

La regulación de la desinformación en el derecho digital europeo

Moisés Barrio Andrés | Letrado, Consejo de Estado | @moisesbarrioa X

Tema

Vivimos inmersos en una ciberdemocracia, donde el ejercicio de las prácticas políticas está vinculado a la imprescindible utilización de las redes sociales. Pero, al mismo tiempo, los bulos y la desinformación representan una amenaza global para la libertad y para la democracia de los Estados.

Resumen

El Reglamento europeo de Servicios Digitales pretende abordar, mediante unos instrumentos de autorregulación supervisada, los problemas que suponen para las libertades informativas –el derecho a la información y a la libertad de expresión– los contenidos ilícitos y nocivos. Su principal objetivo es la creación de un espacio seguro digital tanto para las plataformas como para los usuarios, introduciendo nuevas obligaciones para luchar contra estos contenidos, aunque no son suficientes.

Análisis

1. Introducción

Uno de los grandes temas del derecho digital europeo es la regulación de la desinformación –o más bien, de los desórdenes informativos en general–, especialmente la que circula por las plataformas de redes sociales. El problema de fondo es que la desinformación no es, *per se*, ilegal, salvo que supere cierto umbral que ponga en riesgo los valores e instituciones democráticos. Por lo general, se tratará de contenido legal pero dañino o tóxico.

Con el inicio de la andadura de las redes sociales, Estados Unidos (EEUU) y la Unión Europea (UE) estimaron que la desinformación en Internet no podía regularse eficazmente sin limitar los derechos individuales. Por eso, en la década de 2010 se estimó que la regulación significaba dar demasiado poder a un único actor para decidir, de forma subjetiva, si un contenido debía clasificarse como nocivo. Tal poder podría utilizarse fácilmente para obtener beneficios políticos, y también habría llevado a ciertos Estados autoritarios a dictar lo que sus ciudadanos podían oír y decir. Las plataformas de redes sociales, por su parte, argumentaron que vigilar y eliminar contenidos sería imposible debido a la enorme cantidad de publicaciones existentes en sus plataformas. Ante tales retos, las respuestas jurídicas siguieron siendo tímidas. Por ejemplo, el servicio diplomático de la UE decidió lanzar, en 2015, un servicio de contrapropaganda, EUvsDisinfo.

Sin embargo, desde 2017, varios incidentes que afectaron a políticos de alto rango han cambiado la tendencia. En 2017, Emmanuel Macron fue blanco reiterado de “bots” rusos mientras hacía campaña para la presidencia de Francia; en 2018, el escándalo de Cambridge Analytica sacó a la luz cómo los actores políticos utilizaban anuncios dirigidos para aumentar el impacto de sus campañas de desinformación; en 2019, Nancy Pelosi, la entonces presidenta de la Cámara de Representantes de EEUU, luchó para que se retirara un vídeo falsificado de ella (un *deep fake*); en 2020, en plena pandemia del COVID-19, Twitter comenzó a marcar las publicaciones del entonces presidente Donald Trump por contener información inexacta sobre la enfermedad. Otros incidentes posteriores también desempeñaron un papel a la hora de iniciar cambios jurídicos, sobre todo a raíz de la pandemia y de la guerra de Rusia con Ucrania, junto con el auge de la Inteligencia Artificial (IA).¹

2. El camino a la regulación

Estos acontecimientos llevaron a algunos Estados miembros de la UE a aprobar su propia legislación nacional para hacer frente a la desinformación. Alemania inició el debate sobre la Ley de aplicación de redes (*Netzwerkdurchsetzungsgesetz* o NetzDG) en 2015 (y la aprobó en 2017), una ley concebida originalmente para combatir los contenidos de odio en línea, pero ampliada después para incluir las *fake news* tras las elecciones presidenciales estadounidenses de 2016. En Francia, al tomar posesión a principios de 2018, el gobierno de Macron presentó en el Parlamento la *Loi contre la manipulation de l'information*, que se aprobó en noviembre del mismo año. La ley francesa otorga a un juez 48 horas para pronunciarse sobre las cuestiones planteadas por cualquier particular para detener la difusión de información falsa en los servicios de comunicación pública en línea, cuando sea probable que altere la autenticidad de un proceso electoral. En España se han presentado varias proposiciones legislativas sobre desinformación y noticias falsas de las que se deduce el vínculo con la seguridad, aunque todas ellas han resultado fallidas hasta la fecha. La última es de 2024, lleva por título “Proposición de Ley Orgánica de garantía del derecho a la información veraz y lucha contra la desinformación” y fue propuesta por el partido Podemos.

A nivel de la UE, de manera paralela, la introducción en 2018 del Código de buenas prácticas en materia de desinformación de la Unión antes de las elecciones al Parlamento Europeo de 2019 fue seguida con la propuesta, en 2020 y ya de una norma jurídica, del Reglamento europeo de Servicios Digitales. Pretende abordar el mismo problema, a saber, el contenido ilegal (y no el contenido dañino más amplio, que es más difícil de precisar). La propuesta ya es norma jurídica de directa aplicación en todos los Estados miembros desde febrero de 2024: el Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales o DSA, por sus siglas en inglés).

¹ Rubio Núñez, Rafael, Franco Alvim, Frederico y De Andrade Monteiro, Vitor (2024), *Inteligencia artificial y campañas electorales algorítmicas. Disfunciones informativas y amenazas sistémicas de la nueva comunicación política*, Centro de Estudios Políticos y Constitucionales, Madrid.

3. El Reglamento europeo de Servicios Digitales

El Reglamento europeo de Servicios Digitales² trata de atajar no sólo las distorsiones informativas (desinformación), sino también la difusión de contenidos ilícitos (en particular el discurso de odio, la difusión de contenidos ilícitos entre menores, la publicidad ilícita, la segmentación de la información y la manipulación de servicios con efecto en los procesos democráticos y la seguridad pública, entre otros). De forma similar, también aborda la utilización de los servicios de intermediación para la comisión de delitos o la realización de actividades ilícitas, como la venta de productos y servicios prohibidos.

Además, la norma pretende que las plataformas de redes sociales con más de 45 millones de usuarios en la UE sean más responsables de lo que ocurre en sus servicios. Las nuevas obligaciones incluyen un requisito obligatorio de “notificación y acción”, la motivación obligatoria de las decisiones de retirada de contenidos y un marco exhaustivo de gestión de riesgos y auditoría.

El Reglamento DSA ha intentado abordar la desinformación en su sentido más amplio posible para incluir la información falsa, la influencia de las operaciones de servicios de inteligencia extranjeros y la manipulación de la información. Pero en oposición al planteamiento de Francia, que otorga a la autoridad judicial un plazo ajustado para resolver los casos, el Reglamento DSA hace recaer en las plataformas, especialmente en las que denomina “plataformas en línea de muy gran tamaño”, la responsabilidad de adoptar salvaguardias y ser transparentes al respecto (por ejemplo, el art. 14 sobre las restricciones de publicación de contenidos que deben reflejarse en las condiciones de uso, así como el art. 17 sobre la notificación motivada de cuentas suspendidas y el art. 34 sobre la evaluación del riesgo sistémico). Y encomienda a la ciudadanía el peso fundamental de la labor de vigilancia y denuncia.

Sin embargo, la norma sigue manteniendo exenciones para los proveedores de servicios intermediarios en cuanto a su responsabilidad por los contenidos (arts. 4-6), como continuación de los artículos 14-15 de la Directiva sobre comercio electrónico de 2000 (Directiva 2000/31/CE), que ya había eliminado esta responsabilidad al tratar a los proveedores intermediarios como meros transmisores de información (con salvedades) y no exigía ninguna obligación general de supervisar los contenidos.

Existen, por tanto, requisitos asimétricos, con la definición de plataformas en línea de muy gran tamaño como aquellas “que tengan un promedio mensual de destinatarios del servicio activos en la Unión igual o superior a cuarenta y cinco millones” (art. 33). El Reglamento DSA las distingue para frenar el riesgo sistémico de desinformación, obligándolas a: revisar “diligentemente” sus algoritmos (art. 34); personalizar y ajustar sus sistemas de recomendación (art. 27); disponer de mecanismos para notificar posibles casos de desinformación (art. 16); y publicar auditorías anuales (art. 37). En concreto, respecto de la desinformación, el considerando 84 del Reglamento DSA indica que: “Por consiguiente, dichos prestadores deben dedicar especial atención a

² Un examen breve lo he realizado en Barrio Andrés, Moisés (2022), “Avanzando en la soberanía digital europea: los reglamentos DSA y DMA”, en ARI, 43/2022, Real Instituto Elcano; y de forma más extensa en Barrio Andrés, Moisés (2024), *Manual de Derecho digital*, Ed. Tirant lo Blanch, 3ª edición.

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”.

Además de detectar y de llevar a cabo la evaluación, el Reglamento 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).

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

La norma no ha estado exenta de críticas, por ejemplo, que las plataformas no tienen que ser transparentes sobre cómo toman las decisiones relativas a la moderación de contenidos y que la división entre las diferentes autoridades para hacer cumplir la norma –en particular, entre el Coordinador de Servicios Digitales a nivel de los Estados miembros y la Comisión Europea– podría causar tensiones. Otra crítica ha sido la “excesiva” confianza en los mecanismos de transparencia con pocas pruebas de que los usuarios se comporten de manera diferente cuando se les presenta más información. En España, la Comisión Nacional de los Mercados y la Competencia (CNMC) ha sido designada por el gobierno como nuestro Coordinador de Servicios Digitales, si bien está pendiente la promulgación de una norma con rango de ley para completar dicha designación (y que tenía que haber sido aprobada antes del pasado 17 de febrero de 2024). El incumplimiento de España, que también se ha producido por parte de Bélgica, Croacia, Luxemburgo, los Países Bajos y Suecia, ha desembocado en la incoación el 25 de julio de 2024 de los correspondientes [procedimientos de infracción por parte de la Comisión Europea](#).

Conclusiones

Los efectos de la desconfianza de los ciudadanos en las redes sociales como canal de información ya son perceptibles. Por ejemplo, la base de usuarios de Facebook ha comenzado a disminuir desde 2022.³

El Reglamento DSA ha creado un marco unificado que cubra a todos los nuevos sujetos intermediarios en el proceso de comunicación digital (plataformas digitales, redes sociales, servicios de alojamiento y otros servicios intermediarios, como los motores de búsqueda) tratando de definir un estatuto que comprenda “un conjunto claro, eficaz, predecible y equilibrado de obligaciones armonizadas de diligencia debida” para garantizar la transparencia y la responsabilidad en su labor de intermediación, atendiendo a los servicios que prestan y a su tamaño como indicador del eventual riesgo que pueden ocasionar para los usuarios.

No obstante, esta norma no está exenta de polémica ya que otorga una función de fiscalización enorme a empresas privadas transnacionales. La evolución futura probablemente pasará por una mayor corresponsabilidad directa del usuario y de la propia plataforma, en la línea de lo avanzado por la [Sentencia del Tribunal Europeo de Derechos Humanos de 15 de mayo de 2023, *Sánchez contra Francia*](#). También los Estados miembros podrían determinar que ciertos tipos de desinformación sean considerados como ilícitos, pues son los jurídicamente competentes para ello, siguiendo el modelo de Francia.

³ Thubron, Rob (2022), “Meta shares plunge 20% after Facebook user numbers fall for the first time ever”, en *Techspot*, 3/11/2022.