EDITORIAL

LA UE Y EL ESPACIO DIGITAL: ENTRE EL INTERNACIONALISMO LIBERAL Y LA SOBERANÍA TECNOLÓGICA

The EU and the digital space: between liberal internationalism and technological sovereignty

ANTONIO SEGURA SERRANO[1]
asegura@ugr.es

Cómo citar/Citation
Segura Serrano, Antonio (2026).
La UE y el espacio digital: entre el internacionalismo liberal y la soberanía tecnológica.
Revista de Derecho Comunitario Europeo, 84, 11-24.
doi: https://doi.org/10.18042/cepc/rdce.84.01

[1] Catedrático en el Departamento de Derecho Internacional Público y Relaciones Internacionales de la Facultad de Derecho de la Universidad de Granada.

SUMARIO

I. INTRODUCCIÓN

La actividad legislativa de la Unión Europea relativa al espacio digital ha estado orientada de forma tradicional hacia la consecución de la ciberseguridad (Segura Serrano, 2023). Esa regulación fundamentalmente persigue reforzar la ciberresiliencia, tal y como se desprende de la Estrategia de Ciberseguridad de la UE aprobada en 2020[2]. De acuerdo con esta estrategia, en el plano interno se ha adoptado el Reglamento de Ciberresiliencia[3], cuyo objetivo fundamental consiste en fijar requisitos obligatorios para la seguridad de los productos con elementos digitales, y que establece obligaciones de diligencia a fabricantes, importadores y distribuidores. Además, cabe mencionar el Reglamento de Cibersolidaridad[4], cuya meta es mejorar la preparación y capacidades de los Estados y operadores para prevenir y responder a incidentes de ciberseguridad significativos y a gran escala. Del mismo modo, se ha avanzado en esa ciberseguridad a través de la Directiva NIS 2[5], junto con el

[2] Comisión Europea y Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad, Comunicación Conjunta al Parlamento Europeo y al Consejo, *La Estrategia de Ciberseguridad de la UE para la Década Digital*, Bruselas, 16.12.2020, JOIN(2020) 18 final.

[3] Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.º 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (DO L, 2024/2847, de 20.11.2024).

[4] Reglamento (UE) 2025/38 del Parlamento Europeo y del Consejo, de 19 de diciembre de 2024, por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar ciberamenazas e incidentes, prepararse y responder a ellos, y por el que se modifica el Reglamento (UE) 2021/694 (Reglamento de Cibersolidaridad) (DO L, 2025/38, de 15.1.2025).

[5] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE)

Reglamento DORA aplicable en el sector financiero[6]. En el plano externo, la «caja de herramientas de la ciberdiplomacia» ha permitido a la UE dotarse de un mecanismo de reacción frente a los ciberataques de origen estatal, con un régimen sancionador al que después se aludirá.

Sin embargo, si dejamos de lado el enfoque basado en la ciberresiliencia, lo que aparece es una aproximación normativa de la UE con relación al espacio digital que se puede calificar como divergente. En efecto, la posición de la Unión Europea y sus Estados miembros con relación a la regulación del espacio digital se mueve últimamente entre dos aguas. En el plano externo, la UE ha manifestado tradicionalmente una postura ortodoxa, esto es, liberal e internacionalista, con respecto a la regulación del ciberespacio a escala global. En ese sentido, la UE ha mantenido siempre el criterio de la aplicabilidad del derecho internacional y la Carta de las Naciones Unidas al ciberespacio, rechazando que el espacio digital sea un ámbito ajeno a la regulación estatal o, en última instancia, no sujeto a regulación alguna. La reciente Declaración de la UE y sus Estados miembros de 2024 sobre una interpretación común de la aplicación del derecho internacional al ciberespacio[7] constituye el más reciente exponente de esta aproximación. Este enfoque acerca a la UE a la interpretación sostenida por el grupo de expertos que ha elaborado el Manual de Tallin (Schmitt, 2017). De esta forma, en mi opinión, la UE y sus Estados miembros ponen de manifiesto una doble intencionalidad. Por una parte, la UE se muestra extremadamente respetuosa con relación al ordenamiento jurídico internacional, frente a otras posiciones expresadas por distintas potencias en este ámbito. Por otro lado, la UE pretende instrumentalizar el derecho internacional en su beneficio, como herramienta protectora frente a los ciberataques, en un contexto en el que la UE asume que no se encuentra a la cabeza del desarrollo tecnológico más puntero.

Esta última afirmación conecta con la segunda parte del análisis que pretendo llevar a cabo. Desde hace algún tiempo, la UE ha iniciado un proceso regulatorio en el plano interno que tiene como destinatarias las actividades llevadas a cabo en el espacio digital y que traduce una aproximación menos

n.º 910/2014 y la Directiva (UE) 2018/1972, y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (DO L 333, de 27.12.2022, pp. 80-152).

6 Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011 (DO L 333, de 27.12.2022, pp. 1-79).

7 Council of the European Union, Declaration on a Common Understanding of International Law in Cyberspace, 15833/24, Brussels, 18 November 2024.

liberal, más intervencionista, desde el momento en que este ciberespacio se ha convertido en un terreno de competición tecnológica y, en la misma medida, económica. En efecto, iniciativas como la Ley de Servicios Digitales (DSA)[8] o la Ley sobre Inteligencia Artificial (AI Act)[9] pueden interpretarse como intentos de remediar a través de las normas del derecho de la UE una situación de evidente retraso tecnológico. En definitiva, el derecho internacional y el derecho de la UE se están utilizando por parte de la UE en el marco de la regulación del espacio digital de forma diversa, es decir, liberal en el primer caso pero intervencionista en el segundo, aunque con un objetivo común, esto es, revertir o, al menos, soslayar el retraso tecnológico de la UE.

II. LA VISIÓN LIBERAL DEL CIBERESPACIO

La Unión Europea ha manifestado de modo formal hace relativamente poco tiempo su visión sobre la regulación internacional del ciberespacio, que pone de relieve una determinada opción normativa. En efecto, la «Declaración de la Unión Europea y sus Estados miembros sobre una interpretación común de la aplicación del derecho internacional al ciberespacio» de 2024 ha explicitado una posición política y jurídica que se puede denominar como propia de la ortodoxia liberal e internacionalista. No obstante, esta interpretación no es nueva, puesto que ya se venía expresando de forma reiterada a través de otros documentos fundamentales dentro de la agenda de ciberseguridad de la UE, como la Estrategia de Ciberseguridad de 2013[10], o la de 2020, antes citada. La posición de la UE se fundamenta en la premisa de que el ciberespacio no es un

[8] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) (DO L 277, de 27.10.2022, pp. 1-102).

[9] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144, y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, de 12.7.2024, pp. 1-144).

[10] Comisión Europea, Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad, Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro*, Bruselas, 7.2.2013, JOIN(2013) 1 final.

espacio sin ley, sino que el derecho internacional es plenamente aplicable, siendo este ordenamiento «apto para su propósito» en la era digital.

Si nos centramos en el contexto, la Declaración de 2024 marca un hito en la política exterior y jurídica de la Unión Europea, definiendo lo que se puede describir como una visión ortodoxa, liberal e internacionalista sobre el ciberespacio. Aunque otros actores regionales como la Unión Africana ya habían emitido declaraciones similares, la postura de la UE es significativa por su alineación con el Manual de Tallin (Schmitt, 2017), un referente doctrinal promovido por la OTAN, que prepara ya su tercera edición. Como se ha mencionado, la UE se configura como una firme defensora del derecho internacional y su aplicabilidad en el ciberespacio. Esto implica la plena aplicabilidad de la Carta de las Naciones Unidas, el derecho internacional de los derechos humanos y el derecho internacional humanitario (DIH) en todas las actividades cibernéticas. Esta posición refuerza estrategias previas de la UE ya citadas y se apoya en las interpretaciones de Estados miembros como Francia, Alemania, Italia y los Países Bajos (Segura Serrano, 2023). La UE justifica la necesidad de esta interpretación común en el aumento en la escala, gravedad y sofisticación de los ataques cibernéticos, tanto de actores estatales como no estatales. Se mencionan amenazas específicas como el *ransomware,* el cual es calificado por la Unión como un peligro potencial para la paz y seguridad internacionales al poner en riesgo infraestructuras críticas y el funcionamiento de la sociedad digital. Ante esto, la UE reafirma su compromiso con el marco de la ONU sobre el comportamiento responsable de los Estados.

En primer lugar, en el apartado de las reglas previstas por esta declaración de 2024, una de las cuestiones más debatidas y fundamentales en la actualidad reside en la determinación de la naturaleza de la soberanía estatal en el ámbito digital. La postura de la UE consiste en lo que se puede denominar la «teoría pura de la soberanía». Esto es, la Declaración de 2024 sostiene que la soberanía es una regla primaria del derecho internacional y no solo un principio general. Esto significa que su violación constituye, por sí misma, un hecho ilícito internacional, incluso si no hay uso de la fuerza o intervención coercitiva. Según la UE, la soberanía se ve vulnerada cuando hay un ataque a la integridad territorial o una usurpación de funciones gubernamentales. Además, se sostiene una «interpretación amplia del daño». A diferencia del Manual de Tallin, que suele exigir daño físico o pérdida de funcionalidad para declarar una violación, la UE adopta una visión más estricta. A partir de la «caja de herramientas de la ciberdiplomacia», la UE ha adoptado medidas restrictivas en este ámbito[11] y este

[11] Decisión (PESC) 2019/797 del Consejo, de 17 de mayo de 2019, relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros

régimen sancionador considera que el mero acceso transfronterizo no autorizado a un sistema de información ya puede constituir una violación de la soberanía. Esta visión ortodoxa choca frontalmente con la del Reino Unido, que niega que la soberanía sea una norma autónoma que prohíba conductas más allá de la no intervención. Por su parte, Estados Unidos mantiene una posición ambigua. Mientras que sus asesores jurídicos históricos defendían la soberanía como regla, el Departamento de Defensa ha sugerido que solo es un principio general que sirve de base para otras normas. La UE rechaza esta visión «relativa» para evitar que las operaciones de baja intensidad queden en la impunidad legal.

La obligación de diligencia debida es igualmente acogida de forma amplia por la UE y sus Estados miembros, lo que acerca esta posición a la del Manual de Tallin. Se presenta así la diligencia debida como la herramienta clave para gestionar la responsabilidad cuando los ataques provienen de actores no estatales o se utilizan infraestructuras de terceros países. El fundamento jurídico es clásico. La UE vincula este principio con la jurisprudencia tradicional de la Corte Internacional de Justicia (asunto del *Canal de Corfú*)[12], estableciendo que los Estados no deben permitir a sabiendas que su territorio sea usado para actos ilícitos contra otros Estados. La diligencia debida se configura como una obligación de conducta, no de resultado, y se define como la obligación de adoptar «todas las medidas adecuadas, razonablemente disponibles y viables» para prevenir y detener actividades dañinas. Sin embargo, no se exige una «monitorización preventiva» de todas las redes, ya que esto podría vulnerar derechos humanos, pero sí se incluye el conocimiento constructivo (lo que el Estado *debería* haber sabido). La utilidad práctica para el ciberespacio de esta articulación jurídica es evidente. La gran ventaja de la diligencia debida es que permite exigir responsabilidades a un Estado por su omisión o negligencia, obviando las extremas dificultades técnicas de la atribución directa de un ciberataque. No obstante, es una obligación polémica para algunos, ya que puede imponer una carga muy pesada a los Estados con gran infraestructura digital (Schmitt, 2015).

En segundo lugar, la Declaración de 2024 analiza cómo los Estados pueden reaccionar ante ciberataques ilícitos, entre otras, a través de las contramedidas, que, como se sabe, son medidas que, siendo normalmente ilícitas, pierden ese carácter cuando se usan para obligar a un Estado infractor

(DO L 129I, 17.5.2019, pp. 13-19); Reglamento (UE) 2019/796 del Consejo, de 17 de mayo de 2019, relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros (DO L 129I, 17.5.2019, pp. 1-12).

12 *Corfu Channel* case, Judgment of April 9th, 1949: *I.C.J. Reports* 1949, p. 4, 22.

a cumplir sus obligaciones. La UE mantiene una postura tradicional y acorde con el proyecto de artículos de la Comisión de Derecho Internacional[13], ya que asume los requisitos de proporcionalidad y reversibilidad, pero introduce un «enfoque pragmático». En efecto, el elemento más crítico consiste en que la UE, siguiendo al Reino Unido y al Manual de Tallin, parece prescindir del requisito de notificar previamente al infractor antes de actuar. Esta interpretación se justifica por la urgencia de la respuesta y para evitar que el infractor enmascare su actividad si es avisado. No obstante, en mi opinión, este enfoque convierte las contramedidas en algo cercano a una represalia punitiva, lo que aumenta el riesgo de escalada y confrontación internacional. Como otra herramienta útil, la UE menciona el estado de necesidad[14] que se puede invocar cuando un ciberataque amenaza un «interés esencial» del Estado (como infraestructuras críticas[15]) y la respuesta basada en el estado de necesidad es la única forma de salvaguardarlo. Esta opción presenta diversas ventajas en el ciberespacio. A diferencia de las contramedidas, el estado de necesidad no requiere atribución previa, ni siquiera la existencia de un ilícito internacional previo. Por tanto, se trata de una herramienta útil para reaccionar ante ciberataques de origen desconocido o procedentes de actores no estatales. Sin embargo, su carácter contextual y subjetivo, así como la falta de consenso sobre su naturaleza consuetudinaria, lo convierten en un instrumento jurídicamente delicado.

---

[13] Comisión de Derecho Internacional, texto del proyecto de artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos, *Anuario de la Comisión de Derecho Internacional*, 2001, Vol. II, Segunda Parte, Naciones Unidas, Nueva York, 2007, p. 26.

[14] *Ibid.*, véase el art. 25.

[15] A este respecto del «interés esencial» de un Estado, la Declaración de 2024 se limita a señalar que «[e]n el ámbito cibernético, un interés puede considerarse esencial en función del tipo de infraestructura que sea objeto real o potencial de una operación cibernética y cuando dicha infraestructura sea relevante para el Estado en su conjunto». No obstante, la UE se ha ocupado de regular en el ámbito de las infraestructuras críticas, señaladamente a través de la Directiva NIS-2 y la Directiva CER: Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (DO L 333 de 27.12.2022, pp. 80-152); Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo (DO L 333 de 27.12.2022, pp. 164-198).

III. LA SOBERANÍA TECNOLÓGICA

La UE se ha embarcado en una apuesta por la soberanía tecnológica que se ha reforzado claramente desde el nombramiento de una comisaria para ocupar una cartera con esta denominación, en concreto, Henna Virkkunen, comisaria de Soberanía Tecnológica, Seguridad y Democracia. La soberanía tecnológica está relacionada con la seguridad económica en su sentido más amplio, donde cabe mencionar la Comunicación sobre la Estrategia Europea de Seguridad Económica de 2023[16], que se ha visto completada con otras comunicaciones de 2024[17] y 2025[18].

No obstante, en lo que aquí interesa desde el punto de vista normativo, se han adoptado diversas iniciativas de calado, donde destacan la Ley de Servicios Digitales (DSA) y la Ley de Inteligencia Artificial (AI Act) como herramientas para la consecución de la soberanía digital. La cuestión que se plantea es si estas normativas representan una verdadera recuperación del control público o si son una reacción tardía ante el dominio estructural de las grandes empresas tecnológicas extranjeras. Además, resulta muy relevante destacar qué opción normativa se ha elegido para conseguir ese objetivo.

El concepto de *soberanía digital* ha dejado de ser un tecnicismo para convertirse en una «palabra de moda» en los círculos de la Unión Europea. Esta noción ha sido adoptada por las instituciones de la UE para impulsar una estrategia que busca elevar el perfil del bloque en el ámbito de las tecnologías digitales. No obstante, este discurso no nace de una posición de fuerza, sino de una percepción de vulnerabilidad que se traduce en la pérdida de competitividad económica, una capacidad de innovación limitada y una dependencia alarmante de infraestructuras y proveedores de servicios extranjeros. En el centro de esta problemática se encuentran las empresas conocidas como GAFAM (Google, Amazon, Facebook/Meta, Apple y Microsoft), que dominan el mercado digital

---

16 Comunicación conjunta de la Comisión Europea y del Alto Representante, Estrategia Europea de Seguridad Económica, Bruselas, JOIN(2023) 20 final, 20 de junio de 2023. En este documento se identifican como riesgos la seguridad tecnológica (incluidas las filtraciones indeseadas de tecnología) y la seguridad física y cibernética de las infraestructuras críticas.

17 Comunicación de la Comisión Europea, «Afianzar la seguridad económica europea: introducción a cinco nuevas iniciativas», Bruselas, COM(2024) 22 final, 24 de enero de 2024, que profundiza en algunas de las medidas identificadas previamente, en particular en aquellas relacionadas con la protección de la tecnología.

18 Comunicación conjunta de la Comisión y de la Alta Representante PESC al Parlamento Europeo y al Consejo, «Fortalecer la seguridad económica de la UE», JOIN(2025) 977 final, de 3 de diciembre de 2025.

en lo que se ha denominado una «soberanía corporativa digital *de facto*». Esta soberanía privada se construye sobre monopolios que trascienden lo económico, alcanzando dimensiones sociales, políticas y geoestratégicas. Ante esto, la UE ha respondido con un enfoque más dirigista, proteccionista y realista, propio de la «Comisión geopolítica» de Ursula von der Leyen, que ve en la acumulación de riqueza y poder en el ciberespacio un pilar de su autonomía estratégica. Desde un punto de vista crítico, la soberanía digital en la UE opera como una «performatividad retórica». Se proyectan desafíos de seguridad, economía y valores hacia un futuro de integración donde la regulación se mezcla con enfoques infraestructurales y geopolíticos. Lo digital ya no se percibe como una actividad separada, sino como un espacio material de la política global donde se ponen en juego la seguridad y los valores europeos.

La DSA se presenta como la «segunda generación» de reglas para los servicios digitales, heredera de la Directiva de Comercio Electrónico (DCE) del año 2000[19]. La DCE, inspirada en el modelo estadounidense de la Digital Millenium Copyright Act (DMCA)[20], estableció un «contrato social digital» basado en la exención de responsabilidad de los intermediarios para fomentar el crecimiento de internet. Este modelo fue esencial para el florecimiento de los servicios que conocemos hoy, vinculando la inmunidad de los proveedores con la libertad de expresión. Sin embargo, transcurridos más de veinte años desde su puesta en marcha, la realidad ha cambiado drásticamente. El uso cotidiano de servicios digitales, el internet de las cosas y la aparición de problemas graves como el terrorismo, el discurso de odio y el abuso infantil han venido a justificar una nueva ola regulatoria. Las tecnológicas ya no son industrias nacientes, sino las empresas más ricas del mundo, con capacidad de influir en procesos electorales y conflictos bélicos. Por esa razón, la DSA mantiene las exenciones de responsabilidad de la DCE, pero introduce un sistema de obligaciones de diligencia debida como contrapeso. Es importante señalar que la DSA prohíbe explícitamente una obligación general de supervisión activa, ya que esto chocaría con los derechos fundamentales. No obstante, introduce la «cláusula del buen samaritano», que permite a los proveedores realizar investigaciones voluntarias para eliminar contenido ilegal sin perder su inmunidad por ello.

La verdadera novedad de la DSA radica en la creación de diferentes niveles de obligaciones, estableciendo una responsabilidad institucionalizada

[19] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el Comercio Electrónico) (DO L 178 de 17.7.2000, pp. 1-16).

[20] Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

basada en el proceso debido. Este sistema es asimétrico y proporcional, es decir, a mayor tamaño y dominio de la plataforma, mayor es la responsabilidad asignada. Las obligaciones se dividen en cuatro capas: a) Obligaciones universales: designación de puntos de contacto y transparencia en las políticas de moderación. b) Obligaciones básicas: para servicios de alojamiento, incluyendo mecanismos de «notificación y acción» contra contenidos ilegales y la obligación de motivar las decisiones de moderación para evitar el *shadow banning*. c) Obligaciones avanzadas: para plataformas que no son pequeñas empresas, centradas en la equidad de los procesos de moderación y la prohibición de «patrones oscuros» (interfaces engañosas). d) Obligaciones para plataformas en línea de muy gran tamaño (VLOP, por sus siglas en inglés) y motores de búsqueda en línea de muy gran tamaño (VLOSE): aplicables a plataformas y buscadores con más de 45 millones de usuarios en la UE.

La DSA ha generado ya una jurisprudencia relativa a la designación de ciertas plataformas como VLOP o VLOSE, una designación que las sujeta, por tanto, a obligaciones más estrictas. Entre las sentencias dictadas por el TG, normalmente favorables a la designación de la Comisión y recurridas por las respectivas plataformas ante el TJUE, se encuentran asuntos como *Zalando, Amazon y otros*[21]. De igual modo, la tasa de supervisión a pagar por los VLOP y los VLOSE de acuerdo con el art. 43 de la DSA ha sido recurrida por las plataformas ante el TG y, tras perder en estos asuntos, la Comisión ha interpuesto recurso de casación ante el TJUE[22]. No obstante, aún no existe jurisprudencia relativa a las nuevas obligaciones materiales previstas en la DSA

[21] Véanse los asuntos T-348/23, Zalando/Comisión; T-367/23, Amazon/Comisión; T-139/24, WebGroup/Comisión; T-138/24, Aylo Freesites/Comisión (en relación con la designación de Pornhub), y C-134/24, Technius/Comisión (en relación con la designación de Stripchat). Las medidas cautelares solicitadas tanto en el asunto *Amazon* como en los asuntos *Aylo y WebGroup* fueron desestimadas mediante autos del presidente del Tribunal General de 23 de septiembre de 2023, 2 de julio de 2024 y 12 de julio de 2024, respectivamente. Amazon ha perdido finalmente el asunto ante el Tribunal General en la Sentencia de 19 de noviembre de 2025, Amazon/Comisión, T-367/23, EU:T:2025:1038 (recurrida ante el TJUE respectivamente por Amazon, asunto C-40/26P, y la Comisión, asunto C-47/26P). Zalando ha perdido el caso en la Sentencia de 3 de septiembre de 2025, Zalando/Comisión, T-367/23, EU:T:2025:821 (recurrida por Zalando ante el Tribunal de Justicia, asunto C-724/25 P).

[22] Meta y TikTok han ganado el caso ante el Tribunal General (Sentencia de 10 de noviembre de 2025, Meta Platforms Ireland/Comisión, T-55/24, EU:T:2025:842; Sentencia de 10 de noviembre de 2025, TikTok Technology/Comisión, T-58/24, EU:T:2025:843). La Comisión ha interpuesto recurso de casación (asuntos C-744/25 P y C-745/25 P, respectivamente).

a cargo de los proveedores de servicios digitales y que, a buen seguro, será la que ofrezca la medida del éxito en el esfuerzo regulador desarrollado a través de esta iniciativa normativa.

A pesar de su ambición, la DSA presenta debilidades críticas. Se ha argumentado por la literatura especializada que la norma es prescriptiva sobre los objetivos, pero no sobre el «cómo» alcanzarlos, lo que otorga a las plataformas una gran discrecionalidad para diseñar sus propios estándares de cumplimiento (Kausche y Weiss, 2025). Un ejemplo claro es la prohibición de la publicidad dirigida a menores, que solo se aplica si la plataforma sabe «con razonable certeza» que el usuario es menor, pero la DSA no les obliga a verificar la edad. Esto revela una tendencia a «subcontratar» las decisiones primordiales sobre derechos fundamentales y gobernanza del discurso a las propias plataformas. En la práctica, las grandes tecnológicas (VLOP y VLOSE) continúan actuando en gran medida según sus propios «términos de uso», preservando el control sobre sus modelos de negocio. Aunque la DSA incluye la protección de derechos fundamentales entre sus preceptos, existe el riesgo de que las plataformas utilicen estos procesos solo para dotar de legitimidad a sus propias decisiones comerciales, sin abordar las cuestiones estructurales de poder. Además, el sistema de auditorías independientes pagadas por las propias plataformas genera el riesgo de *audit-washing* (lavado de imagen mediante auditorías). La expectativa de futuros contratos puede influir en la objetividad del auditor, permitiendo que las plataformas ejerzan su poder de mercado frente a los mecanismos de control. En última instancia, la supervisión de la DSA podría ser considerada de «guante de seda», dejando a los gigantes tecnológicos una autonomía relativa considerable.

Por lo que se refiere a la Ley de Inteligencia Artificial (AI Act), ha surgido como un esfuerzo para recuperar el control frente a la brecha tecnológica, especialmente evidente tras la irrupción de modelos generativos como ChatGPT, dominados por empresas estadounidenses. La ley persigue dos metas principales, esto es, el funcionamiento del mercado interior y la protección de los derechos fundamentales. Asimismo, busca el llamado «efecto Bruselas» (Bradford, 2019), intentando establecer el estándar global para la IA. La UE ha optado por regular la IA centrándose en sus «objetos» o productos, aplicando su metodología tradicional de «seguridad de productos». La ley distingue entre «sistemas de IA» (componentes de *software*) y «modelos de IA de propósito general». El sistema se basa en un enfoque de riesgo: a) riesgo inaceptable: prácticas prohibidas como la puntuación social, la manipulación subliminal y el raspado masivo de imágenes faciales; b) alto riesgo: sistemas en sectores críticos (empleo, salud, justicia) que deben cumplir con «requisitos esenciales» de gestión de riesgos, gobernanza de datos y super-

visión humana; y c) riesgo limitado: sistemas como los chatbots que están sujetos principalmente a obligaciones de transparencia.

La crítica fundamental que formula la doctrina especializada al AI Act es el desajuste existente entre los medios (seguridad de producto) y los fines (protección de derechos fundamentales) (Cantero Gamito y Marsden, 2024). La ley se inspira en el Nuevo Marco Legislativo, que delega los detalles técnicos a organizaciones de estandarización privadas como el Comité Europeo de Normalización (CEN) o el Comité Europeo de Normalización Electrotécnica (CENELEC). Pero este enfoque plantea dos problemas graves. En primer lugar, da lugar a la denominada captura regulatoria, esto es, los detalles técnicos de la ley son redactados por actores industriales privados en procesos opacos, lo que significa que las empresas están redactando las mismas normas por las que serán gobernadas. En segundo lugar, se produce una asimilación de la lógica binaria frente a la proporcionalidad. En otras palabras, mientras que la seguridad de un producto se puede evaluar con una lógica de «se cumple o no se cumple», la protección de los derechos fundamentales requiere un juicio de proporcionalidad dependiente del contexto, para el cual los estándares técnicos son instrumentos inadecuados. Además, en la literatura académica (Almada y Petit, 2025) se ha criticado ya que el AI Act es más un instrumento orientado al mercado que uno relativo a la protección de derechos fundamentales, a diferencia de normativas como el Reglamento General de Protección de Datos (RGPD)[23]. Aunque la ley menciona los valores democráticos en su preámbulo, su inclusión en disposiciones vinculantes es muy limitada. Asimismo, el posible «efecto Bruselas» podría ser contraproducente si lo que se exporta globalmente es una protección inadecuada de los derechos fundamentales.

IV. REFLEXIONES FINALES

La UE pretende instrumentalizar el derecho internacional y el derecho de la UE para alcanzar sus objetivos tecnológicos y económicos en el marco de la regulación del ciberespacio. Por una parte, la UE ha adoptado una interpretación de la aplicación del derecho internacional en el ciberespacio que se antoja típicamente ortodoxa y liberal, muy respetuosa de las reglas básicas de

[23] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, pp. 1-88).

este ordenamiento. Ahora bien, a través de esa interpretación resulta evidente que la UE aspira a alcanzar una meta última, como es la de dotarse de instrumentos jurídico-internacionales contundentes para hacer frente a las actividades maliciosas desarrolladas en el ciberespacio. La UE y muchos Estados miembros no cuentan con las capacidades tecnológicas suficientes como para contrarrestar con garantías estas actividades cibernéticas de carácter malicioso, por lo que el derecho internacional se convierte en un recurso idóneo en manos de la UE para reaccionar frente a los actores estatales, pero también no estatales, que pueden causar importantes daños a los ciudadanos de la UE. En este sentido, la postura de la UE busca fortalecer el imperio de la ley en el ciberespacio mediante una defensa cerrada de la soberanía y la diligencia debida. Al adoptar, además, interpretaciones que facilitan la respuesta jurídica asertiva (como prescindir de la notificación en las contramedidas o el recurso al estado de necesidad), la Unión Europea intenta dotar a las democracias liberales de herramientas eficaces de ciberdefensa activa, asumiendo los riesgos de una posible inestabilidad en las relaciones internacionales debido a la falta de consenso global sobre estas normas.

Sin embargo, por otra parte, el derecho de la UE también está siendo utilizado para hacer frente al retraso tecnológico de la UE, que la hace tan dependiente y vulnerable frente a los gigantes del sector. La búsqueda de la soberanía digital a través de la regulación refleja una respuesta estratégica de la UE ante su bajo rendimiento tecnológico. La DSA y el AI Act representan el paso de un modelo de «libre acceso» a uno de «orden público», donde lo digital es un espacio más de la política global en la que se ponen en juego valores y seguridad. No obstante, persiste una tensión fundamental en este esfuerzo regulador que consiste en el deseo de una intervención pública robusta frente a la realidad de que las grandes plataformas siguen operando mayoritariamente bajo sus propios términos de uso. La dependencia de estándares técnicos privados y la supervisión «laxa» que estas nuevas normativas incluyen sugieren que la UE podría estar legitimando el poder de las Big Tech en lugar de desafiarlo estructuralmente. Para que la soberanía digital sea una realidad y no solo una retórica performativa, la UE deberá encontrar formas de cerrar la brecha entre sus ambiciones geopolíticas y la capacidad práctica de controlar un ecosistema digital dominado por actores que, a pesar de las nuevas leyes, mantienen una autonomía estratégica formidable.

Bibliografía

Almada, Marco y Petit, Nicolas (2025). The EU AI Act: Between the rock of product safety and the hard place of fundamental rights. *Common Market Law Review,* 62, 85-120. Disponible en: https://doi.org/10.54648/COLA2025004.

Bradford, Anu (2019). *The Brussels Effect: How the European Union rules the world.* Oxford: Oxford University Press. Disponible en: https://doi.org/10.1093/oso/9780190088583.001.0001.

Cantero Gamito, Marta y Marsden, Christopher T. (2024). Artificial intelligence co-regulation? The role of standards in the EU AI Act. *International Journal of Law and Information Technology,* 32, 6. Disponible en: https://doi.org/10.1093/ijlit/eaae011.

Kausche, Katharina y Weiss, Moritz (2025). Platform power and regulatory capture in digital governance. *Business and Politics,* 27, 288-289. Disponible en: https://doi.org/10.1017/bap.2024.33.

Schmitt, Michael N. (2015). In defense of due diligence in cyberspace. *The Yale Law Journal Forum,* 68-81.

Schmitt, Michael N. (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations.* Cambridge: Cambridge University Press.

Segura Serrano, Antonio (2023). *El desafío de la ciberseguridad global. Análisis desde el derecho internacional y europeo.* Valencia: Tirant lo Blanch.