Considerando 30 DSA), sí se corre el riesgo de que las grandes plataformas, en un intento de evitar responsabilidades acaben realizando este control de cribado general de todos los contenidos. De hecho, como decíamos anteriormente, sabemos que las grandes compañías digitales vienen realizando *motu proprio* este tipo de monitorización o filtrado de los contenidos que circulan o se depositan en sus plataformas desde hace años.

Ahora nos encontramos no solo con la posibilidad de que voluntariamente las corporaciones digitales continúen con ese control y moderación de contenidos, sino que además las VLOPs y VLOSEs tendrán que hacerlo en relación con los riesgos sistémicos y en supuestos de crisis.

Se vuelve a abrir la cuestión acerca de la capacidad de una empresa privada como X (antes Twitter) de decidir en democracia quién habla y quién no y qué se puede decir y qué no. Y abre el interrogante de la naturaleza de estas plataformas. ¿Se trata de un control privado? Creo que ya no pueden ser consideradas como empresas privadas por el papel que desempeñan en el flujo público de información y comunicación a nivel global y para millones de usuarios. Se han convertido en un canal de naturaleza pública. En todo caso, ¿se puede dejar en sus manos la capacidad de controlar el discurso público?

El Tribunal Supremo español ponía de manifiesto el riesgo que supone dejar en manos de empresas o instituciones no independientes o sin la transparencia debida el cribado y censura de contenidos falsos. En la sentencia STS 652/2022, de 8 de marzo de 2022, dejaba constancia de lo «insatisfactorio que, tanto en lo procedimental como en lo material, es el escaso tratamiento legal de ese poder censor que se reservan contractualmente las redes sociales, erigidas hoy día en medios de difusión masiva de todo tipo de contenidos, también políticos, con un poder e influencia manifiestos en tiempos electorales».

Efectivamente, existe una preocupación compartida de que, con esta habilitación normativa europea, especialmente los grandes proveedores de servicios de Internet, así como las organizaciones y personas que representan a determinadas categorías de opinión política legítima y que actúan permanentemente en redes, puedan practicar todo tipo de censura privada. Se les estaría convirtiendo en censores privados del ejercicio de determinadas libertades públicas. Ello supone habilitar a las empresas a ejercer una función que tradicionalmente ha correspondido a la autoridad judicial. Permitiría despojar a los órganos tradicionales legitimados para determinar cuándo puede limitarse la libertad de expresión, esto es, los jueces. Por eso es importante que la DSA haya establecido un conjunto de garantías que vienen a asegurar que la moderación de contenidos que pueda llevarse a cabo por las plataformas intermediarias de servicios digitales esté justificada, sea razonable, proporcional y pueda ser revisada.

Y ello es especialmente importante cuando hablamos de moderación de contenidos que presumiblemente pueden generar desinformación, porque se trata de evitar que el monopolio sobre las opiniones o informaciones que puedan circular en internet o no, sobre lo que se considera verdad o mentira, quede a discreción de las grandes compañías digitales. Por poner un ejemplo reciente, se denunciaba que las redes sociales no están tratando de igual modo a los diferentes intervinientes en la contienda entre Israel y Hamás. Individuos y asociaciones palestinas han manifestado que muchos de los contenidos publicados en las redes han sido censurados por las plataformas, produciéndose un trato desigual entre propalestinos y proisraelíes, en favor del relato que ofrecen estos segundos en internet (40). Al igual que la desinformación sobre la guerra de Ucrania se ha extendido de forma desenfrenada desde el comienzo, especialmente con información falsa lanzada desde el gobierno ruso que ha tratado de justificar ante su ciudadanía la invasión del país vecino, lo mismo está ocurriendo con los acontecimientos que se vienen sucediendo en Israel y la zona de Gaza. Se suceden las informaciones no veraces en redes, unas que tratan de justificar ante la opinión pública las bárbaras actuaciones de Hamas y otras las del gobierno israelí, cuando tan reprochables y los horrendos fueron los ataques de Hamás del 7 de octubre de 2023 como, más aún, la indiscriminada y desproporcionada respuesta de Israel contra la población de la Franja de Gaza. Lo censurable no es la defensa en redes de los unos o los otros, sino el uso de la mentira para sustentar esas posturas y emponzoñar la formación de la opinión pública, que habría de hacerse de un modo libre y pluralmente informado. Por lo tanto, cabría entender que han de activarse mecanismos para limitar la circulación de esos contenidos desinformadores, pero cuando en ese debate las grandes plataformas, o incluso las instituciones nacionales o europeas, adoptan una postura excesivamente moderadora de contenidos e incluso desigualitaria, quien pierde es la democracia.

Por estas razones, la DSA ha establecido numerosos mecanismos de control del cumplimiento del propio Reglamento y de las actuaciones de moderación de contenidos. Entre ellos podemos encontrar los siguientes:

a) Los informes de los prestadores de servicios digitales

El prestador de servicios digitales debe presentar a la autoridad competente informes sobre las medidas específicas tomadas, cuando haya sido conminado a actuar contra determinados contenidos o cuando lo haya hecho en aplicación del Reglamento, informando del número de suspensiones de servicio llevadas a cabo.

Además, los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben elaborar informes sobre las medidas que han ido adoptando y sobre el funcionamiento de los órganos de resolución extrajudicial (art. 21.4, art. 42).

b) La designación de las autoridades estatales responsables de la supervisión de los prestadores de servicios digitales

Los Estados miembros designarán una o varias autoridades competentes responsables de la supervisión de los prestadores de servicios intermediarios y de la ejecución de la DSA, que se denominan coordinadores de servicios digitales. Estos dispondrán de la facultad de

investigación respecto de la conducta de los servicios intermediarios y la capacidad de exigirles el cumplimiento de las previsiones de la DSA e incluso la posibilidad de imponer una multa o solicitar a una autoridad judicial del Estado que lo haga (art. 51 DSA).

La DSA prevé también la creación de un grupo consultivo independiente a escala de la Unión, una Junta Europea de Servicios Digitales, que debe prestar apoyo a la Comisión y ayudar a coordinar las acciones de los coordinadores de servicios digitales y velar por que este Reglamento se aplique de forma coherente. Esa Junta debe estar integrada por los coordinadores de servicios digitales, allí donde hayan sido nombrados.

c) El control del posible incumplimiento por las VLOPs o VLOSEs de la DSA

Dada la importancia de las plataformas en línea de muy gran tamaño o los motores de búsqueda de muy gran tamaño, en vista de su alcance y repercusión, el incumplimiento por su parte de las obligaciones específicas que les son aplicables puede afectar a un número importante de destinatarios de los servicios de diferentes Estados miembros y puede causar grandes perjuicios sociales, mientras que dichos incumplimientos pueden ser además especialmente difíciles de detectar y corregir.

Por este motivo, por un lado, se indica que las plataformas de muy gran tamaño tendrán uno o varios encargados de cumplimiento del Reglamento (art. 41 DSA) y se les exige el sometimiento, a su propia costa y una vez al año, a auditorías independientes para evaluar el cumplimiento de obligaciones derivadas de dicho Reglamento (art. 37 DSA); y, por otro lado, la Comisión Europea, en cooperación con los coordinadores de servicios digitales y la Junta, podrá desarrollar medios de supervisión de las plataformas en línea de muy gran tamaño o los motores de búsqueda de muy gran tamaño, también con ese fin (arts. 64 y 65 DSA).

La Comisión debe poder investigar las infracciones por iniciativa propia, de conformidad con las competencias previstas en el presente Reglamento, en particular solicitando el acceso a los datos y a la información o realizando inspecciones, y debe poder contar con el apoyo de los coordinadores de servicios digitales. En particular, lo que la Comisión podrá controlar específicamente es el cumplimiento de «las obligaciones adicionales de gestión de riesgos sistémicos de las VLOPs», recogidas en la sección quinta del capítulo III de la DSA. También podrá actuar cuando un asunto le sea remitido.

Una vez que se haya constatado una infracción de una de las disposiciones del Reglamento que se aplican únicamente a las plataformas en línea de muy gran tamaño o a los motores de búsqueda en línea de muy gran tamaño, la Comisión debe pedir al prestador de dicha plataforma o de dicho motor de búsqueda que actúe en un determinado sentido y que elabore un plan de acción detallado para subsanar cualquier efecto de la infracción en el futuro y que comunique dicho plan de acción, en un plazo señalado por la Comisión, a los coordinadores de servicios digitales, a la Comisión y a la Junta.

Si después de la ejecución del plan de acción, la Comisión sigue considerando que la infracción

no ha sido totalmente subsanada, o si el plan de acción no ha sido comunicado o no se considera adecuado, y se constata el incumplimiento de compromisos o disposiciones del Reglamento, esta puede hacer uso de las facultades de investigación o ejecución, emitiendo una decisión de incumplimiento y utilizando las facultades para imponer multas coercitivas y la incoación del procedimiento para bloquear el acceso al servicio infractor (art. 66 DSA).

Y, en última instancia, todas las decisiones adoptadas por la Comisión en virtud de la DSA están sujetas al control del Tribunal de Justicia de la Unión Europea de conformidad con el TFUE (art. 81 DSA).

5. BREVE RECAPITULACIÓN

Los beneficios de la digitalización son evidentes en múltiples ámbitos y lo son también como motores de difusión de opiniones y hechos noticiables, lo cual es un componente sustancial en nuestras democracias. Sin embargo, como se decía al comienzo de este trabajo, también es verdad que se ha realizado un uso interesado de las plataformas digitales y de las herramientas que estas brindan para interferir en esa opinión pública, —al igual que para llevar a cabo actividades ilícitas—, y la desinformación se encuentra entre esos instrumentos utilizados para influir en la conformación del parecer de los ciudadanos. El recurso a la desinformación, a la mentira y a la creación falsa de un relato público es algo tan antiguo como el ser humano. Se cuenta que Ramses II hizo que sus escribas anotaran sus victorias en numerosas batallas, que con el tiempo se demostró que nunca fueron ganadas o no sucedieron. Pero la leyenda para aquel pueblo fue la que fue.

Así, esa capacidad de manejar el relato público o tratar de influir en la conciencia pública para que la gente piense de un modo u otro, actúe de tal manera o de tal otra, vote a un determinado partido, etc. ha sido una constante en nuestra historia. Y, especialmente la radicalización y los discursos extremos son los que más se han apoyado en narrativas sustentados en información falsa. Es una realidad que estos discursos extremos, muchas veces mentirosos, incluyen no pocas veces el rechazo social hacia determinados colectivos, potenciando su exclusión (extranjeros, personas de raza negra, miembros de la etnia romaní, creyentes de determinado signo religioso...). Y, si la democracia busca y se fundamenta en la igualdad y en el respeto de las minorías, cualquier actividad desinformativa de este tipo puede dañar esos fundamentos. Al igual que si lo que precisa la democracia es de una opinión pública fundada sobre información plural y veraz, la desinformación golpea los cimientos de esta.

Lo que ha cambiado con la era digital es el exponencial valor que las redes tienen para difundir relatos, para difundir contenidos desinformadores. En esa nueva realidad, las plataformas digitales donde se almacenan o circulan esos contenidos tienen un indudable poder en sus manos y al mismo tiempo una gran responsabilidad. Algunas de estas plataformas, que ocupan una posición dominante en el mercado, cuentan con una ventaja desproporcionada sobre sus competidores. Estas pueden influir de una forma notable —positiva o negativamente— sobre la democracia, los derechos fundamentales, las sociedades y la economía. De las plataformas en línea que operan en la UE un 90% son pequeñas o medianas, pero ese 10% restante, que lo conforman las grandes plataformas y

las muy grandes plataformas digitales (VLOPs), tiene en sus manos un especial poder sobre la circulación de contenidos de toda naturaleza. Por ello la UE ha querido establecer una regulación de sus márgenes de actuación, adelantándose a otros países del mundo que se enfrentan a la misma realidad, pero han optado por una respuesta distinta. Diferimos en ello con la opción estadounidense, donde se ha partido de las plataformas digitales como foros privados que, como tales, no son susceptibles de un tipo de regulación como la que ha decidido poner en marcha la UE. No obstante, también el gigante norteamericano empieza a ser consciente de la necesidad de controlar a aquellas plataformas que manejan una ingente cantidad de datos, entre otras cosas, por razón de geoestrategia y seguridad. La comparecencia del CEO de Tik-Tok ante el Congreso de los Estados Unidos en abril de 2023 fue una muestra de ello (41). Por no olvidar que, incluso las empresas digitales que tienen su sede matriz en EEUU, si prestan servicios en la UE, deben someterse a la normativa de este espacio.

La DSA, además de crear un entorno digital más seguro para todos, que respete los derechos fundamentales, supone una oportunidad sin precedentes para definir adecuadamente el papel que corresponde a las plataformas digitales en el control de los contenidos on-line en la persecución de objetivos de interés público, entre ellos la lucha contra la desinformación. Y lo hace reforzando los derechos de los usuarios frente a contenidos ilícitos y desinformadores nocivos y estableciendo mecanismos públicos de supervisión de la actuación de esas plataformas proveedoras de contenidos online, tanto en relación con el adecuado cumplimiento de los objetivos DSA, como en relación a la salvaguarda de los derechos a la libertad de expresión y las libertades informativas, así como convirtiéndolas en colaboradoras necesarias en el logro de los objetivos generales de la UE en el mundo digital (eliminación de contenidos ilícitos o desinformadores, lucha contra riesgos sistémicos, o adopción de respuestas en tiempos de crisis...) Ahora queda un camino por delante para ver cómo se va implementando esta normativa y qué controles van aplicándose desde la UE. En todo caso, no olvidemos tampoco que la misma Comisión Europea no es una institución neutra.

6. REFERENCIAS BIBLIOGRÁFICAS

- Aba Catoira, A. (2020), «Desórdenes informativos en un sistema de comunicación democrático», *Revista de Derecho Político*, n. 109, pp. 119-151.
- Abad Soto, J. (2020), «La guerra de percepción en la crisis de la COVID-19», *Documento de Opinión IEEE* n. 66, 21/05/2020.
- Arenas Ramiro, M. (2019), «Partidos políticos, opiniones políticas e internet: la lesión del derecho a la protección de datos», *Teoría y Realidad Constitucional*, n. 44, p. 341-372.
- Barrio Andrés, M. (2022), *Manual de Derecho Digital*, Valencia, Ed. Tirant lo Blanch, 2.ª edición.
- Bernigaud, A. (2023), «Defending the vote: France acts to combat foreign disinformation», *Global Challenges. Election Disinformation*, Princeton School of Public and International Affairs, p. 2.
- Burger, M. A. (2022), «France debates making fake news a crime», *ACEprensa*, 10 febrero 2023.

Comisión Europea (2023). «Commission opens formal proceedings against X under the Digital Services Act», Press Release, 18 December 2023.

https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709

Comisión Europea (2023), «More responsibility, less opacity: what it means to be a *Very Large Online Platform*-Statement by Commissioner Breton».

https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_23_2452

Diges, J. (EFE) (2023), «Detector de bulos ambientales. La falsa catástrofe ecológica de las placas solares», *El País*, 26 junio 2023.

Domínguez de Olazábal, I. (2023), «Una batalla desigual también en las redes sociales», *El País*, 21 de octubre de 2023.

Habermas, J. (1981), *Historia y crítica de la opinión pública*, Traducción de Antonio Domenech, Barcelona, Ed. Gustavo Gili, S.L.

Harari, Y. N. (2023), «El posible fin de la historia humana», *La Vanguardia*, 3 de mayo de 2023.

Harris, B. (2020), «El consejo asesor de contenido comienza a recibir casos. *Facebook-Meta Newsroom*», 22 de octubre. Disponible en: <https://about.fb.com/es/news/2020/10/el-consejo-asesor-de-contenido-comienza-a-recibir-casos>

Herreros López, J. M. (2004), «La formación de la opinión pública», en Vidal Climent, V. y García Manglano, M. (Coords.), *Información, libertad y derechos humanos: la enseñanza de la ética y el derecho de la información*, Valencia: Fundación Coso de la Comunidad Valenciana, pp. 161-176.

Magallón Rosa, R. (2019), «La (no) regulación de la desinformación en la Unión Europea. Una perspectiva comparada», *Revista de Derecho Político*, n. 106, p. 319-347.

Martínez Martínez, R. (2023), *El caso Tik Tok: geoestrategia, internet y derechos fundamentales*, Cinco Días. El País, 13 abril 2023.

Pauner Chulvi, C. (2018-a), «Las noticias falsas y las campañas de desinformación como nuevas amenazas para la seguridad», en *Seguridad y derechos. Análisis de las amenazas, evaluación de las respuestas y valoración del impacto en los derechos fundamentales*, González Cussac, J. L. y Flores Giménez, F. (Coords.), Valencia, Tirant lo Blanch.

Pauner Chulvi, C. (2018-b), «Noticias falsas y libertad de expresión e información. El control de los contenidos informativos en la red», *Teoría y Realidad Constitucional*, n. 41, pp. 301 y 302.

Rubio Núñez, R. (2018), «Los efectos de la posverdad en la democracia», *Revista de Derecho Político*, n. 108, pp. 97-126.

Sahuquillo, M.R. (2023), «Bruselas abre una investigación a X por difusión de desinformación tras el

ataque de Hamás», *El País*, 12 de octubre de 2023.

Sánchez Navarro, A. y Fernández Riveira, R.M. (Dirs.) (2021). *Reflexiones para una democracia de calidad en una era tecnológica*, Pamplona, Aranzadi Thomson Reuters.

Torres del Moral, A. (2013), *La opinión pública y su tratamiento jurisprudencial. Constitución y desarrollo político*, Valencia, Tirant lo Blanch.

-
- (1) Este trabajo se ha realizado en el marco del Proyecto de I+D+i PROMETEO/2021/013 «Responsabilidad social de la empresa» y del Proyecto I+D financiado por el Ministerio de Ciencia e Innovación y fondos FEDER: «Tiempos y espacios de una justicia inclusiva. Derechos para una sociedad resiliente frente a los nuevos retos. IN_ JUSTICE». Ref. PID2021-126552OB-I00.

Ver Texto

- (2) rosario.serra@uv.es

Código Orcid: <https://orcid.org/0000-0003-3154-5313>

Ver Texto

- (3) Comisión Europea (2023), «Commission opens formal proceedings against X under the Digital Services Act», Press Release, 18 December 2023.

https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709 (Consulta: 08/01/2024)

Ver Texto

- (4) Sahuquillo, M.R. (2023), «Bruselas abre una investigación a X por difusión de desinformación tras el ataque de Hamás», *El País*, 12 de octubre de 2023.

Ver Texto

- (5) Comisión Europea (2023), «More responsibility, less opacity: what it means to be a *Very Large Online Platform*-Statement by Commissioner Breton».

https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_23_2452 (Consulta: 24/10/2023)

Ver Texto

- (6) La normativa obliga a que las plataformas analicen los riesgos sistémicos que provocan. Y tendrá que efectuar un análisis de reducción de esos riesgos en relación con los temas mencionados [salud mental, protección de menores y violencia de género], para lo cual deberán realizar un informe con periodicidad

anual.

[Ver Texto](#)

- (7) La DSA define en su art. 3 la moderación de contenidos como «las actividades, estén o no automatizadas, realizadas por los prestadores de servicios intermediarios, que estén destinadas, en particular, a detectar, identificar y actuar contra contenidos ilícitos o información incompatible con sus condiciones generales, que los destinatarios del servicio hayan proporcionado, por ejemplo la adopción de medidas que afecten a la disponibilidad, visibilidad, y accesibilidad de dicho contenido ilícito o de dicha información, como la relegación, la desmonetización de la información, el bloqueo de esta o su supresión, o que afecten a la capacidad de los destinatarios del servicio de proporcionar dicha información, como la supresión o suspensión de la cuenta de un destinatario del servicio».

[Ver Texto](#)

- (8) Council Decision (CFSP) 2022/351 of 1 March 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

[Ver Texto](#)

- (9) El Tribunal Constitucional declaró tempranamente que la «opinión pública es una institución política fundamental (...) indisolublemente ligada con el pluralismo político que es un valor fundamental y un requisito del funcionamiento del Estado democrático» (STC 12/1982, FJ 3). En la misma línea, ha indicado que el proceso de formación de la opinión pública, en tanto que actividad previa al ejercicio del derecho de sufragio, ha de considerarse como «uno de los pilares de la sociedad libre y democrática» (STC 159/1986). Herreros López, J. M. (2004). «La formación de la opinión pública», en Vidal Climent, V. y García Manglano, M. (Coords.), *Información, libertad y derechos humanos: la enseñanza de la ética y el derecho de la información*, Valencia: Fundación Coso de la Comunidad Valenciana, pp. 161-176. Véase también, Torres del Moral, A. (2013), *La opinión pública y su tratamiento jurisprudencial. Constitución y desarrollo político*, Valencia, Tirant lo Blanch. O el más clásico trabajo Habermas, J. (1981), *Historia y crítica de la opinión pública*, Traducción de Antonio Domenech, Barcelona, Ed. Gustavo Gili, S.L.

[Ver Texto](#)

- (10) A propósito de la calidad democrática en la era digital puede consultarse el trabajo colectivo: Sánchez Navarro, A. y Fernández Riveira, R.M. (Dirs.) (2021), *Reflexiones para una democracia de calidad en una era tecnológica*, Pamplona, Aranzadi Thomson Reuters.

[Ver Texto](#)

- (11) El filtrado excesivo de información causa que se empobrezca el debate público virtual, puesto que al solamente mostrarse lo que el usuario desea ver, se dificulta la recepción de informaciones contrarias a las creencias o a los gustos del usuario, pero que sería necesario que recibiese, para enriquecer el debate democrático.

[Ver Texto](#)

- (12) Pauner Chulvi relata cómo gran parte de las noticias falsas son creadas por *spammers*, como se viralizan a través de redes sociales como Facebook o Twitter, como se usan los conocidos como *trolls* y otros

instrumentos de creación y difusión de bulos, Pauner Chulvi, C. (2018-b), «Noticias falsas y libertad de expresión e información. El control de los contenidos informativos en la red», *Teoría y Realidad Constitucional*, n. 41, pp. 301 y 302. Véase también el interesante trabajo: Aba Catoira, A. (2020), «Desórdenes informativos en un sistema de comunicación democrático», *Revista de Derecho Político*, n. 109, pp. 119-151.

[Ver Texto](#)

- (13) Rubio Núñez, R. (2018), «Los efectos de la posverdad en la democracia», *Revista de Derecho Político*, n. 108, pp. 97-126. Abad Soto, J. (2020). «La guerra de percepción en la crisis de la COVID-19», *Documento de Opinión IEEE* n. 66, 21/05/2020.

[Ver Texto](#)

- (14) Diges, J. (EFE) (2023), «Detector de bulos ambientales. La falsa catástrofe ecológica de las placas solares», *El País*, 26 junio 2023.

[Ver Texto](#)

- (15) La Estrategia de Seguridad Nacional de 2021 incluyó las campañas de desinformación como uno de los retos que desafían a España, insistiendo en que tienen la voluntad de generar confusión y socavar la cohesión social. Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021. Más recientemente la Comisión Europea, en la nueva Estrategia de Seguridad de la Unión 2020-25 (24 de junio de 2020) hacía hincapié en la lucha contra «las campañas de desinformación y la radicalización de la narrativa política».

[Ver Texto](#)

- (16) La pandemia generada por el Covid-19 nos ofreció numerosos ejemplos de bulos que se difundieron, que persiguieron objetivos de lo más diverso, pero entre ellos se buscaba tratar de desprestigiar la actuación o la respuesta política dada por los gobiernos en luchar contra la pandemia. La DSA también hace referencia en sus considerandos a los riesgos que pueden derivarse de campañas coordinadas de desinformación relacionadas con la salud pública (Considerando 83)

[Ver Texto](#)

- (17) Pauner Chulvi, C. (2018-a), «Las noticias falsas y las campañas de desinformación como nuevas amenazas para la seguridad», en *Seguridad y derechos. Análisis de las amenazas, evaluación de las respuestas y valoración del impacto en los derechos fundamentales*, González Cussac, J. L. y Flores Giménez, F. (Coords.), Valencia, Tirant lo Blanch, p. 395.

[Ver Texto](#)

- (18) Así, pudo comprobarse como este tipo de campañas de desinformación, orquestadas por Rusia, condicionaron el voto en la decisión sobre el *Brexit* o en la elección de Donald Trump como presidente, o ha estado presente en otros procesos de votación como durante el denominado proceso catalán.

[Ver Texto](#)

(19) Harari, Y. N. (2023), «El posible fin de la historia humana», *La Vanguardia*, 3 de mayo de 2023.

Ver Texto

(20) Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021.

Ver Texto

(21) Décret n° 2021-922 du 13 juillet 2021 portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénommé « service de vigilance et de protection contre les ingérences numériques étrangères »

Ver Texto

(22) Bernigaud, A. (2023). «Defending the vote: France acts to combat foreign disinformation», *Global Challenges. Election Disinformation*, Princeton School of Public and International Affairs, p. 2.
(https://successfultsities.princeton.edu/sites/g/files/toruqf56o1/files/France_AB_Viginum_.pdf.
Consulta: 28/10/2023).

Ver Texto

(23) Lo hicieron el Grupo Parlamentario Popular, y el Grupo Parlamentario Confederal de Unidas-Podemos-En Comú Podem-En Marea. Sobre las mismas puede verse Pauner Chulvi, C. (2018-a), «Las noticias falsas y las campañas de desinformación...», op. cit., pp. 414 y ss.

Ver Texto

(24) Magallón Rosa, R. (2019), «La (no) regulación de la desinformación en la Unión Europea. Una perspectiva comparada», *Revista de Derecho Político*, n. 106, p. 319-347.

Ver Texto

(25) Burger, M. A. (2022). «France debates making fake news a crime», ACEprensa, 10 febrero 2023.
<https://www.aceprensa.com/english/france-debates-making-fake-news-a-crime/> (Consulta: 28/10/2023)

Ver Texto

(26) Arenas Ramiro analiza también diversas medidas legislativas que los Estados han ido adoptando para proteger el debate político y la formación de la opinión pública frente a las campañas de desinformación en la red, especialmente durante las campañas electorales. Arenas Ramiro, M. (2019), «Partidos políticos, opiniones políticas e internet: la lesión del derecho a la protección de datos», *Teoría y Realidad Constitucional*, n. 44, p. 344.

Ver Texto

(27) Ha de recordarse que, en Austria, hasta 2015 la difusión de falsos rumores estaba prohibido como delito en el art. 276 del Código penal.

[Ver Texto](#)

- (28) Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

[Ver Texto](#)

- (29) En la Sentencia en el asunto C-18/18 Eva Glawischnig-Piesczek/Facebook Ireland Limited, de 3 de octubre de 2019, el Tribunal de Justicia de la UE ya había señalado que el Derecho de la Unión no se opone a que se obligue a un prestador de servicios de alojamiento de datos como Facebook a suprimir comentarios idénticos y, en determinadas condiciones, similares a un comentario declarado ilícito con anterioridad. El Derecho de la Unión tampoco se opone a que esa medida cautelar produzca efectos a escala mundial, en el marco del Derecho internacional pertinente que los Estados miembros deben tener en cuenta.

[Ver Texto](#)

- (30) *EU Security Union Strategy*, adoptada por la Comisión Europea para el período de 2020-2025.

[Ver Texto](#)

- (31) Así lo recordaba Pauner Chulvi, C. (2018-b), «Las noticias falsas y las campañas de desinformación...», op. cit., p. 404.

[Ver Texto](#)

- (32) 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 (también conocido como Reglamento de Servicios Digitales).

[Ver Texto](#)

- (33) Fighting disinformation and dissemination of illegal content in the context of the Digital Services Act and in times of conflict – Speech by Commissioner Breton. Bruselas, 18 octubre 2023, *SPEECH/23/5126*.

[Ver Texto](#)

- (34) Cuando hablamos de «Difusión pública» de una información falsa entendemos la «puesta a disposición de un número potencialmente ilimitado de personas (de la misma), es decir, hacer que la información sea fácilmente accesible para los destinatarios del servicio en general, sin necesidad de que el destinatario del servicio que proporciona la información haga nada más, con independencia de si dichas personas acceden efectivamente a la información en cuestión» (Considerando 14 DSA).

[Ver Texto](#)

- (35) Los grupos definidos por la DSA los siguientes:

- Servicios de intermediación: este grupo contiene a los proveedores que ofrecen infraestructuras

de red, como proveedores de acceso a internet o registradores de dominio.

- Servicios de alojamiento de datos: como puedan ser servicios de alojamiento de archivos y de alojamiento web.
- Plataformas en línea que permiten la interacción de consumidores con vendedores, como tiendas de aplicaciones, mercados en línea o redes sociales. No entran en esta categoría los proveedores que sean microempresas o pequeñas empresas.
- Plataformas en línea de muy gran tamaño, siendo estas las plataformas del grupo anterior que sean utilizadas mensualmente por más de un 10% de los consumidores europeos. Sí entrarían en esta categoría los proveedores que sean microempresas o pequeñas empresas.

Las plataformas de muy gran tamaño (VLOPs) designadas por la Comisión Europea son: X (Twitter), TikTok, Instagram, Wikipedia, Zalando, AliExpress, Amazon, AppStore de Apple, Booking, Facebook, Google Play, Google Maps, Google Shopping, LinkedIn, Pinterest, Snapchat y YouTube. A ello se añaden también dos buscadores: Google Search y Bing.

Ver Texto

- (36) El *Reglamento sobre la lucha contra la difusión de contenidos terroristas en línea* establece que se debe imponer a los prestadores de servicios en línea la obligación de garantizar que se retiren los contenidos terroristas a que se refiere la orden de retirada, o que se bloquee el acceso a ellos en todos los Estados miembros, lo más pronto posible y, en cualquier caso, en el plazo de una hora desde la recepción de la orden de retirada. Excepto en situaciones de emergencia debidamente justificadas, la autoridad competente debe proporcionar al prestador de servicios de alojamiento información sobre los procedimientos y los plazos aplicables con al menos doce horas de antelación a la emisión de la primera orden de retirada a ese prestador. Los casos de emergencia debidamente justificados se producen cuando la retirada de los contenidos o el bloqueo del acceso a los contenidos terroristas transcurrida más de una hora desde la recepción de la orden de retirada produciría un daño grave, como por ejemplo situaciones de amenaza inminente para la vida o para la integridad física de una persona o cuando dichos contenidos muestren acontecimientos en curso que produzcan daños continuados para la vida o para la integridad física de una persona. La autoridad competente debe determinar si constituyen casos de emergencia y justificar debidamente su decisión en la orden de retirada. El prestador de servicios de alojamiento de datos debe informar lo antes posible a la autoridad competente que dictó la orden en caso de que no pueda acatar la orden de retirada en el plazo de una hora desde su recepción por motivos de fuerza mayor o imposibilidad de hecho, incluidos los motivos técnicos u operativos justificados, y cumplirá la orden de retirada tan pronto como se haya resuelto la situación.

Ver Texto

- (37) Pauner Chulvi, C. (2018-b), «Noticias falsas y libertad de expresión...», *op. cit.*, p. 305.

Ver Texto

- (38) Harris, B. (2020), El consejo asesor de contenido comienza a recibir casos. *Facebook-Meta Newsroom*, 22 de octubre. Disponible en: <https://about.fb.com/es/news/2020/10/el-consejo-asesor-de-contenido-comienza-a-recibir-casos>

Ver Texto

(39) Véase el recurso de inconstitucionalidad contra el art. 607.2 del Código Penal, resuelto por el Tribunal Constitucional en la STC 235/2007, y que tuvo como objeto la punición de la denegación de la existencia del holocausto.

[Ver Texto](#)

(40) Domínguez de Olazábal, I. (2023), «Una batalla desigual también en las redes sociales», *El País*, 21 de octubre de 2023.

[Ver Texto](#)

(41) Martínez Martínez, R. (2023), *El caso Tik Tok: geoestrategia, internet y derechos fundamentales*, Cinco Días . El País, 13 abril 2023.

[Ver Texto](#)