

Inteligencia artificial aplicada por las plataformas en línea y motores de búsqueda de muy gran tamaño para mitigar los riesgos sistémicos en línea*

Artificial intelligence applied by very large online platforms and search engines to mitigate systemic online risks

JOSÉ JUAN CASTELLÓ PASTOR

*Profesor titular de Derecho internacional privado
Universitat de València*

ORCID ID: 0000-0002-7517-0296

Recibido: 08.12.2024 / Aceptado: 15.01.2025

DOI: 10.20318/cdt.2025.9331

Resumen: En los últimos años, el uso de la inteligencia artificial para la moderación de contenidos se ha convertido en una práctica habitual entre las grandes plataformas en línea y buscadores. Estos sofisticados sistemas algorítmicos desempeñan funciones esenciales al detectar, restringir y eliminar con celeridad contenidos considerados ilícitos (o incompatibles con las condiciones generales) en la red. Esta creciente utilización de la inteligencia artificial responde al exponencial incremento del volumen de datos y al ritmo acelerado de creación y difusión de contenidos en internet. Sin embargo, su aplicación requiere ser tratada con cautela porque puede conducir a resultados equívocos con el consiguiente impacto negativo en los derechos y libertades constitucionalmente protegidos de los usuarios digitales. Un desafío que puede verse agravado aún más por la necesidad de estos oligarcas tecnológicos de dirigir sus esfuerzos en atenuar los “contenidos incorrectos o engañosos, incluida la desinformación” por el riesgo sistémico relacionado con sus servicios.

Palabras clave: riesgos sistémicos, inteligencia artificial, algoritmo, motores de búsqueda, plataformas en línea.

Abstract: In recent years, the use of artificial intelligence for content moderation has become a prevalent practice among major online platforms and search engines. These sophisticated algorithmic systems perform vital functions, namely the rapid detection, restriction and removal of content deemed illegal (or otherwise incompatible with the terms and conditions) on the web. This increasing utilization of artificial intelligence is a response to the exponential growth in the volume of data and the volume and the accelerated pace of content creation and dissemination on the internet. However, its implementation requires caution to avoid misleading results and the consequent negative impact on the constitutionally protected rights and freedoms of digital users. This challenge may be further exacerbated by the need for these technological oligarchs to direct their efforts at mitigating “incorrect or misleading content, including misinformation” due to the systemic risk associated with their services.

Keywords: systemic risks, Artificial Intelligence, algorithm, online search engines, online platforms.

* Esta publicación es parte del Proyecto TED2021-129307A-I00 financiado por MICIU/AEI/10.13039/501100011033 y por la Unión Europea NextGenerationEU/ PRTR, denominado *Hacia una transición digital centrada en la persona en la Unión Europea* IP. José Juan Castelló Pastor.

Sumario: I. Planteamiento inicial. II. Moderación de contenidos en línea: ¿mecanismo necesario para fortalecer la confiabilidad en el entorno digital? 1. La moderación proactiva de contenidos como herramienta para combatir contenidos y cuentas que violan las normas o políticas internas de las plataformas en línea y buscadores. A) Destacado uso de mecanismos automatizados en la moderación de contenidos en línea. B) Actuales desafíos por el empleo de mecanismos automatizados en la moderación de contenidos en línea. III. Riesgos de carácter sistémico y medidas de obligatoria observancia frente a ellos. 1. Marco jurídico digital uniforme para las actividades de internet en la Unión Europea. A) ¿Proteccionismo encubierto? El carácter imperativo de las reglas del Reglamento (UE) de servicios digitales a las tecnológicas situadas en terceros Estados. B) David c. Goliath: tutela jurídico-pública y privada del nuevo marco jurídico-digital. 2. Disposiciones de obligada observancia con respecto a la moderación de contenidos en el Reglamento (UE) de servicios digitales. 3. Comportamiento responsable y diligente frente al riesgo sistémico, pero ¿quién? IV. Reflexión final.

I. Planteamiento inicial

1. El pasado mes de octubre, las plataformas en línea y los motores de búsqueda en línea de muy gran tamaño informaron a la Comisión Europea sobre las actividades de moderación de contenidos, las medidas adoptadas en relación con la disponibilidad, visibilidad y accesibilidad de la información facilitada por el destinatario del servicio, así como de cualquier otra restricción o suspensión de contenidos o de cuentas de los usuarios, entre otros datos, del segundo trimestre de 2024 de acuerdo con los requisitos de transparencia fijados en los artículos 15, 24 y 42 del Reglamento (UE) de servicios digitales¹, aplicable en todos los Estados miembros desde el 17 de febrero de 2024², aunque algunas de sus disposiciones tuvieron una fecha de aplicación anterior³.

Los informes facilitados por el conglomerado tecnológico Meta, que incluye plataformas como Instagram y Facebook; por Alphabet, la empresa matriz de Google y YouTube; por la red social X y por Tik-Tok, por mencionar algunos populares servicios digitales, muestran un significativo volumen de datos sobre la moderación de contenidos, denuncias y restricciones de visibilidad de contenidos en la red. Estos informes también revelan que, en promedio, alrededor de un setenta por ciento de estas decisiones se realizan utilizando sistemas completamente automatizados⁴.

2. Estos conocidos actores digitales vienen implementando desde hace tiempo políticas de moderación que comporta la eliminación de millones de contenidos y cuentas que infringen sus propias directrices del servicio. Y como se ha referido, en su mayoría, son procesos llevados a cabo de forma automatizada mediante el uso de tecnología avanzada, actualmente, basada en la inteligencia artificial⁵.

¹ 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, en adelante: Reglamento (UE) de servicios digitales (o RSD). OJ L 277, 27.10.2022, p. 1–102.

² Véase el art. 93 RSD sobre la entrada en vigor y aplicación.

³ De acuerdo con el art. 33.4 RSD, se estableció la obligación de informar sobre el promedio mensual de destinatarios del servicio activos en la Unión antes del 17 de febrero de 2023. Posteriormente, el 25 de abril de 2023, la Comisión Europea designó como plataformas en línea de muy gran tamaño a Alibaba Aliexpress, Amazon Store, Apple, AppStore, Booking.com, Facebook, Google Maps, Google Play, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, Youtube y Zalando; y motores de búsqueda en línea de muy gran tamaño a Bing y Google Search, según lo establecido en el artículo 33.6 del RSD y publicado en el Diario Oficial de la Unión Europea DO C 249/2 del 14 de julio de 2023. Este listado puede estar sujeto a cambios, tal y como ha sucedido: a fecha 18 de octubre de 2024, la Comisión Europea ha reconocido un total de 23 servicios de gran tamaño: 21 como VLOPs y 2 como VLOSEs. Además de los indicados, se han incorporado las plataformas: Pornhub, Booking.com, Shein, Stripchat, Xvideos. Para más información sobre la “supervisión de las plataformas en línea y los motores de búsqueda de muy gran tamaño designados en virtud de la Ley de Servicios Digitales” visítense la página de la Comisión: digital-strategy.ec.europa.eu (última consulta 5.12.2024).

⁴ Información obtenida de la página web de la Comisión Europea “DSA Transparency Database” (disponible en: <https://transparency.dsa.ec.europa.eu>). Llegando la plataforma YouTube, por ejemplo, al 99,6 % de los 1.372.493.981 comentarios retirados fueron por detección automática (véase la nota al pie n.º 17).

⁵ Si bien precisa T. GILLESPIE, “Content Moderation, AI, and the Question of Scale”, *Big Data & Society*, 2020, vol. 7, n.º 2, p. 3 que “aunque algunas plataformas utilizan técnicas de aprendizaje automático para identificar nuevos casos de acoso, discursos de odio o pornografía, la mayoría realiza una sofisticada versión de la comparación de patrones: se limita a comparar el nuevo contenido con una lista negra de ejemplos ya conocidos. Esto es automatización, pero difícilmente es IA, salvo una definición lo más amplia posible”.

Con ello se permite dar una respuesta ágil y eficiente, sobre todo en aquellas situaciones donde el contenido subido a la plataforma en línea pueda comportar una significativa amenaza -v.g.: como las publicaciones referidas a terrorismo, abuso sexual infantil o incitación al suicidio- causando potenciales daños fuera del entorno virtual. O en situaciones donde el contenido puede volverse viral y rápidamente alcanzar una amplia audiencia (incluso mundial), siendo el empleo de esta tecnología fundamental para mitigar el alcance e impacto negativo del contenido (ilícito, dañino o nocivo), así como reducir el potencial daño que pueda causar esta viralización para afianzar, en definitiva, un entorno digital más seguro y confiable.

3. La implementación de herramientas algorítmicas para realizar tareas de moderación de contenidos se ha fortalecido considerablemente en los últimos años.

Y si bien pudieran ser idóneas por su eficacia ante el volumen de datos en la red y la rapidez en crearse y compartirse este contenido -porque una revisión llevada a cabo exclusivamente por un equipo humano sería inviable por la propia escala de datos y usuarios, así como por la propia dinámica de funcionamiento en la red-, las herramientas algorítmicas no están exentas de controversias y nuevos desafíos como se aborda en este estudio.

4. Sobre la base de este planteamiento descrito, se analiza en primer término la importancia de la moderación de contenidos en línea realizada de forma automatizada mediante el uso de tecnología avanzada por las plataformas en línea y los motores de búsqueda en línea de muy gran tamaño, así como las controversias y desafíos que presentan la inclusión de estos mecanismos algorítmicos. En segundo término, las disposiciones de obligada observancia a las plataformas en línea y motores de búsqueda de muy gran tamaño en materia de información, transparencia y rendición de cuentas para mitigar los riesgos sistémicos en línea con especial énfasis en el uso de la inteligencia artificial en el marco del Reglamento (UE) de servicios digitales.

II. Moderación de contenidos en línea: ¿mecanismo necesario para fortalecer la confiabilidad en el entorno digital?

1. La moderación proactiva de contenidos como herramienta para combatir contenidos y cuentas que violan las normas o políticas internas de las plataformas en línea y buscadores

5. Con más de 5.4 billones de personas conectadas globalmente⁶ y una creciente tendencia hacia la participación activa del usuario en la red, donde crea su propio contenido y comparte información en línea, la moderación de contenidos constituye, sin duda alguna, un mecanismo de gobernanza indispensable para estructurar la dinámica participación de los usuarios en estos espacios virtuales, facilitar el acceso a la información en la red, prevenir y combatir el incremento de contenidos y actividades ilícitas (o incompatibles con sus directrices) y de cuentas infractoras por parte de estos actores digitales.

6. La moderación de contenidos es definida por la doctrina como “el mecanismo de gobernanza que estructura la participación en una comunidad para facilitar la cooperación y evitar los abusos⁷” o “el conjunto de prácticas utilizadas por las plataformas en línea para hacer cumplir sus directrices sobre contenidos aceptables⁸”, y por el legislador 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

⁶ Según la página web *statista* (última consulta el 5.12.2024).

⁷ J. GRIMMELMANN, “The virtues of moderation”, *Yale Journal of Law & Technology*, n.º 17, 2015, p. 47.

⁸ B. GANESH Y J. BRIGHT, “Countering extremists on social media: challenges for strategic communication and content moderation”, *Policy & Internet*, vol. 12, n.º 1, 2020, p. 8.

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 servicio⁹. Y si bien, indudablemente, representa un mecanismo esencial de gobernanza en el entramado virtual, la falta de transparencia por parte de los gigantes tecnológicos puede ensombrecer el buen propósito de estos mecanismos¹⁰.

7. Las políticas proactivas de moderación de contenidos incentivadas por el legislador¹¹ contribuyen a la eliminación de millones de publicaciones y de cuentas de usuarios que infringen sus normas o políticas internas, siendo en este punto relevante el diseño empleado en estos procedimientos.

De este modo, los gigantes tecnológicos principalmente recurren a mecanismos algorítmicos, aunque también cuentan con equipos humanos encargados de identificar, revisar y aplicar o ejecutar las medidas correspondientes de millones de contenidos diarios subidos a las más conocidas redes sociales. En consecuencia, el control y la gestión privada de los contenidos en la red se encomienda tanto a la tecnología avanzada como a la intervención humana, o a un enfoque híbrido que combina ambas metodologías¹².

8. Cada uno de estos modelos que regulan la aplicación y ejecución de las políticas internas (o los términos y condiciones generales) del servicio digital y, por lo tanto, el comportamiento en línea de los usuarios¹³, presentan ventajas e inconvenientes.

A este respecto, la moderación algorítmica es ciertamente eficaz porque procesa de forma rápida la escala masiva de datos publicados en la red, pero no debe obviarse que es un algoritmo el encargado de aplicar las condiciones generales del servicio digital, con el riesgo que podría suscitar para la salvaguarda de los derechos fundamentales de los usuarios en la red. Creado este *leviatán algorítmico*¹⁴, el dilema radica en la imprecisión y el posible sesgo¹⁵ de sus decisiones, además de la falta de transparencia en el funcionamiento del propio sistema algorítmico.

En cambio, la moderación encomendada a un equipo humano implica una menor rapidez -necesaria sin duda en el entorno digital- en la toma de estas decisiones, al margen de no solventar el aspecto del sesgo, porque también las personas se ven influenciadas por sus valores y principios al tomar cualquiera de estas decisiones. Es por ello por lo que el enfoque híbrido, que combina el mecanismo automatizado y en algunos supuestos la revisión del equipo del servicio digital, es el más utilizado por las grandes plataformas en línea y motores de búsqueda: eliminan automáticamente cualquier contenido lesivo y, específicamente señala Facebook, sólo el contenido de alta gravedad “con potencial para causar

⁹ Vid. art. 3 letra t) RSD.

¹⁰ Como afirma T. GILLESPIE, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, New Haven: Yale University Press, 2018, p. 198 que “los llamamientos a una mayor transparencia en la crítica de las redes sociales son tan habituales que casi resultan vacuos. Pero el funcionamiento de la moderación de contenidos en la mayoría de las plataformas de redes sociales es escandalosamente opaco, y no por casualidad”.

¹¹ A lo largo de los años, la Comisión Europea ha firmado diversos acuerdos con grandes tecnológicas para fomentar un entorno digital más seguro. Uno de estos acuerdos es el *Código de conducta para combatir el discurso de odio ilegal en línea* para prevenir y contrarrestar la propagación del discurso de odio ilegal en línea, creado en 2016 junto con Facebook, Microsoft, Twitter y YouTube y al que se han sumado otras compañías tecnológicas con el tiempo. En 2018, la Comisión lanzó el *Código de Prácticas sobre Desinformación*, que se ha revisado recientemente con el *Código de Buenas Prácticas en materia de Desinformación 2022* (disponible en <https://digital-strategy.ec.europa.eu/es/policies/code-practice-disinformation>). Además, una novedad importante en la moderación proactiva de contenidos es su incorporación en el art. 7 RSD, en similares términos, de la conocida cláusula del buen samaritano estadounidense, referido *infra* en el apartado III.2 de este trabajo.

¹² K. KLONICK, “The New Governors: The People, Rules, and Processes Governing Online Speech”, *Harvard Law Review*, 2018, vol. 131, p. 1635.

¹³ Las plataformas en línea y motores de búsqueda configuran libremente sus políticas internas de funcionamiento del servicio y con ello delimitan el perímetro de los derechos de los usuarios del servicio. Es decir: el usuario de un servicio digital que acepta sus términos y condiciones está asumiendo las directrices de uso y convivencia con la plataforma en línea, pero también con respecto a otros usuarios de la plataforma.

¹⁴ K. CREEL Y D. HELLMAN, “The Algorithmic Leviathan: Arbitrariness, Fairness, and Opportunity in Algorithmic Decision-Making Systems”, *Canadian Journal of Philosophy*, 2022, vol. 52, pp. 26-43.

¹⁵ Así lo indica la profesora S. BARONA VILAR, *Algoritmos de Derecho y de la Justicia. De la Inteligencia Artificial a la Smart Justice*, Tirant Lo Blanch, Valencia, 2021, p. 170.

daños fuera de línea (por ejemplo, mensajes relacionados con el terrorismo y el suicidio) y a los contenidos virales que se propagan rápidamente y tienen el potencial de llegar a una gran audiencia, con el fin de evitar el mayor daño posible”¹⁶ es revisado por el equipo humano.

A) Destacado uso de mecanismos automatizados en la moderación de contenidos en línea

9. Los datos reflejan un manifiesto uso de los mecanismos automatizados, incluyendo aquellos basados en la inteligencia artificial, en la moderación de contenidos que permite a estos actores digitales detectar, restringir y eliminar contenidos ilícitos o incompatibles con sus condiciones generales. A modo de ejemplo, YouTube eliminó en el segundo trimestre de 2024 un total de 1.372.493.981 comentarios de los que el 99,6 % fueron retirados por detección automática¹⁷.

10. Con todo, por más que estos sistemas algorítmicos pudieran ser apropiados para gestionar el volumen de datos y la rapidez a la que se crea y comparte el contenido e información en la red en busca de entornos digitales más seguros y confiables, es importante tomar en consideración si estos mecanismos automatizados empleados justifican esta encomiable finalidad.

11. La insuficiente precisión y especialmente la presencia de sesgos en la moderación algorítmica de contenidos, como se ha referido, pueden conducir a resultados erróneos con el consiguiente impacto negativo en el ejercicio de los derechos y libertades constitucionalmente protegidos, como la libertad de expresión y de información¹⁸.

Cabe subrayar, a este respecto, que el Reglamento admite explícitamente la tasa de error de los sistemas algorítmicos al establecer que los intermediarios que utilicen estos medios automatizados para moderar contenidos deben incluir “una descripción cualitativa, una especificación de los fines precisos, los indicadores de la precisión y la posible tasa de error de los medios automatizados empleados para cumplir dichos fines, y las salvaguardias aplicadas” en los informes relacionados con las disposiciones de transparencia informativa¹⁹.

12. De este modo, el interrogante que plantea el empleo de estos mecanismos automatizados radica en la complejidad que enfrentan los sistemas algorítmicos para diferenciar entre la licitud y la ilicitud del contenido publicado en internet, en la medida en que se trata de una consideración que no depende únicamente del contexto en el que se realiza la publicación sino también de la intencionalidad subyacente del autor. Y estas herramientas algorítmicas no suelen tener en cuenta todos estos datos contextuales²⁰. Más aún, resulta ciertamente complejo entrenarlos con datos que puedan advertir el contexto histórico, cultural o político, o distinguir el uso satírico, educativo o informativo de cualquier expresión publicada en la red²¹.

13. En consecuencia, pese a permitir a los intermediarios detectar y reaccionar rápidamente frente al exponencial incremento de comportamientos ilícitos y nocivos en la red, la idoneidad del uso de

¹⁶ De acuerdo con el informe de transparencia facilitado por Meta el 27 de octubre de 2023 a la Comisión Europea (disponible en: <https://transparency.dsa.ec.europa.eu>).

¹⁷ De acuerdo con los datos facilitados por YouTube a la Comisión Europea (disponible en: <https://transparency.dsa.ec.europa.eu>).

¹⁸ F. LLANO ALONSO, *Homo ex machina. Ética de la inteligencia artificial y Derecho digital ante el horizonte de la singularidad tecnológica*, Valencia, Tirant Lo Blanch, 2024, p. 185 y ss.

¹⁹ Art. 15.1.e) RSD.

²⁰ N. ELKIN-KOREN y P. MAAYAN, “Guarding the guardians: content moderation by online intermediaries and the rule of law”, en G. FROSIO, *Oxford Handbook of Online Intermediary Liability*, Oxford Academic, 2020 (versión digital); D. KELLER, “Inception Impact Assessment: Measures to Further Improve the Effectiveness of the Fight Against Illegal Content Online” (disponible en: <https://ssrn.com/abstract=3262950>).

²¹ T. GILLESPIE, *Custodians of the Internet*, cit., p. 169; S. MYERS WEST, “Censored, suspended, shadowbanned: user interpretations of content moderation on social media platforms”, *New Media & Society*, 2018, vol. 20, n.º 11, pp. 4376-77.

la inteligencia artificial en estas herramientas requiere ser abordada con precaución porque puede llevar a resultados equívocos con respuestas que pueden ser inexactas, sesgadas o incluso discriminatorias²². Y es importante acentuar que el legislador de la Unión, como se ha mencionado, reconoce expresamente que los algoritmos utilizados para moderar contenidos pueden incurrir en errores²³.

14. A tal efecto, un resultado falso positivo implicaría identificar incorrectamente el contenido como ilícito (o contrario a las políticas internas del servicio digital), lo que incentivaría su censura, además de limitar injustamente la libertad de expresión del usuario por cuanto se eliminan contenidos evidentemente legítimos. A diferencia de un resultado falso negativo, que permitiría que el contenido permaneciera en la red, dando lugar a cierta impunidad al difusor de contenido²⁴.

B) Actuales desafíos por el empleo de mecanismos automatizados en la moderación de contenidos en línea

15. Sin perjuicio de lo expuesto, a mi modo de ver, la escasa transparencia de las políticas de detección automatizada de contenidos representa uno de los principales desafíos en la gobernanza de la red, en la medida en que se delega en estos algoritmos -creados por unos actores privados actualmente esenciales en la difusión y distribución de todo tipo de contenidos en la red²⁵- las acciones de sus usuarios, proporcionando o negando su servicio y amplificando o atenuando el discurso en la red²⁶. Y no debe subestimarse su importancia.

16. Los algoritmos que sustentan estas herramientas automatizadas son, ciertamente, los responsables de hacer cumplir las condiciones generales del servicio y de determinar, por lo tanto, lo que constituye un contenido ilícito, cuando ello depende del Derecho material aplicable al fondo de la controversia.

17. Una forma de eludir este aspecto conflictual por las tecnológicas es configurando en los términos y condiciones del servicio digital aquellos comportamientos que pueden realizar sus usuarios, de manera que un contenido (información, servicio o cuenta) podría ser lícito pero contrario a sus políticas internas (esto es: a las condiciones del servicio, las normas de la comunidad o las políticas de publicidad) y actuar automáticamente frente a su acceso y visibilidad en la red. De hecho, un análisis empírico realizado a partir de los datos de la *DSA Transparency Database* es revelador en este sentido: “el 99,8% se notifican como violación de las condiciones de servicio y solo el 0,2% como contenido ilegal”²⁷.

²² E. DOUEK, “Content moderation as systems thinking”, *Harvard Law Review*, 2022, vol. 136, p. 548. De hecho, el propio Reglamento (UE) de servicios digitales reconoce que los algoritmos de moderación de contenidos pueden cometer errores, de acuerdo con el cdo. n.º 26 RSD.

²³ De acuerdo con el cdo. n.º 26 RSD.

²⁴ E. LLANSÓ, J. VAN HOBOKEN, P. LEERSSEN y J. HARAMBAM, “Artificial Intelligence, Content Moderation, and Freedom of Expression”, *Working paper of the Transatlantic Working Group on Content Moderation Online and Freedom of Expression*, 2020, p. 7.

²⁵ Es sabido que las plataformas en línea son actores (privados) esenciales de la actual sociedad con una función de intermediación clave para la actividad económica, social o cultural. En efecto, realizan actualmente una función esencial en todos los sectores de la Unión Europea por facilitar la interacción entre usuarios, operadores económicos y también con los organismos públicos a través de la red. En este sentido favorecen el acceso a la información, la comunicación de los usuarios y mejoran los mercados al permitir la conexión entre todos ellos. No obstante, esta fuerte influencia (e incluso también dependencia) en nuestras vidas diarias pudiera carecer de mayor trascendencia si no fuera por el excesivo poder en manos de unas pocas grandes empresas tecnológicas cuyas acciones, a menudo desprovistas de transparencia, implican en ocasiones importantes desafíos individuales y a la sociedad global en su conjunto.

²⁶ Como señala K. KLONICK, “The New Governors”, cit., p. 1630: la configuración de estas normas de moderación puede afectar al discurso público, a la información en la red y a los derechos individuales de libertad de expresión.

²⁷ R. KAUSHAL, J. VAN DE KERKHOFF, C. GOANTA, G. SPANAKIS y A. IAMNITCHI, “Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database”, 2024, p. 7 (disponible en: <https://doi.org/10.48550/arXiv.2404.02894>).

18. A la luz de lo expuesto, resulta fundamental hacer hincapié que la ausencia de un marco normativo exhaustivo que regule de la gobernanza de los servicios digitales a lo largo de los años ha permitido que estos actores privados formulen y apliquen sus propias políticas internas de cumplimiento. Se puede afirmar, en este sentido, que tácitamente se creó un *ius tecnológico* impropio. Ello implica indirectamente que la regulación de la sociedad digital esté en manos de unos pocos gigantes tecnológicos, que gestionan el acceso y la visibilidad de la información en la red, ganando cada vez más relevancia para el funcionamiento del ecosistema digital.

Efectivamente, estas últimas décadas muestran el poder sistémico adquirido por unos pocos oligarcas tecnológicos, que no debería tener mayor relevancia si no fuera por la gestión de este poder, en ocasiones de un modo arbitrario, que puede conculcar directa o indirectamente los derechos fundamentales de los usuarios de internet, sobre la base contractual de unos términos y condiciones, dicho sea de paso, aceptados bajo técnicas que complican su lectura²⁸.

19. Este control del poder de las plataformas en línea y motores de búsqueda guarda cierta similitud con la estructura de un Estado. Como se afirma con buen criterio²⁹, estos sujetos privados se constituyen como verdaderos sistemas jurídicos en tanto ejercen -sobre sus usuarios y en su propia “jurisdicción”- un poder regulatorio, ejecutivo y judicial, obviamente con la permisividad de la Ley del Estado de su constitución y de la Ley del Estado donde dirija su actividad. En este sentido, el usuario que acepta las condiciones generales (y/o directrices) del servicio asume las reglas y se obliga al cumplimiento, so pena de ser sancionado³⁰. De ahí, desde mi punto de vista, este *ius technologicum* que podría considerarse, en cierto sentido, como impropio.

20. Ahora bien, el alcance de estas políticas internas del servicio digital va más allá del usuario (a título individual), afectando indirectamente a la sociedad en su conjunto, puesto que, en última instancia, son estos actores privados quienes determinan el acceso y la visibilidad del contenido disponible en internet, pudiéndose afirmar sin ambages que el ecosistema digital se ve intervenido por unos oligarcas tecnológicos que desempeñan, con sus herramientas algorítmicas dotadas de un velo de opacidad, un papel decisivo en el contenido disponible en la red y, por lo tanto, en el ejercicio de las libertades fundamentales de la sociedad en su conjunto.

21. En este contexto, una preocupación de las autoridades europeas ciertamente viene por la escasa transparencia de las plataformas en línea en relación con algunas de sus prácticas, de ahí el interés por entender y supervisar estas acciones realizadas por estos actores privados para prevenir a todas luces cualquier resultado injusto o arbitrario derivado de su omnímodo poder, como se analiza seguidamente.

²⁸ Sobre este punto, véase: J.J. CASTELLÓ PASTOR, “Interrelación del Reglamento (UE) de servicios digitales con el Reglamento *platform to business* (p2b): el necesario contrapeso de la Unión Europea al poder de las plataformas en línea”, en J.J. CASTELLÓ PASTOR (dir.), *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024 (versión digital).

²⁹ Entre nuestra doctrina, véase a T. RODRÍGUEZ DE LAS HERAS BALLELL, “Las plataformas: nuevos actores (y reguladores) de la actividad económica”, *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid*, 2021, n.º Extra-2, pp. 403, 405-406. Señala esta autora que las plataformas en línea emergen como “reguladores, supervisores, creadores de comunidades para el ejercicio de derechos y libertades” [...] y “aspiran a emular internamente un sistema jurídico, con sus normas, sus fórmulas de supervisión y sus mecanismos de resolución de disputas” [...]. Las plataformas en línea “se esfuerzan por crear espacios autorregulados, auténticas comunidades, que se superponen a los sistemas estatales de regulación, supervisión y resolución (esencialmente) judicial de los conflictos”. En misma línea, entre otros: K. KLONICK, “The New Governors”, cit., p. 1647; N. ELKIN-KOREN y P. MAAYAN, “Guarding the guardians”, cit., pp. 89-93.

³⁰ Esta “medida disciplinaria o sanción” impuesta al destinatario del servicio, que podría ser generada por estas herramientas algorítmicas, podría incluir, entre otras: la disponibilidad, visibilidad y accesibilidad del contenido o de la información en la red, el bloqueo o supresión de este contenido publicado, así como de la supresión o suspensión de la cuenta del usuario.

III. Riesgos de carácter sistémico y medidas de obligatoria observancia frente a ellos

1. Marco jurídico digital uniforme para las actividades de internet en la Unión Europea

22. Plenamente aplicable en todos los Estados miembros desde el 17 de febrero de 2024³¹, el Reglamento (UE) de servicios digitales crea un conjunto uniforme de reglas aplicables exclusivamente a los intermediarios³² -y en su mayoría especialmente dirigidas a las plataformas en línea³³- que tiene por meritorio objetivo contribuir al correcto funcionamiento del mercado interior de la Unión Europea, en consonancia con la Directiva de comercio electrónico, su predecesora³⁴.

Este reglamento sustantivo de la Unión efectivamente configura un marco horizontal de exenciones condicional de responsabilidad de estos actores digitales³⁵ y un conjunto armonizado de obligaciones asimétricas, siendo de singular relevancia las disposiciones dirigidas específicamente a las plataformas en línea muy grandes y a los motores de búsqueda muy grandes para evaluar y gestionar los riesgos sistémicos: esto es, prevenir las actividades ilícitas y nocivas en línea y la difusión de desinformación, garantizar la seguridad de los usuarios, proteger los derechos fundamentales y consolidar, en definitiva, un entorno digital más justo y abierto³⁶. También establece un conjunto de normas sobre la aplicación y ejecución del propio texto normativo.

23. En un contexto marcadamente transfronterizo, a mi modo de ver, estas reglas sustantivas digitales logran un avance significativo hacia la uniformidad en la protección de los derechos fundamentales en toda la Unión Europea. Se evitan las posibles divergencias entre las legislaciones de los Estados miembros que dificultan la libre circulación de servicios en el mercado de la Unión y se garantiza una protección uniforme de los derechos y obligaciones, tanto de los operadores económicos como de los usuarios digitales en toda la Unión Europea. Esta uniformidad es esencial para reducir la fragmentación jurídica y ofrecer una mayor seguridad jurídica, que se veía anteriormente comprometida, por ejemplo, con la Directiva sobre el comercio electrónico³⁷.

24. Por cuestiones de limitación de espacio, en este epígrafe se analiza el alcance del Reglamento (UE) de servicios digitales y en el siguiente epígrafe las disposiciones más relevantes de obligada observancia en relación con la moderación y curación de contenidos en la red por parte de las plataformas en línea y motores de búsqueda.

³¹ Aunque, como se ha referido, algunas de sus disposiciones tuvieron una fecha de aplicación anterior, *vid. supra* nota al pie n.º 3.

³² Si bien se hace referencia en este trabajo indistintamente al término “servicios digitales”, es cierto que el RSD no lo utiliza, sino que se refiere al “servicio de la sociedad de la información” definido en el artículo 1.1 b) de la Directiva (UE) 2015/1535, pero limita su ámbito al “servicio intermediario” y que se refiere únicamente a tres categorías de servicios de la sociedad de la información: el servicio de “mera transmisión”, el de “memoria caché” y el de “alojamiento de datos” (léase respectivamente el art. 3 letra a) y g) RSD).

³³ Incluye a las plataformas en línea en un subgrupo del “alojamiento de datos” a efectos fundamentalmente del cumplimiento de las obligaciones de diligencia, conforme lo matiza el cdo n.º 13 RSD.

³⁴ De acuerdo con el art. 89 RSD, la Directiva 2000/31/CE sobre el comercio electrónico continúa en vigor, sólo se suprimen los artículos 12 a 15 y estas referencias se entienden hechas a los arts. 4, 5, 6 y 8 RSD respectivamente.

³⁵ Que no se abordan en este estudio por cuestión de espacio, si bien véase: J.J. CASTELLÓ PASTOR, “Nuevo régimen de responsabilidad de los servicios digitales que actúan como intermediarios a la luz de la propuesta de Reglamento relativo a un mercado único de servicios digitales”, en J.J. CASTELLÓ PASTOR (dir.), *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales*, Aranzadi Thomson-Reuters, 2021, pp. 37-76; C. I. CORDERO ÁLVAREZ, “El régimen de responsabilidad de las plataformas online en la DSA ante contenidos ilícitos lesivos de derechos fundamentales: evolución de la figura de puerto seguro”, en J.J. CASTELLÓ PASTOR (dir.), *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024 (versión digital); A. GASCÓN MARCÉN, “La responsabilidad de los intermediarios de Internet en la Unión Europea: iniciativas recientes y perspectivas de futuro”, en J.J. CASTELLÓ PASTOR (dir.), *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales*, Aranzadi, 2021, pp. 133-160.

³⁶ De acuerdo con el art. 1 RSD.

³⁷ P. DE MIGUEL ASENSIO, *Derecho privado de internet*, 6.ª edición, Civitas Thomson-Reuters, 2022, p. 370; *Id.*: *Manual de Derecho de las nuevas tecnologías*, Aranzadi, 2023, p. 59.

A) ¿Proteccionismo encubierto? El carácter imperativo de las reglas del Reglamento (UE) de servicios digitales a las tecnológicas situadas en terceros Estados

25. Uno de los aspectos de mayor relevancia de este nuevo marco jurídico digital posiblemente sea el desafío que supone el cumplimiento de sus reglas uniformes para las grandes empresas tecnológicas que dominan el mercado de los servicios digitales, mayoritariamente establecidas en Estados Unidos y en China con millones de sus usuarios en la Unión Europea.

En este punto, la Comisión Europea ha sido explícita al acentuar que cualquier operador tecnológico situado fuera de la Unión que desee realizar actividades económicas en nuestro territorio debe cumplir con las normativas aquí establecidas. Y ha subrayado que se emplearán todos los recursos disponibles para garantizar el cumplimiento estricto de la legislación de la Unión Europea y de las normas internacionales, con el objetivo de asegurar condiciones equitativas en el entorno digital³⁸.

26. El legislador de la Unión reconoce efectivamente el reto que implica configurar un entorno digital más seguro, transparente y responsable con medidas de obligada observancia a todos los servicios digitales, incluso para aquellos que operan desde fuera de nuestro territorio, por el carácter intrínsecamente transfronterizo de internet, y lo alcanza, no sin cierta dificultad (a modo de ejemplo: el listado designando a las plataformas en línea de muy gran tamaño publicado en el Diario Oficial de la Unión Europea DO C 249/2 de 14.7.2023, conforme a lo dispuesto en el artículo 33.6 del Reglamento (UE) de servicios digitales, ha sido impugnado por varias tecnológicas como Zalando y Amazon ante el Tribunal General, asuntos T-348/23 y T-367/23 respectivamente, para no tener que cumplir así con todas las adicionales obligaciones impuestas a las muy grandes plataformas digitales³⁹) al someter el complejo cumplimiento de sus disposiciones con base en un criterio de conexión fáctico: se extiende su ámbito de aplicación espacial a los prestadores de servicios intermediarios con independencia de su lugar del establecimiento (domicilio o ubicación) en la medida en que ofrezcan sus servicios en el territorio de la Unión, de acuerdo con el artículo 2.1 del Reglamento (UE) de servicios digitales⁴⁰.

27. Este criterio de conexión tiene como objetivo garantizar la eficacia de las normas de la Unión como la equidad de condiciones a todos los operadores económicos en el mercado interior⁴¹, esencial en este contexto digital⁴². Aunque un problema adicional pudiera venir en la determinación del referido criterio fáctico para que sean aplicables las disposiciones de la normativa de la Unión Europea a estas empresas tecnológicas situadas en terceros Estados, se solventa con cierto éxito al referirse por “ofrecer un servicio en la Unión” como el hecho de “hacer posible que las personas físicas o jurídicas de uno o varios Estados miembros utilicen los servicios de un prestador de servicios intermediarios que tenga una conexión sustancial con la Unión”⁴³. Por su parte, especifica el propio instrumento que la conexión sustancial se da si el prestador tiene su establecimiento en la Unión, o bien -y he aquí el *quid* de la cuestión en la determinación de lo que constituye esta conexión sustancial- porque tiene un número

³⁸ Bruselas, 19.2.2020 COM (2020) 67 final.

³⁹ Igualmente pudo leerse en los medios de comunicación las reticencias de algunas tecnológicas como X (antes, Twitter) al cumplimiento de las medidas impuestas en el RSD, planteándose el bloqueo del servicio en toda la Unión (elconfidencial.com de 19.10.2023).

⁴⁰ Con mayor profundidad, S. FELIU ÁLVAREZ SOTOMAYOR, “Ámbito territorial y aplicación del principio del control en origen en el Reglamento UE de servicios digitales”, en J.J. CASTELLÓ PASTOR (dir.), *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024 (versión digital).

⁴¹ Cdo n.º 7 RSD.

⁴² Desde mi punto de vista es apropiado porque las grandes tecnológicas (de origen y residencia) estadounidenses o asiáticas, cuyos servicios son utilizados por millones de usuarios en la Unión, quedan sujetas al cumplimiento de las mismas medidas y estándares que los operadores económicos europeos. Aunque este enfoque pudiera desincentivar la prestación de servicios digitales en el territorio de la Unión, según C. SCHMON y K. GULLO, “European Commission’s Proposed Digital Services Act got several things right, but improvements are necessary to put users in control” (disponible en www.eff.org).

⁴³ *Vid.* art. 3 letra d) RSD.

significativo de destinatarios del servicio en uno o varios Estados miembros en relación con su población, o dirige sus actividades hacia uno o varios Estados miembros⁴⁴.

En otras palabras, cuando el establecimiento del servicio digital esté en un tercer Estado serán de aplicación sus disposiciones si tiene un promedio mensual de destinatarios del servicio activos en la Unión Europea de más de cuarenta y cinco millones⁴⁵. Se trata de un criterio cuantitativo razonable (*i.e.* una cifra equivalente al diez por ciento de la población de la Unión), ya que estas plataformas en línea de muy gran tamaño y motores de búsqueda en línea de muy gran tamaño, como se analiza en el siguiente apartado, pueden entrañar riesgos sistémicos para la sociedad. Por lado, también estarán sujetos a la normativa de la Unión aquellos servicios digitales establecidos en un tercer Estado que dirijan sus actividades hacia uno o más Estados miembros⁴⁶.

28. Desde mi punto de vista, esta disposición de aplicación también a situaciones privadas de tráfico jurídico externo -mediante una norma de alcance extraterritorial- constituye una eficaz estrategia geopolítica de la Unión para salvaguardar de manera adecuada los valores fundamentales de la Unión Europea.

Una estrategia que cobra singular relevancia en un contexto donde las relaciones privadas digitales son inherentemente transfronterizas, el principio de territorialidad se vuelve difuso debido a la naturaleza ubicua de internet, y tanto los usuarios como la sociedad en general se enfrentan a serias vulnerabilidades frente a empresas tecnológicas, muchas de las cuales están establecidas en terceros Estados con intereses económicos significativos. Por esta razón, reforzar la protección y cumplimiento de este nuevo marco jurídico digital, no solo en las relaciones *ad intra*, sino también en las relaciones *ad extra* -por su vínculo estrecho con la Unión- resulta clave para alcanzar los objetivos establecidos por nuestro legislador.

29. Con todo, estos gigantes tecnológicos podrían optar por no cumplir con las disposiciones sustantivas de obligada observancia, en cuyo caso, la cuestión radica en determinar si este marco jurídico digital de la Unión Europea contempla mecanismos que garanticen de manera efectiva el cumplimiento de sus objetivos, o si, por el contrario, adolece de la capacidad para imponer consecuencias jurídicas frente a eventuales incumplimientos, como se analiza seguidamente.

B) David c. Goliat: tutela jurídico-pública y privada del nuevo marco jurídico-digital

30. Dado el considerable poder de las multinacionales tecnológicas situadas fuera de la Unión Europea, eludir la observancia de las disposiciones del Reglamento (UE) de servicios digitales podría percibirse como una sugerente alternativa. Aunque el potencial económico del mercado de la Unión Europea, compuesto por cerca de quinientos millones de consumidores, constituye, en mi opinión, una *vis atractiva* suficiente para incentivar la adopción de este nuevo marco jurídico digital.

31. En todo caso, resulta fundamental acentuar que el Reglamento establece mecanismos tanto de tutela jurídico-pública de supervisión destinados a garantizar su cumplimiento, como de tutela jurídico-privada. En particular, se prevé la supervisión a cargo de las autoridades competentes de cada Estado miembro, así como un papel destacado de la Comisión en este ámbito. Además, se otorga a las personas físicas y jurídicas la facultad de presentar reclamaciones por la infracción de esta normativa digital⁴⁷.

⁴⁴ De acuerdo con la definición incorporada en el art. 3 letra e) RSD.

⁴⁵ Véase, al respecto, el cdo. n.º 76 RSD.

⁴⁶ Recogiendo el cdo n.º 8 RSD la consolidada jurisprudencia del Tribunal de Justicia sobre el “criterio de las actividades dirigidas”.

⁴⁷ Como señala DE MIGUEL, estos mecanismos representan cambio significativo “habida cuenta de las tradicionales carencias de la aplicación efectiva del ordenamiento jurídico a muchos de estos prestadores intermediarios, incluidos aquellos que son objeto de obligaciones más estrictas”. *Vid.* P. DE MIGUEL ASENSIO, *Derecho privado de internet*, 6.ª edición, Civitas Thomson-Reuters, 2022, p. 370.

32. Este novedoso marco normativo digital efectivamente impone a los Estados miembros la obligación de designar “una o varias autoridades competentes responsables de la supervisión de los prestadores de servicios intermediarios y de su ejecución”⁴⁸, siendo una de las autoridades competentes su coordinador de servicios digitales, que será responsable de todas las materias relacionadas con la supervisión y garantía del cumplimiento del Reglamento en ese Estado miembro⁴⁹.

A modo de ejemplo, la Comisión Nacional de los Mercados y la Competencia (CNMC) ha sido designada como Coordinador de Servicios Digitales de España.

33. En consecuencia, corresponde al Estado miembro donde se encuentre el establecimiento principal del prestador de servicios intermediarios la competencia exclusiva para supervisar y hacer cumplir el Reglamento⁵⁰. Como se observa, esta disposición se alinea con el principio del control del país de origen establecido en el artículo 3 de la Directiva sobre el comercio electrónico.

34. Asimismo, es importante señalar que la determinación del establecimiento principal del prestador de servicios intermediarios se refiere al lugar en el que tenga su sede central o domicilio social en el que ejerza las principales funciones financieras y el control de sus operaciones. En el caso de que el prestador no esté establecido en la Unión, pero que ofrezca sus servicios aquí, la competencia corresponderá al Estado miembro en el que haya designado a su representante legal⁵¹, sin perjuicio de las competencias que recaen en la Comisión⁵².

Con esta claridad se recoge en la definición de “coordinador de servicios digitales del establecimiento” contenida en el artículo 3 letra n), donde se establece que el término hace referencia al “coordinador de servicios digitales del Estado miembro en el que el establecimiento principal del prestador de un servicio intermediario esté ubicado o su representante legal resida o esté establecido”. Esta definición, nótese, también abarca la referencia a la residencia o al establecimiento del representante legal, ya que uno de los requisitos que deben cumplir todos los prestadores de servicios intermediarios es, precisamente, la designación (o nombramiento) de estos representantes legales⁵³.

⁴⁸ Vid. art. 49.1 RSD.

⁴⁹ Y este asumirá la responsabilidad en todas las cuestiones relacionadas con la supervisión y el cumplimiento de este Reglamento dentro del Estado miembro correspondiente. Además, tendrá la tarea de garantizar la coordinación a nivel nacional en estas materias y de contribuir a la supervisión y aplicación efectivas y uniformes del Reglamento en toda la Unión Europea, según el art. 49.2 RSD.

⁵⁰ De acuerdo con el art. 56.1 RSD.

⁵¹ Vid. cdo. n.º 123 RSD *in fine*.

⁵² De acuerdo con el art. 56.6 RSD: “cuando un prestador de servicios intermediarios no tenga un establecimiento en la Unión, el Estado miembro en el que su representante legal resida o esté establecido o la Comisión tendrán competencias, según proceda, de conformidad con los apartados 1 y 4 del presente artículo, para supervisar y hacer cumplir las obligaciones pertinentes en virtud del presente Reglamento”.

⁵³ De acuerdo con el art. 13 RSD:

1. Los prestadores de servicios intermediarios que *no tengan un establecimiento* en la Unión pero que ofrezcan servicios ven la Unión *designarán, por escrito, a una persona física o jurídica para actuar como su representante legal en uno de los Estados miembros en los que el prestador ofrezca sus servicios*.

2. Los prestadores de servicios intermediarios mandatarán a sus representantes legales, además o en lugar de dichos prestadores, con el fin de ser los destinatarios de las comunicaciones enviadas por las autoridades competentes de los Estados miembros, la Comisión y la Junta sobre todas las cuestiones necesarias para la recepción, el cumplimiento y la ejecución de las decisiones adoptadas en relación con el presente Reglamento. Los prestadores de servicios intermediarios otorgarán a su representante legal las facultades necesarias y recursos suficientes para garantizar su cooperación eficiente y en tiempo oportuno con las autoridades competentes de los Estados miembros, la Comisión y la Junta, y cumplir dichas decisiones.

3. *El representante legal designado podrá ser considerado responsable por el incumplimiento de las obligaciones en virtud del presente Reglamento*, sin perjuicio de la responsabilidad del prestador de servicios intermediarios y de las acciones legales que puedan iniciarse contra este.

4. Los prestadores de servicios intermediarios notificarán el nombre, el domicilio postal, la dirección de correo electrónico y el número de teléfono de su representante legal al coordinador de servicios digitales del Estado miembro en el que dicho representante legal resida o esté establecido. Velarán por que dicha información esté a disposición del público, sea fácilmente accesible, sea exacta y esté actualizada.

5. La *designación de un representante legal* en la Unión en virtud del apartado 1 *no constituirá un establecimiento en la Unión* (énfasis añadido).

35. Y no cabe desatender, por otro lado, el *superpoder* de la Comisión en este contexto digital. En efecto, la Comisión tiene competencias para supervisar y hacer cumplir las obligaciones adicionales de gestión de riesgos sistémicos para prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño⁵⁴. A este respecto, un ejemplo reciente es la solicitud por la Comisión a las plataformas YouTube, Snapchat y TikTok instándoles a ofrecer más información sobre el diseño y el funcionamiento de sus sistemas de recomendación⁵⁵.

36. Al margen de lo anterior, cobra especial importancia el reconocimiento a las personas físicas y a determinadas entidades de una legitimación (extraordinaria) para tutelar (colectivamente) sus derechos e intereses ante estas autoridades en caso de infracción por el incumplimiento de esta normativa digital.

37. En efecto, el Reglamento contiene normas diseñadas para reforzar esta tutela jurídico-pública que permiten a los usuarios digitales defender los derechos otorgados por esta normativa solicitando la intervención del coordinador de servicios digitales, además de autorizar a determinadas entidades a ejercer acciones de representación, lo que contribuye a proteger los intereses generales de los particulares⁵⁶.

A tal efecto, se otorga al destinatario del servicio, así como a los organismos, organizaciones o asociaciones autorizados a ejercer en su nombre, el derecho a presentar una reclamación contra los prestadores de servicios intermediarios por una presunta infracción del Reglamento⁵⁷. Y cabe referirse también a las acciones de representación⁵⁸, siendo un ejemplo de esta tutela colectiva la demanda presentada contra la plataforma digital Temu por la Federación de Consumidores y Usuarios (CECU) y por la Organización de Consumidores y Usuarios (OCU) ante la CNMC⁵⁹.

⁵⁴ De acuerdo con el art. 56.2 RSD. Por su parte, señala el cdo. n.º 140 RSD que “en vista de los problemas concretos que puedan surgir para asegurar el cumplimiento por parte de los prestadores de plataformas en línea de muy gran tamaño o de motores de búsqueda de muy gran tamaño y de la importancia de hacerlo de manera efectiva, tomando en consideración su dimensión e impacto y los perjuicios que pueden causar, *la Comisión debe poseer amplios poderes de investigación y ejecución que le permitan investigar, hacer cumplir y vigilar el cumplimiento de las normas establecidas en el presente Reglamento, respetando plenamente el derecho fundamental a ser oído y a tener acceso al expediente en el contexto de los procedimientos de ejecución, el principio de proporcionalidad y los derechos e intereses de los afectados*” (énfasis añadido).

⁵⁵ Según indica la nota de prensa de la Comisión de 2 de octubre de 2024, esta información deberá ser proporcionada antes del 15 de noviembre y en función de la evaluación de sus respuestas, la Comisión valorará los próximos pasos; lo que podría implicar la apertura formal de un procedimiento e imponer multas por información incorrecta, incompleta o engañosa en respuesta a las solicitudes de información. En caso de falta de respuesta, la Comisión podrá presentar una solicitud formal mediante decisión y dentro del plazo podría dar lugar a la imposición de multas coercitivas. Esta información puede verse en la página web <https://digital-strategy.ec.europa.eu/es/policies/list-designated-vlops-and-vloses> sobre una visión general de las plataformas en línea de muy gran tamaño y los motores de búsqueda en línea de muy gran tamaño objeto de supervisión por la Comisión, así como de las principales actividades de aplicación (actualizada la información al 29 de noviembre de 2024).

⁵⁶ P. DE MIGUEL ASENSIO, *Manual de Derecho de las nuevas tecnologías*, Pamplona, Aranzadi, 2023, pp. 102-103.

⁵⁷ De acuerdo con el art. 53 RSD. Esta reclamación puede presentarse ante el coordinador de servicios digitales del Estatal o miembro donde esté situado o establecido el destinatario del servicio. El coordinador evaluará la reclamación y si corresponde, la remitirá al coordinador de servicios digitales de establecimiento, acompañándola de un dictamen si lo estima apropiado. Cuando la reclamación sea responsabilidad de otra autoridad competente en su Estado miembro, el coordinador de servicios digitales que reciba la reclamación la transmitirá a dicha autoridad. Durante el procedimiento, ambas partes tendrán derecho a ser oídas y a recibir información adecuada sobre el estado del procedimiento conforme con el Derecho nacional.

⁵⁸ *Vid.* arts. 86 y art. 90 RSD.

⁵⁹ Señala la nota de prensa que: “Temu, el mercado en línea operado por la compañía comercial china PDD Holdings, que ya cuenta en Europa con más de 75 millones de usuarios mensuales, no proporciona determinada información relevante para los consumidores europeos, como, por ejemplo, la identidad del vendedor, para confirmar si el producto cumple con los requisitos de seguridad de la UE o sobre sus sistemas de recomendación, para conocer cuáles son los diferentes criterios que utiliza para proponer determinados productos. Además, la citada plataforma está plagada de técnicas de manipulación (patrones oscuros) para lograr que los consumidores gasten más de lo que originalmente querrían o para complicar el proceso de cerrar su cuenta. Por todo ello, OCU y CECU consideran que Temu estaría infringiendo la nueva Ley de Servicios Digitales, y a tal efecto, han puesto las citadas prácticas en conocimiento de la CNMC, como Coordinador Nacional de Servicios Digitales, para que proceda a su investigación y en su caso, imponga la correspondiente sanción” (disponible en: <https://www.ocu.org/organizacion/prensa/notas-de-prensa/2024/denunciatemu160524>).

38. Y en relación con las consecuencias jurídicas que podrían surgir ante un posible incumplimiento de las disposiciones obligatorias establecidas en este nuevo marco jurídico digital, no considero que puedan ser interpretadas como insignificantes (o caer en *papel mojado*). Por el contrario, la estricta naturaleza de las sanciones previstas en caso de incumplimiento debería representar un estímulo o incentivo significativo para su cumplimiento, incluso para los gigantes tecnológicos estadounidenses y asiáticos, cuyas valoraciones bursátiles superan el billón de dólares.

39. Así es, esta norma sustantiva digital establece un severo régimen de sanciones en caso de incumplimiento⁶⁰. El considerando n.º 144 lo expresa de manera inequívoca: “el cumplimiento de las obligaciones pertinentes impuestas en virtud del presente Reglamento debe garantizarse mediante multas sancionadoras y multas coercitivas”.

A este respecto, son los Estados miembros los encargados de fijar estas sanciones al intermediario que esté bajo su competencia y deberán ser “efectivas, proporcionadas y disuasorias”⁶¹. No obstante, el legislador de la Unión ha fijado que el importe máximo de las multas sea el 6 % del volumen de negocios anual en todo el mundo del prestador del servicio que se trate en el ejercicio fiscal anterior. Asimismo para infracciones como, por ejemplo, proporcionar información incorrecta, incompleta o engañosa, por no responder o por no rectificar información incorrecta, incompleta o engañosa y por no someterse a una inspección las sanciones se fijan en el 1 % de los ingresos anuales, o del volumen de negocios anual en todo el mundo; y se prevé que el importe máximo de una multa coercitiva sea del 5 % del promedio diario del volumen de negocios en todo el mundo o de los ingresos del prestador de servicios intermediarios de que se trate en el ejercicio fiscal anterior por día, calculado a partir de la fecha especificada en la decisión de que se trate⁶².

40. Debe tenerse en cuenta que la Comisión Europea puede imponer también multas de hasta un máximo de dichos importes y, en todo caso, para fijar el importe de la multa se tendrá en cuenta “la naturaleza, gravedad, duración y recurrencia de la infracción y la demora causada al procedimiento”⁶³. Igualmente puede adoptar una decisión por la que se impongan una multa coercitiva al prestador de la plataforma en línea de muy gran tamaño o del motor de búsqueda en línea de muy gran tamaño que no excedan del 5 % del promedio diario de los ingresos o del volumen de negocios anuales en todo el mundo del ejercicio fiscal anterior por día, calculados a partir de la fecha fijada por esa decisión⁶⁴. En cualquier caso, el Tribunal de Justicia de la Unión Europea tiene competencia jurisdiccional plena para someter a control las decisiones por las que la Comisión haya impuesto multas sancionadoras o multas coercitivas; pudiendo anular, reducir o aumentar la multa sancionadora o la multa coercitiva impuesta⁶⁵. Y en aquellos casos en que el incumplimiento sea reiterado, podrá dar lugar, a través del coordinador de servicios digitales de establecimiento del prestador que solicite a la autoridad judicial competente de su Estado la orden de que se limite temporalmente el acceso de los destinatarios al servicio afectado por la infracción o bien, únicamente cuando ello no sea técnicamente viable, a la interfaz en línea del prestador de servicios intermediarios en la que tenga lugar la infracción⁶⁶.

41. Junto a estos mecanismos jurídico-públicos, cabe referirse también a la aplicación privada de este marco jurídico digital, es decir: la tutela judicial civil con respecto a los daños y perjuicios causados por una infracción de este texto digital.

Se trata, en puridad, de un sistema de garantías de su efectividad en el que la iniciativa privada complementa la referida aplicación pública. La eventual indemnización por el daño causado a cargo de

⁶⁰ Véase el capítulo IV dedicado a la “aplicación, cooperación, sanciones y ejecución” y en particular el artículo 52 “sanciones” y el artículo 74 “multas” RSD respectivamente.

⁶¹ De acuerdo con el art. 52.1 RSD.

⁶² Art. 52 *in fine* RSD.

⁶³ *Vid.* art. 74 *in fine* RSD.

⁶⁴ Art. 76 RSD.

⁶⁵ Art. 81 RSD.

⁶⁶ De acuerdo con el art. 82 en relación con el art. 51, apartado 3 RSD.

estos intermediarios por el incumplimiento de las disposiciones del Reglamento contribuye, también, a su efectividad.

42. En relación con la aplicación privada, tiene especial relevancia el artículo 54 del Reglamento (UE) de servicios digitales en la medida en que “los destinatarios del servicio tendrán derecho a solicitar, de conformidad con el Derecho de la Unión o nacional, una indemnización con cargo a los prestadores de servicios intermediarios por cualquier daño o perjuicio sufrido como consecuencia del incumplimiento por parte de dichos prestadores de sus obligaciones en virtud del presente Reglamento”.

De su lectura se desprende que no solo impone obligaciones a los intermediarios, sino que también otorga derechos subjetivos a los particulares, cuyas infracciones podrán dar lugar a una indemnización⁶⁷.

43. Así, la legitimación activa corresponde a los destinatarios del servicio que, a tenor de la definición incorporada en la letra b) del artículo 3, se refiere a “toda persona física o jurídica que utilice un servicio intermediario, en particular para buscar información o para hacerla accesible”.

Esta definición debe interpretarse de manera amplia, incluyendo al suscriptor de un servicio o a quien lo difunda, como a quién utilice una plataforma o un buscador -porque se expone a la información mostrada en el interfaz-⁶⁸. De Miguel Asensio sugiere, con buen criterio, que se podría adoptar “una interpretación incluso más amplia en el contexto del artículo 54. En particular, afectadas por la difusión de contenidos ilícitos y perjudicadas por la infracción del Reglamento (UE) de servicios digitales puede ser, por ejemplo, cualquier persona cuyo derecho al respeto de la vida privada y familiar se ve menoscabado por prácticas de los prestadores de servicios intermediarios que infringen lo dispuesto en el Reglamento (UE) de servicios digitales. Una interpretación amplia resulta avalada por el contenido de otras disposiciones del Reglamento, como su artículo 20 que refleja el criterio de que cualquier persona física o entidad que notifica al prestador de servicios de alojamiento la presencia de contenidos que considere ilícitos en el marco del artículo 16 debe ser considerado un destinatario del servicio⁶⁹”. Por último, cabe recordar que es posible interponer acciones colectivas y que el destinatario del servicio puede mandar “a un organismo, organización o asociación para que ejerza los derechos atribuidos por el presente Reglamento en su nombre”⁷⁰.

44. Con respecto al tribunal internacionalmente competente para conocer de la acción de reclamación por los daños y perjuicios causados por una supuesta infracción del Reglamento (UE) de servicios digitales por parte del intermediario de las obligaciones establecidas en esta normativa, es importante señalar que este texto no contiene normas especiales relativas al Derecho internacional privado, a diferencia de lo que ocurre con el Reglamento General de Protección de Datos⁷¹, y quizá hubiera sido oportuno incorporar alguna disposición similar en su articulado que evitara que, en la mayoría de los casos, las demandas deban interponerse en Irlanda, dado que es allí donde se encuentran las sedes de los principales gigantes tecnológicos en la Unión Europea.

⁶⁷ En este sentido cabe referirse al cdo. n.º 121 RSD: “[...] un prestador de servicios intermediarios debe ser responsable por los perjuicios sufridos por destinatarios del servicio causados por un incumplimiento de las obligaciones establecidas en el presente Reglamento por dicho prestador. Dicha compensación debe ajustarse a las normas y procedimientos establecidos en el Derecho nacional aplicable y sin perjuicio de otras vías de recurso disponibles en virtud de las normas de protección de los consumidores”.

⁶⁸ Véanse las definiciones de “destinatario activo de una plataforma en línea” (art. 3 letra p) y “destinatario activo de un motor de búsqueda en línea” (art. 3 letra q) respectivamente.

⁶⁹ P. DE MIGUEL ASENSIO. Entrada del blog 1 de diciembre de 2022 titulada “Reglamento de Servicios Digitales (VII): supervisión y aplicación” (pedrodemiguelasensio.blogspot.com).

⁷⁰ De acuerdo con lo dispuesto en el art. 86 RSD.

⁷¹ Sobre los fueros especiales del RPGD, véase, P. DE MIGUEL ASENSIO, “Derecho a indemnización en materia de datos personales: aspectos internacionales”, *Cuadernos de Derecho Transnacional*, vol. 16, n.º 2, 2024, pp. 487-500, en particular, pp. 492-496.

Por lo tanto, será necesario recurrir a las normas de Derecho internacional privado⁷² para determinar el tribunal internacionalmente competente que conocerá de las acciones de reclamación por los daños y perjuicios causados por una supuesta infracción del Reglamento (UE) de servicios digitales por parte del intermediario de las obligaciones establecidas en esta normativa. En síntesis, el Reglamento Bruselas I bis.

45. Al hilo de lo anterior, cabe referirse, por último, a las primeras resoluciones judiciales en el marco de la aplicación privada del Reglamento (UE) de servicios digitales.

En lo que concierne a las acciones colectivas, el pasado 12 de septiembre el Tribunal Regional Superior de Fráncfort dictó la primera condena por infracción del Reglamento (UE) de servicios digitales. La demanda fue interpuesta por una asociación de consumidores alemana, que lucha contra las prácticas comerciales desleales, contra la plataforma digital Temu, un mercado en línea con más de 75 millones de usuarios mensuales. Esta plataforma ofrece grandes descuentos en sus productos a los consumidores de diferentes países y envía los productos directamente desde China, siendo demandada por incumplir el artículo 30 del Reglamento (UE) de servicios digitales⁷³. Concretamente por no garantizar una adecuada trazabilidad de los comerciantes que operan en su plataforma, por emplear prácticas manipuladoras y por la falta de transparencia en los sistemas de recomendación de los productos.

Y por lo que respecta a una acción a título individual, el pasado 5 de julio de 2024 se dictó la primera resolución. El Tribunal de Distrito de Ámsterdam condenó a la plataforma X por infracción de las obligaciones impuestas en el Reglamento (UE) de servicios digitales, en concreto la demanda analizó la infracción de los artículos 12 y 17 al no designar un único punto de contacto para los destinatarios de sus servicios y ocultar silenciosamente la cuenta de un usuario de las sugerencias de búsqueda (técnica conocida como *shadow banning*) respectivamente⁷⁴.

2. Disposiciones de obligada observancia con respecto a la moderación de contenidos en el Reglamento (UE) de servicios digitales

46. La práctica de moderar la difusión de contenidos nocivos e ilegales por las plataformas en línea y buscadores es habitual desde hace más de una década. Si bien es cierto que ni la Directiva sobre el comercio electrónico ni el Reglamento (UE) de servicios digitales imponen explícitamente esta obligación⁷⁵, resulta relevante subrayar que otras legislaciones sectoriales recientes adoptadas en el ámbito de la Unión Europea sí establecen este requerimiento⁷⁶.

47. El artículo 7 del Reglamento (UE) de servicios digitales fomenta la seguridad jurídica de los intermediarios que voluntariamente implementen mecanismos para detectar, identificar y retirar contenidos ilícitos, o inhabilitar el acceso a los mismos de sus servicios, en la medida en que no perderán su inmunidad si estas investigaciones voluntarias se llevan a cabo de buena fe y con diligencia⁷⁷. Sin

⁷² Es importante tener en cuenta, al respecto, el cdo. n.º 10 RSD que establece que: “el presente Reglamento también ha de entenderse sin perjuicio de las normas de la Unión en el ámbito del Derecho internacional privado, en particular las relativas a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil, como el Reglamento (UE) n.º 1215/2012, y a la ley aplicable a las obligaciones contractuales y extracontractuales” y el cdo. n.º 126 RSD que “las normas del presente Reglamento sobre el reparto de competencias deben entenderse sin perjuicio de las disposiciones del Derecho de la Unión y de las normas nacionales de Derecho internacional privado relativas a la competencia judicial y a la ley aplicable en materia civil y mercantil, como las acciones emprendidas por consumidores ante los órganos jurisdiccionales del Estado miembro en el que estén domiciliados de conformidad con las disposiciones pertinentes del Derecho de la Unión”.

⁷³ Según puede leerse en la noticia publicada en la página <https://www.wettbewerbszentrale.de/dsa-verfahren-temu-verpflichtet-sich-zur-unterlassung/>

⁷⁴ ECLI:NL:RBAMS:2024:3980 - Rechtbank Amsterdam, 05-07-2024/10767307 CV FORM 23-13934.

⁷⁵ Hubiera sido contrario al art. 15 DCE, actualmente art. 8 RSD sobre la obligación general de monitorización o de búsqueda activa de hechos en la red.

⁷⁶ Como el controvertido art. 17 de la Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE. DO L 130 de 17.5.2019, p. 92/125.

⁷⁷ El art. 7 RSD recoge, en similares términos, la protección del buen samaritano de la sección 230 de la *Communications*

embargo, al implementar estas herramientas algorítmicas para la moderación proactiva de contenidos, es fundamental garantizar que “la tecnología de que se trate tenga la fiabilidad suficiente para limitar en la mayor medida posible el porcentaje de errores”⁷⁸.

Explícitamente está reconociéndose la existencia de un margen de error en los algoritmos. Y aunque resulte positivo que se incorpore la consideración de una tasa de error en los modelos algorítmicos, conforme apunta alguna voz, su implementación debería ser más ambiciosa y superar esta recomendación relativamente imprecisa⁷⁹.

48. En mi opinión, este impulso legal en la salvaguarda de quienes implementen estas herramientas de moderación de contenido en aras de una sociedad digital más segura, predecible y digna de confianza es muy conveniente para reforzar su seguridad jurídica.

49. En cuanto a las disposiciones de obligada observancia con respecto a la moderación de contenidos en línea, conforme se ha avanzado, están esencialmente relacionadas con el deber de transparencia, información y rendición de cuentas.

En este sentido, la falta de transparencia de las plataformas en línea en relación con algunas de sus prácticas representa una inquietud del legislador de la Unión, ya que estos actores privados regulan el acceso y el servicio de millones de usuarios de la red a través de las condiciones generales (y/o las directrices) del servicio, ampliamente aceptadas sin margen para la negociación y con cierto grado de opacidad, de ahí su interés por comprender y supervisar las acciones que realizan estos actores digitales, fundamentales en la actividad económica, social o cultural de la Unión, para evitar cualquier resultado injusto o arbitrario asociado a su poder⁸⁰.

50. Es cierto que la mayor parte de estos titanes tecnológicos publican desde hace tiempo sus directrices o políticas internas, pero la crítica en buena medida reside en la falta de precisión, de ahí que esta nueva normativa tenga por objeto reforzar la exigencia de claridad de las políticas internas de los servicios digitales y también su fácil accesibilidad.

51. Por este motivo, el legislador de la Unión centra la atención en las condiciones generales⁸¹ de los servicios digitales, haciendo hincapié en que se redacten en un “lenguaje claro, sencillo, inteligible, accesible al usuario e inequívoco, y se hará pública en un formato fácilmente accesible y legible por máquina” la información relacionada con cualquier restricción que se imponga en relación con el uso del servicio de la información facilitada por el destinatario. Esta información, se enfatiza en particular, incluirá “datos sobre cualesquiera políticas, procedimientos, medidas y herramientas empleadas para moderar los contenidos, incluidas la toma de decisiones mediante algoritmos”⁸².

Decency Act estadounidense. Un análisis de esta disposición y su jurisprudencia, véase, J.J. CASTELLÓ PASTOR, “Exoneración de responsabilidad de los prestadores de servicios de la información en la sección 230 de la *Communications Decency Act* estadounidense”, *Revista Aranzadi de derecho y nuevas tecnologías*, 2015, n.º 39, pp. 175-194.

⁷⁸ Así lo puntualiza el cdo. n.º 26 RSD.

⁷⁹ Conforme señala F. G’SELL, “The Digital Services Act: A General Assessment” en A. UNGERN-STERNBERG (ed.), *Content Regulation in the European Union. The Digital Services Act*, vol. 1, Verein für Recht und Digitalisierung e.V, Trier, 2023, p. 92.

⁸⁰ Es importante puntualizar que la libertad contractual de estos actores digitales para fijar las condiciones generales de sus servicios se ve limitada en la medida que, según el cdo. n.º 45 RSD, “es oportuno establecer determinadas normas sobre el contenido, la aplicación y la ejecución de las condiciones generales de dichos prestadores por motivos de transparencia y protección de los destinatarios del servicio y para evitar resultados injustos o arbitrarios”.

⁸¹ Definidas como “todas las cláusulas, sea cual sea su nombre y forma, que rijan la relación contractual entre el prestador de servicios intermediarios y los destinatarios del servicio” en el art. 3 letra u) RSD. Como se ha subrayado, la relación contractual entre el servicio digital y el destinatario del servicio queda incorporada en las condiciones generales usualmente determinadas de forma unilateral por el servicio intermediario y aceptadas por el usuario con un simple clic (esto es: el consentimiento dado por los usuarios de la mayoría de las aplicaciones, redes sociales y demás sitios web suele darse generalmente por medio del *click-wrap agreement* y del *browse-wrap agreement*) sin una lectura previa, razón por la que resulta ciertamente deseable una mayor claridad de la caja negra de los intermediarios. Sobre este aspecto, con mayor profundidad, véase J.J. CASTELLÓ PASTOR, “Interrelación del Reglamento”, cit. (versión digital).

⁸² Art. 14.1 RSD.

52. Junto a estas obligaciones aplicables a todos los prestadores de servicios intermediarios, se configuran dos obligaciones más en materia de información y transparencia de las condiciones generales por el particular papel y alcance⁸³ de los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño: facilitar “un resumen sucinto, fácilmente accesible y legible por máquina de las condiciones generales, incluidas las medidas correctivas y los mecanismos de recurso disponibles, en un lenguaje claro e inequívoco⁸⁴” y “publicar sus condiciones generales en todas las lenguas oficiales de todos los Estados miembros en los que presten sus servicios”⁸⁵.

53. Asimismo, el prestador del servicio de alojamiento de datos que aplique alguna restricción sobre la visibilidad del contenido (o información), la suspensión del servicio o de la cuenta del destinatario del servicio, tiene la obligación de informarle de forma clara y específica los motivos y las medidas aplicadas⁸⁶. En relación con la información requerida en la declaración de motivos, es relevante especificar si esta decisión ha sido adoptada sobre la base de investigaciones por propia iniciativa de carácter voluntario, así como información sobre el uso de medios automatizados para adoptar la decisión, incluida si la decisión se ha adoptado respecto de contenidos detectados o identificados utilizando medios automatizados⁸⁷.

54. En mi opinión, este principio de transparencia contribuye la mejora de la confianza de los usuarios en el ecosistema digital y conduce a la buena gobernanza digital, de modo que esta información incluida en las condiciones generales de los servicios digitales aporta seguridad jurídica y previsibilidad. Y toda acción frente a ellos debe estar rigurosamente fundamentada en este, *mutatis mutandis*, principio de legalidad.

55. Unido a lo anterior, uno de los aspectos más relevantes posiblemente sea la obligación de transparencia informativa de todos los intermediarios, de acuerdo con el artículo 15 del Reglamento (UE) de servicios digitales, materializada en publicar anualmente informes legibles por máquina y de fácil acceso en el que se detalle cualquier actividad de moderación de contenidos durante ese periodo de tiempo.

Estos informes deberán incluir, en particular, información clara y fácilmente entendible sobre la moderación proactiva de contenidos, debiendo explicar cómo utilizan las referidas herramientas automatizadas, además de dar cuenta detallada sobre el uso de estos medios automatizados (incluida “la posible tasa de error de los medios automatizados para cumplir dichos fines”)⁸⁸.

⁸³ Cdo. n.º 48 RSD.

⁸⁴ De acuerdo con el apdo. 5 del art. 14 RSD y añade el cdo. n.º 48 que “[...] en dichos resúmenes se deben indicar los principales elementos de las obligaciones de información, incluida la posibilidad de excluir fácilmente las cláusulas opcionales”.

⁸⁵ *Vid.* art. 14.6 RSD.

⁸⁶ La decisión del prestador del servicio de retirar o bloquear el acceso a la información publicada en la red por un usuario, la de suspender, cesar o suprimir la prestación del servicio o la cuenta del usuario por infringir las directrices o políticas internas de la plataforma sin ofrecer mayor argumento e información al respecto son prácticas frecuentes en estos últimos años. Frente a estas situaciones, el legislador de la Unión diseña estas disposiciones basadas en la transparencia y en la protección de los derechos fundamentales de los usuarios en la red precisamente para evitar, en lo posible, un trato injusto o arbitrario con respecto a la decisión que tome la plataforma en línea y disponer el usuario, en su caso, de garantías procedimentales contra la misma. Amén de la referida información preceptiva en las condiciones generales, se configuran derechos procesales al usuario como el derecho a recibir información sobre la restricción mediante la motivación de su decisión (i.e. declaración de motivos que la justifique) junto con información sobre las posibles vías para recurrirla. Sobre una detallada valoración de los derechos procesales y garantías procedimentales de los usuarios del servicio, véase: P. LLOPIS NADAL, “Plataformas en línea y decisiones sobre contenidos: el sistema interno de reclamación y la resolución extrajudicial de litigios como vías de impugnación reguladas en la Ley de Servicios Digitales”, en E. HERNÁNDEZ SÁINZ, L. C. MATE SATUÉ, y M. T. ALONSO, *La responsabilidad civil por servicios de intermediación prestados por plataformas digitales* (ed.) Colex, 2023, pp. 150-169; G. PALAO MORENO, “Las órdenes de actuación contra contenidos ilícitos en el nuevo reglamento europeo de servicios digitales”, en J.J. CASTELLÓ PASTOR (Dir.), *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea* Aranzadi, 2024 (versión digital); R. PLÁ ALMENDROS, “Los ADR en el reglamento de servicios digitales”, en S. BARONA VILAR (ed.), *Masc, to be or not to be?: (medios adecuados de solución de conflictos en la justicia)*, Tirant lo Blanch, Valencia, 2024, pp. 571-598.

⁸⁷ *Vid.* apdo. primero y tercero letras c) del art. 17 RSD.

⁸⁸ Esto es, aquellas medidas que adopten para proporcionar formación y asistencia a quienes se encarguen de la moderación de contenidos y las restricciones del servicio, entre otras. Véanse conjuntamente los apdos. c) y e) del art.15.1 RSD.

56. Unas obligaciones de transparencia informativa y rendición de cuentas que se ven incrementadas a las plataformas en línea de muy gran tamaño y a los motores de búsqueda de muy gran tamaño⁸⁹. En tal sentido, deben publicar informes de transparencia dos veces al año en el que se indique información pertinente sobre los recursos de moderación de contenidos y cualificación de sus moderadores, además de facilitar al regulador el acceso a todos estos datos para comprobar el cumplimiento de las disposiciones del Reglamento⁹⁰. Sin duda alguna, toda esta información contribuye al enriquecimiento y actualización de la base de datos (*DSA Transparency Database*).

3. Comportamiento responsable y diligente frente al riesgo sistémico, pero ¿quién?

57. El Reglamento (UE) de servicios digitales establece una política innovadora al atribuir a los intermediarios la responsabilidad de salvaguardar un entorno en línea seguro, predecible y confiable, instándoles a adoptar un comportamiento responsable y diligente⁹¹.

A tal efecto, el legislador de la Unión considera oportuno establecer adicionalmente un estándar más alto a las plataformas en línea de muy gran tamaño y a los motores de búsqueda de muy gran tamaño (sección 5ª, artículos 33 a 43), ya que el número de usuarios que utilizan estos servicios pueden plantear especiales riesgos.

58. Se trata ciertamente de un enfoque basado en el riesgo: estos gigantes tecnológicos pueden ejercer una fuerte influencia social -incluso desproporcionada- en la Unión Europea, motivo por el cual resulta necesario someterlos a un exigente régimen de evaluaciones y toma de medidas para mitigar cualesquiera de los riesgos sistémicos⁹².

59. Con este fin, se establece un sistema de gestión de riesgos que consta dos obligaciones: de un lado, se les encomienda a analizar y evaluar de forma diligente cualquier riesgo sistémico en la Unión Europea derivado del diseño o del funcionamiento de sus servicios y los sistemas utilizados con estos, incluidos los sistemas algorítmicos, o del uso que se haga de sus servicios⁹³. De otro lado, a implementar una serie de medidas con el fin de disminuir estos riesgos sistémicos⁹⁴.

⁸⁹ Art. 42 RSD.

⁹⁰ Tal y como indica el art. 40.1 RSD. Amén del regulador, el acceso de estos datos puede extenderse a investigadores autorizados. Sobre este aspecto, véase A. GASCÓN MARCÉN, “Acceso de los investigadores a los datos de las plataformas según la DSA”, en J.J. CASTELLÓ PASTOR (dir.), *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024 (versión digital).

⁹¹ Cdo. n.º 76 RSD.

⁹² Conforme a los cdos. n.º 80 a 83 RSD, los riesgos sistémicos se refieren a los riesgos asociados a la difusión de contenidos ilícitos; a los efectos reales o previsibles del servicio para el ejercicio de los derechos fundamentales; también aquellos se refiere a los efectos negativos reales o previsibles sobre los procesos democráticos, el discurso cívico y los procesos electorales, así como sobre la seguridad pública y las relacionadas con el diseño, el funcionamiento o la utilización, también mediante la manipulación, de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño, con un efecto negativo real o previsible en la protección de la salud pública, los menores y graves consecuencias negativas para el bienestar físico y mental de una persona, o en la violencia de género.

⁹³ A tenor del art. 34 RSD. En síntesis, esta evaluación se realizará, al menos, una vez al año y “será específica de sus servicios y proporcionada a los riesgos sistémicos, teniendo en cuenta su gravedad y probabilidad, e incluirá los siguientes riesgos sistémicos: a) la difusión de contenido ilícito a través de sus servicios; b) cualquier efecto negativo real o previsible para el ejercicio de los derechos fundamentales [...]; c) cualquier efecto negativo real o previsible sobre el discurso cívico y los procesos electorales, así como sobre la seguridad pública; d) cualquier efecto negativo real o previsible en relación con la violencia de género, la protección de la salud pública y los menores y las consecuencias negativas graves para el bienestar físico y mental de la persona”. Señala F. G’SSELL, “The Digital Services Act”, cit., p. 114 que “la definición de riesgos sistémicos del apartado 1 del artículo 34 es particularmente amplia y vaga. Por ejemplo, cualquier cosa que pueda menoscabar los derechos fundamentales podría considerarse un riesgo sistémico, lo que implica que cualquier tipo de contenido podría vincularse a dicho riesgo. Esto crea una gran incertidumbre sobre lo que las plataformas, los investigadores y los reguladores podrían clasificar como riesgos sistémicos. Una interpretación global de los “riesgos sistémicos” podría dar lugar a la aparición de una categoría “gris” de contenidos que no son explícitamente ilegales pero que se consideran indeseables por su potencial para crear riesgos sistémicos. Además, la creación de esta categoría “gris”, a medio camino entre lo ilegal y lo legal, representa una amenaza real para la libertad de expresión”.

⁹⁴ Según el art. 35 RSD. Estas medidas de detección deben ser razonables, proporcionadas y efectivas, teniendo especialmente en cuenta las consecuencias de dichas medidas sobre los derechos en liza.

60. Y por lo que interesa al objeto de este estudio, los gigantes tecnológicos deben evaluar los riesgos asociados con sus métodos de moderación de contenidos, incluido los aspectos con la ampliación de contenidos y el diseño de sus algoritmos de recomendación. Es esencial que realicen un análisis de cómo estas prácticas impactan en el discurso cívico, los procesos electorales, la salud pública y la seguridad.

61. Sin embargo, estos sistemas de gestión de riesgos sistémicos plantean objeciones tanto por el amplio margen de discrecionalidad que el Reglamento otorga a estos actores digitales como por el poder de control que concentra la Comisión Europea⁹⁵.

62. Con respecto a la falta de concreción del término contenido ilícito⁹⁶, constituye una cuestión controvertida para abordar los riesgos sistémicos porque, como se ha referido⁹⁷, se permite cierto grado de flexibilidad a estos actores digitales para establecer en las condiciones generales las conductas para evaluar el posible riesgo de su difusión.

Y tampoco se ve beneficiada esta función de la evaluación del riesgo por el hecho de que estos operadores tecnológicos deban dirigir su atención también a “*la información que no sea ilícita, pero que contribuya a los riesgos sistémicos identificados en el presente Reglamento*” incluyendo en este punto aquellos “*contenidos incorrectos o engañosos, incluida la desinformación*”⁹⁸, esto es: contenidos nocivos o con efectos negativos.

63. Es innegable que los servicios digitales desempeñan un papel esencial en la difusión de información y están en una posición privilegiada para abordar los riesgos sistémicos.

Ahora bien, a mi parecer, es ciertamente preocupante que la determinación de lo que constituye el carácter nocivo de un contenido recaiga exclusivamente en estas empresas privadas -o más específicamente, en sus algoritmos-, ya que puede incentivar o motivar la eliminación de estos contenidos (¿promover la censura?) con el fin de reducir los riesgos, legitimadas por la propia normativa⁹⁹.

64. Con este margen de discrecionalidad para determinar el contenido que puede estar en la red – sea lícito, pero se entienda que contribuye al riesgo–, se permite a estos sujetos privados seguir disponiendo del control del discurso en el ecosistema digital, respaldado en este caso por las autoridades públicas; aun cuando reiteradamente se haga hincapié en el Reglamento en la obligación de proceder de manera no arbitraria y no discriminatoria, así como en la necesidad de tener en cuenta los derechos e intereses legítimos de los destinatarios del servicio, incluidos los derechos fundamentales amparados por la Carta¹⁰⁰.

65. Y con respecto al poder de control que concentra la Comisión Europea, de acuerdo con el artículo 56 del Reglamento (UE) de servicios digitales, se materializa en supervisar y hacer cumplir estas disposiciones dirigidas a las plataformas en línea de muy gran tamaño y a los motores de búsqueda de muy gran tamaño.

⁹⁵ Ampliamente tratado por I. REIG FABADO, “Las VLOPS y los riesgos sistémicos en la DSA: algunos aspectos problemáticos”, en J.J. CASTELLÓ PASTOR (dir.), *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*, Aranzadi, 2024 (versión digital).

⁹⁶ Definido “contenido ilícito” en la letra h) del artículo 3 del RSD como “toda información que, por sí sola o en relación con una actividad, incluida la venta de productos o la prestación de servicios, incumpla el Derecho de la Unión o el Derecho de cualquier Estado miembro que cumpla el Derecho de la Unión, sea cual sea el objeto o carácter concreto de ese Derecho”. Aunque ciertamente puede hablarse de un contenido ilícito armonizado, como el contenido terrorista, la incitación ilegal al odio (racismo y xenofobia) en línea, etc. Véase la Recomendación (UE) 2023/2425 de la Comisión, de 20 de octubre de 2023, sobre la coordinación de las respuestas a incidentes, en particular, derivados de la difusión de contenidos ilegales, antes de la plena entrada en aplicación del Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo (Ley de Servicios Digitales) (notificado en virtud del documento C (2023) 7170). DO L, 2023/2425, 26.10.2023 y la normativa indicada (en especial, en el párrafo 11 y 13).

⁹⁷ Ya que, recuérdese, es una cuestión que depende del derecho material aplicable al fondo de la controversia y una forma de sortear este aspecto es fijando en las políticas o directrices del servicio digital los comportamientos pueden realizarse (con independencia del carácter lícito o ilícito), *vid supra* párrafo 17.

⁹⁸ Cdo. n.º 84 RSD.

⁹⁹ J. BARATA MIR, “Libertad de expresión y moderación privada de contenidos”, *Teorder*, 2022, n.º 32, pp. 99 y 100.

¹⁰⁰ Cdos. n.º 47 y 79 RSD.

66. En el ámbito de los sistemas algorítmicos, en particular, este poder de la Comisión se manifiesta en la facultad para realizar las inspecciones necesarias en las instalaciones del operador tecnológico, pudiendo exigir acceso a aspectos relacionados con la organización, el funcionamiento, el sistema informático y los algoritmos, así como solicitar explicaciones y formular preguntas al personal clave del gigante digital¹⁰¹.

67. A mi modo de ver, la Comisión dispone de *carta blanca* a partir de ahora para analizar estos algoritmos¹⁰². En cualquier caso, todas estas funciones de ejecución y supervisión de la Comisión se verán facilitadas indudablemente por la tarea que desempeña el Centro Europeo para la Transparencia Algorítmica.

68. Por último, cabe referirse a una cuestión igualmente compleja: la facultad de la Comisión de emitir directrices y recomendaciones específicas sobre riesgos sistémicos concretos¹⁰³.

Si bien esta medida, que viene realizándose en estos últimos años, representa un avance positivo, la preocupación de esta estrategia aplicada para mitigar determinados riesgos viene porque pueda percibirse como una imposición de normas de comportamiento vinculantes a las plataformas en línea de muy gran tamaño y a los motores de búsqueda de muy gran tamaño.

Con estas acciones, la Comisión podría, de manera indirecta, ejercer un control sobre comportamiento de los usuarios en la red del que carece. De ahí mi interrogante de quién debería exhibir un comportamiento responsable y diligente en este contexto digital: si los referidos actores (privados) tecnológicos o las autoridades (públicas) europeas.

IV. Reflexión final

69. El Reglamento (UE) de servicios digitales es un importante eslabón en la regulación de la moderación de contenidos en internet. Con medidas asimétricas de obligada observancia a los intermediarios -construidas esencialmente sobre la base del principio de la transparencia, información y rendición de cuentas- suponen un acierto para promover entornos digitales más seguros y respetuosos, al mismo tiempo que refuerzan la confianza de los usuarios en el ecosistema digital.

70. Era necesario establecer, en mi opinión, un mayor control democrático sobre las actividades realizadas por estas multinacionales tecnológicas para contrarrestar la creciente privatización y automatización del control del discurso en línea y situar, así, al usuario en el centro de la transición digital.

71. El empleo de la inteligencia artificial en la innovadora política establecida en el Reglamento (UE) de servicios digitales, que atribuye a las plataformas en línea de muy gran tamaño y los motores de búsqueda de muy gran tamaño la responsabilidad de salvaguardar un entorno en línea seguro, predecible y confiable, instándoles a adoptar un comportamiento responsable y diligente, desempeña un papel fundamental para detectar, restringir y eliminar con rapidez aquellos contenidos que pudieran ser ilícitos, nocivos o dañinos.

72. Es necesario, no obstante, abordar con reserva estos sistemas algorítmicos en la moderación de contenidos, ya que, como expresamente lo reconoce el legislador de la Unión, pueden cometer erro-

¹⁰¹ Art. 69 *in fine* RSD. Así como puede ordenarles que proporcionen acceso a sus bases de datos y algoritmos, y explicaciones al respecto como acción necesaria para la vigilancia, de acuerdo con el art. 72 RSD.

¹⁰² Tal y como hiciera previamente en el caso Google Shopping (AT.39740 de 27 de junio de 2017), donde examinó el algoritmo del buscador y constató su manipulación para beneficiar a Google Shopping en perjuicio de otros sitios de comparación.

¹⁰³ Como las Directrices para plataformas en línea de muy gran tamaño y a los motores de búsqueda de muy gran tamaño sobre la mitigación de los riesgos sistémicos para los procesos electorales publicadas el 26 de marzo de 2024 y con orientaciones para las elecciones al Parlamento Europeo del pasado mes de junio o la Recomendación (UE) 2024/915 de la Comisión de 19 de marzo de 2024 sobre medidas destinadas a luchar contra la falsificación y a reforzar la observancia de los derechos de propiedad intelectual e industrial.

res y carecen de suficiente transparencia, de modo que puede acarrear un efecto negativo en los derechos y libertades constitucionalmente protegidos de los usuarios en la red (y de la sociedad en su conjunto).

Y tampoco debe pasarse por alto la importancia de que sea un algoritmo, desarrollado por empresas privadas con fuertes objetivos económicos, que estructuran sus políticas para atraer una mayor audiencia y mantener la atención de sus usuarios, el encargado de la visibilidad de los contenidos e información en la red.

73. Mas allá del notable esfuerzo que representa este *new deal* tecnológico, es importante reflexionar sobre cómo estas tecnológicas abordan los riesgos sistémicos, porque no solo se enfrentan al desafío de disminuir la presencia de contenido ilícito en la red, sino también de restringir aquellos contenidos que puedan ser nocivos (o con efectos negativos), cuando la naturaleza de esta calificación recae ciertamente en estos actores privados. Y la experiencia evidencia el fomento de la censura para mantener su exención de responsabilidad.

74. Por ello, alcanzar un equilibrio entre la protección de los derechos y libertades de los usuarios y de la sociedad en su conjunto, los objetivos económicos de estas multinacionales tecnológicas y la reducción de contenido ilícito, dañino o nocivo en la red parece ser un objetivo difícil de alcanzar.