1

LAS NUEVAS COORDENADAS DEL DERECHO DIGITAL EUROPEO

THE NEW COORDINATES OF EUROPEAN DIGITAL LAW

Moisés Barrio Andrés

Letrado del Consejo de Estado. Profesor de Derecho digital. Consultor.
Director del Diploma de Alta Especialización en Legal Tech y transformación digital (DAELT)
de la Escuela de Práctica Jurídica de la Universidad Complutense de Madrid

Sumario

I. INTRODUCCIÓN

El Derecho digital europeo, a diferencia de sus equivalentes estadounidense y chino, tiene como principio estructural el respeto de los derechos fundamentales. La Unión Europea (UE) ha adoptado un enfoque centrado en el ser humano para regular la sociedad digital, en el que los derechos fundamentales y la noción de un mercado justo constituyen la base de la regulación (BARRIO ANDRÉS, 2022, pp. 120-134). Según este modelo, la intervención regulatoria es necesaria para defender

los derechos fundamentales de las personas, preservar las estructuras democráticas de la sociedad y garantizar una distribución justa de los beneficios de la economía digital.[1] La tecnología debe aprovecharse para el empoderamiento humano y con el objetivo de salvaguardar la autonomía política de los ciudadanos digitales.

Por eso, a diferencia del Derecho digital norteamericano, que se centra en la protección de la libertad de expresión como derecho fundamental casi absoluto y en la primacía del mercado, el Derecho digital de la UE trata de equilibrar el derecho a la libertad de expresión con una serie de otros derechos fundamentales, como la dignidad humana y el derecho a la intimidad. Frente al Derecho digital chino —que también reserva un papel importante al Estado en la dirección de la economía digital—, el Derecho digital europeo está orientado a mejorar, no a recortar, los derechos de los ciudadanos frente a las empresas tecnológicas y al Estado.

El marco regulador de la UE también pone especial énfasis en que la transformación digital debe estar firmemente anclada en el Estado de Derecho y la gobernanza democrática. Mientras que el Derecho digital norteamericano impulsado por el mercado a menudo hace hincapié en que los gobiernos no entienden la tecnología y, por lo tanto, deberían abstenerse de regularla, el Derecho digital europeo guiado por la salvaguardia de los derechos está más preocupado por que las empresas tecnológicas respeten los pilares de la democracia constitucional y los derechos fundamentales de los usuarios de Internet (NEMITZ, 2018). Como resultado, según el modelo regulador europeo, el Estado debe regular la economía digital con el objetivo de proteger los valores superiores y los derechos fundamentales como pilares de una sociedad democrática liberal.

Por eso, la Unión Europea reglamenta el mundo digital de forma exhaustiva. En los últimos años se ha producido no sólo un aumento del volumen de esa regulación del Derecho digital europeo (número de instrumentos normativos —directivas, reglamentos y actos delegados de la Comisión Europea—), sino también una ampliación de su ámbito de aplicación (número de materias incluidas), la profundidad (extensión de la intervención del legislador) y los requisitos de cumplimiento que afectan a las empresas (el llamado *compliance*).

---

1. Así lo expresa la Declaración Europea sobre los Derechos y Principios Digitales para la década digital, de 15 de diciembre de 2022, que sigue los pasos de la Carta española de Derechos Digitales, de 14 de julio de 2021. El objetivo de la Declaración, como también de nuestra Carta, es guiar a los responsables de las políticas públicas cuando reflexionen sobre la concepción de la transformación digital, así como determinar un marco de referencia a las empresas y otros agentes pertinentes a la hora de desarrollar e implantar las tecnologías emergentes. Y aclara cómo se aplican los valores constitucionales y los derechos fundamentales de la UE en el entorno en línea, y los sitúa en el núcleo de su marco. Por tanto, no es una norma jurídica. A pesar de ser un documento puramente declarativo, la Declaración Europea sobre los Derechos y Principios Digitales viene a reforzar los valores ya anunciados en iniciativas previas como la Declaración de Tallin sobre la administración electrónica de 2017, la Declaración de Berlín sobre la sociedad digital y el gobierno digital basado en valores de 2020, y la Declaración de Lisboa: democracia digital con propósito de 2021.

Ahora bien, estas nuevas coordenadas crean incertidumbres, ya que las organizaciones se enfrentan a entornos normativos inéditos, nuevos preceptos que deben interpretarse en un conjunto no siempre bien trabado, mecanismos de aplicación desconocidos, nuevas agencias reguladoras y un entorno en rápida evolución que depende de una combinación de regulación tradicional, actos delegados y *soft law*. Además, y debido al denominado «efecto Bruselas» (BRADFORD, 2020)[2], el Derecho digital europeo ha adquirido una importancia planetaria, más allá de sus fronteras jurisdiccionales. A ello dirigiremos nuestros próximos pasos.

II. LA INFLUENCIA DE LA UNIÓN EUROPEA EN LA REGULACIÓN DIGITAL MUNDIAL

La regulación del mundo digital en la Unión Europea es importante a nivel mundial debido al gran volumen de comercio transatlántico, intercambios bilaterales y de otro tipo con la UE (ORTEGA JIMÉNEZ, 2022). Las empresas que entablan negocios con la UE no tienen más remedio que conocer el marco normativo del Derecho digital europeo y cumplirlo. Esto se debe a que la legislación europea impone exigencias directas sobre los productos, servicios o prácticas comerciales de las empresas debido a su efecto extraterritorial (arts. 3 del RGPD, 2.1 del Reglamento DSA y 1.2 del Reglamento DMA).

Los entornos normativos dinámicos como la UE plantean retos únicos a los operadores jurídicos: así, pueden incluir normas jurídicas que cambian rápidamente y, en ocasiones, están redactadas de forma amplia; interpretaciones inciertas que, a menudo, acaban en procesos administrativos y jurisdiccionales que duran años; nuevas agencias públicas reguladoras con mayores competencias y la necesidad de cumplir un conjunto muy diverso de grupos normativos que rigen funciones empresariales que van desde el comercio electrónico, la protección de los consumidores y la protección de datos, hasta las telecomunicaciones y las normas sectoriales sobre nuevas tecnologías emergentes.

Obsérvese que este modelo trastoca las nociones tradicionales de gobierno corporativo, gestión de riesgos y cumplimiento de las organizaciones privadas. Hoy

2. El «efecto Bruselas» es un término que se refiere a la influencia que la legislación y las regulaciones de la Unión Europea (UE) tienen sobre los estándares y normas jurídicas en otros países y regiones del mundo. Esta influencia puede surgir directamente, por ejemplo, cuando las empresas quieren acceder al mercado de la UE y, por lo tanto, deben cumplir con sus regulaciones, o indirectamente, cuando otros países adoptan normas similares a las de la UE debido a su liderazgo y ejemplo en ciertas áreas. La Unión Europea, dada su dimensión económica y política, tiene una gran capacidad para influir en los estándares globales. Por ejemplo, el Reglamento General de Protección de Datos (RGPD) de la UE ha influenciado la forma en que se configuran las leyes de protección de datos en todo el mundo. Y muchas empresas radicadas fuera de la UE han adoptado políticas y prácticas acordes con el RGPD para garantizar el acceso al mercado europeo. De manera similar, otros países han tomado el RGPD como el modelo para sus propias leyes de privacidad –incluyendo a Estados Unidos– (BARRIO ANDRÉS, 2022c).

en día, el cumplimiento o *compliance* —tradicionalmente considerado como la observancia por parte de las empresas de las normas creadas externamente por los legisladores o la administración pública— no se ajusta a los nuevos modelos de gobierno corporativo, sino que fuerza cambios en la estructura de gobierno interno de una empresa desde el exterior (CAMPOS ACUÑA, 2020). También el cumplimiento es, cada vez más, un ejercicio de gestión de riesgos (BARRIO ANDRÉS, 2023). Al mismo tiempo, los directivos jurídicamente avezados pueden utilizar estratégicamente aspectos del marco regulatorio del Derecho digital europeo en el mundo digital para la legítima ventaja competitiva de su empresa (por ejemplo, estableciendo sus centros de datos en Europa o España).

Una organización moderna es necesariamente digital en uno o varios de sus pilares: presencia digital (correo electrónico, página web, cuentas en redes sociales, sede electrónica en el caso de las Administraciones Públicas…), prácticas de venta (pedidos, entregas, suministros), pagos y operaciones complementarias. Aunque las nuevas normas del Derecho digital europeo están específicamente destinadas a los intermediarios, los agentes digitales y las plataformas, también son importantes para todas las organizaciones por la sencilla razón de que las plataformas permiten llegar al cliente y reducir los costes de transacción, y desempeñan un papel crucial en la cadena de valor. Las empresas deben ajustar sus estrategias tanto si consideran que las normas son favorables al sector privado como si no. Ello requiere unos comentarios adicionales.

III. EL IMPACTO DEL DERECHO DIGITAL EN LAS EMPRESAS PRIVADAS

El modelo regulatorio del Derecho digital europeo ha cambiado significativamente en los últimos años. Las nuevas normas afectan a la estrategia empresarial tanto de las empresas de la UE como de las de fuera de ella de dos maneras fundamentalmente distintas. En primer lugar, las propias empresas están sujetas a tales normas en la medida en que entran en el ámbito de aplicación de los nuevos instrumentos marco de la UE y los reglamentos europeos sectoriales del sector digital. En segundo lugar, dado que las empresas dependen de las plataformas, el comportamiento de éstas afecta a la estrategia empresarial del propio sector privado en su conjunto (MONTERO PASCUAL, 2023, p. 67).

Mientras que los clientes reclaman que las plataformas deben proteger a los usuarios y promover la seguridad, las empresas dan prioridad a la limitación de su responsabilidad y se centran en utilizar plataformas que puedan ser proactivas a la hora de moderar el riesgo. Aunque las empresas se esfuerzan por conseguirlo, también necesitan mantener los costes bajos y seguir siendo competitivas en la UE y en otros mercados. Unas obligaciones procedimentales claras con sanciones conocidas para las plataformas crean un clima de certidumbre, pero las empresas perciben el exceso de regulación de las plataformas como algo indeseable, ya que consideran que disminuyen las oportunidades de negocio. Unas normas coherentes, como el

nuevo Reglamento europeo de Servicios Digitales (el Reglamento DSA o *Digital Services Act* por sus siglas inglesas), contribuyen a crear condiciones equitativas para las empresas al favorecer este equilibrio.

El vigente Derecho digital europeo ha aumentado la regulación de las plataformas, los requisitos de protección de los consumidores/usuarios y las exigencias de mejora de la ciberseguridad. La normativa digital tradicional de la UE, formulada en gran medida a principios de la década de 2000 siguiendo el modelo norteamericano de la *Communications Decency Act* (CDA) de 1996 y la *Digital Millennium Copyright Act* (DMCA) de 1998, se basaba en la idea de que no debía «regularse por regular» y que incluso Internet no debía regularse prácticamente en absoluto. Este planteamiento de *laissez-faire* ha sido sustituido por normas complejas y exigentes. Las nuevas normas estructurales europeas, incluidas algunas sectoriales que se comentan a continuación, no sólo presentan más densidad regulatoria, sino que tienen características novedosas que exigen ajustes de estrategia. A mi juicio, cabe destacar cinco rasgos: legislación asimétrica, enfoque *ex ante*, legislación basada en el riesgo, mayor incertidumbre en la aplicación de la normativa e incierta interacción entre las fuentes del Derecho.

La regulación asimétrica significa que las distintas plataformas están reguladas de manera diferente, con obligaciones progresivamente más onerosas impuestas a las mayores plataformas intermediarias. Esto aporta más flexibilidad, pero también más incertidumbre. El enfoque *ex ante* es un nuevo método de regulación ya presente en el Reglamento europeo de Mercados Digitales (el Reglamento DMA por sus siglas inglesas de *Digital Markets Act*) de la UE y en la propuesta de Reglamento europeo de Inteligencia Artificial (RIA o *AI Act*). Impone restricciones a las plataformas dominantes que corren el riesgo de abusar de su posición. A diferencia de la regulación *ex post*, este enfoque se aplica antes de que se produzca una infracción real y en previsión de la misma. Los nuevos modelos de aplicación implican nuevos organismos públicos reguladores nacionales y de la UE, pero también la presencia de actos delegados que complican aún más el marco normativo. Por último, la multitud de fuentes reguladoras disminuye la claridad normativa y menoscaba la seguridad jurídica.

La segunda novedad, y posiblemente la más importante, es el aumento de las obligaciones de cumplimiento, en particular el cumplimiento basado en el riesgo (el *risk-based compliance*). El cumplimiento es el acto de ajustarse a las leyes, reglamentos y normas establecidas por el legislador, los organismos reguladores o a través de las normas del sector. Los programas de cumplimiento se aplican para garantizar que una organización opera dentro de los límites de las leyes y reglamentos aplicables. A diferencia del cumplimiento tradicional, que consiste en ajustarse a unas normas respaldadas por un sistema de sanciones, y que se presenta en forma binaria de cumplir/no cumplir, el cumplimiento basado en el riesgo impone que se lleve a cabo un proceso de evaluación de riesgos antes de formarse una idea clara de lo que hay que cumplir. En concreto, el cumplimiento basado en el riesgo exige que la dirección de la empresa identifique los riesgos específicos a los que se enfrenta una organización, que evalúe la magnitud y la probabilidad de

dichos riesgos y que aplique medidas para gestionarlos y mitigarlos, todo ello sin perder competitividad.

IV. EL NUEVO DERECHO DIGITAL EUROPEO BASADO EN EL RIESGO

Las cuatro principales normas estructurales del Derecho digital europeo imponen un cumplimiento basado en el riesgo. Se trata del Reglamento General de Protección de Datos (RGPD)[3], el Reglamento de Servicios Digitales (DSA)[4], la propuesta de Reglamento europeo de Inteligencia Artificial (RIA)[5] y la Directiva sobre Seguridad de las Redes y de la Información 2 (NIS2)[6].

Cada una aborda un aspecto fundamental del negocio digital: datos, economía de plataformas, tecnologías de IA y ciberseguridad. Cada una de ellas supone un cambio radical en su propio ámbito regulado, pero también todas son de importancia general para cualquier empresa, no solo aquellas que se dedican a comercializar productos o servicios digitales. Y la normativa de cumplimiento basada en el riesgo tiene un aspecto diferente para las distintas partes afectadas: creadores, colaboradores, minoristas y consumidores.

En el centro del enfoque de la regulación basado en el riesgo se encuentra una idea sencilla: los riesgos de los distintos sectores regulados son diferentes y los esfuerzos deben concentrarse en identificar y mitigar los más graves. La regulación basada en el riesgo es tanto un intento de centrarse en los riesgos como de darles una respuesta proporcionada. Entre los retos del cumplimiento basado en el riesgo figuran la incertidumbre, la complejidad del sector digital, la naturaleza siempre cambiante de la regulación digital y la dificultad de mantenerse al día (MUÑOZ VELA, 2022).

Existen dos enfoques básicos para la regulación basada en el riesgo: ascendente y descendente (DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, 2023; ROMERO JÍMENEZ, 2021), dependiendo de si la evaluación del riesgo está definida en la norma jurídica o no. La elección del método repercute en

---

3. 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).

4. 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).

5. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. COM/2021/206 final.

6. 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) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

la carga impuesta a los abogados internos. El enfoque ascendente, que se observa en el RGPD, deja el cumplimiento de la normativa principalmente en manos de la entidad regulada. Por el contrario, el enfoque descendente ordena la adopción de medidas en caso de que se identifiquen riesgos. A continuación veremos cómo se configuran en las señaladas normas estructurales del Derecho digital europeo.

1. Protección de datos

El precitado Reglamento General de Protección de Datos de 2016, una norma mundial *de facto* para la protección de datos personales, introdujo normas estrictas para la protección de datos personales, multas significativas y nuevos requisitos de cumplimiento. Aunque es bien conocido por sus rigurosos requisitos de cumplimiento, fue la primera «ley» digital europea en basar también algunas de sus disposiciones más importantes en la evaluación de riesgos (LÓPEZ CALVO, 2019).

La protección de datos desde el diseño y la protección de datos por defecto son conceptos clave que incorporan la evaluación de riesgos (art. 25 RGPD). Éstos exigen que se establezcan «medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados». En otras palabras, la protección de datos debe estar «integrada» o «encastrada» en los productos y servicios, y las empresas deben adoptar un enfoque mínimo en la recogida de datos. Y lo que es más importante, esto debe hacerse teniendo en cuenta «los riesgos de probabilidad variable».

Cuando el tratamiento de datos con nuevas herramientas entrañe un «alto riesgo para los derechos y libertades de las personas físicas», el artículo 35 del RGPD obliga a realizar una evaluación de impacto de la protección de datos. Se mencionan específicamente tres casos, frecuentes en la economía moderna: el tratamiento automatizado de datos y la elaboración de perfiles, las categorías especiales de datos del artículo 9.1 del RGPD y la vigilancia sistémica de espacios públicos.

Las evaluaciones de riesgos del RGPD no se centran únicamente en la ciberseguridad o los riesgos de apoderamiento inconsentido de datos, sino también en la destrucción, pérdida o divulgación accidental o ilícita. En otras palabras, se trata de crear modelos empresariales en los que los datos puedan utilizarse de forma segura, legal y ética en beneficio de las empresas.

2. Servicios digitales

El Reglamento de Servicios Digitales (DSA) de 2022 es una de las dos grandes normas estructurales (la otra es el Reglamento de Mercados Digitales también de 2022) que modifican el marco de la UE para la regulación de las plataformas. Se

trata de un instrumento global que adopta un enfoque asimétrico, aumentando gradualmente las obligaciones a las que están sujetas las plataformas.

La Comisión Europea, en virtud del Reglamento DSA, puede definir las «plataformas en línea de muy gran tamaño» y los «motores de búsqueda en línea de muy gran tamaño», y someterles al nivel más alto de obligaciones. Esto incluye la evaluación de riesgos (art. 34), la mitigación de riesgos (art. 35) y el nuevo sistema de sanciones.

Con fecha 25 de abril de 2023, la Comisión Europea ha establecido la siguiente designación:

A) Plataformas en línea de muy gran tamaño (VLOP):
   1. Alibaba AliExpress.
   2. Amazon Store.
   3. Apple AppStore.
   4. Booking.com.
   5. Facebook.
   6. Google Play.
   7. Google Maps.
   8. Google Shopping.
   9. Instagram.
   10. LinkedIn.
   11. Pinterest.
   12. Snapchat.
   13. TikTok.
   14. Twitter.
   15. Wikipedia.
   16. YouTube.
   17. Zalando.

B) Motores de búsqueda en línea de muy gran tamaño (VLOSE):
   1. Bing.
   2. Google Search.

Estos actores estructurales del mundo digital «detectarán, analizarán y evaluarán con diligencia cualquier riesgo sistémico en la Unión que se derive del diseño o del funcionamiento de su servicio y los sistemas relacionados con este, incluidos los sistemas algorítmicos, o del uso que se haga de sus servicios» (art. 34.1 DSA). La evaluación del riesgo se realiza al menos una vez al año, y debe tener en cuenta

la gravedad y la probabilidad. El artículo 34 establece que deben tomarse en consideración los siguientes riesgos sistémicos:

- difusión de contenidos ilícitos;
- efectos negativos sobre el ejercicio de los derechos fundamentales;
- efectos negativos sobre el discurso cívico y los procesos electorales, así como sobre la seguridad pública;
- efectos negativos en relación con la violencia de género, la protección de la salud pública y de los menores y consecuencias negativas graves para el bienestar físico y mental de la persona.

Del mismo modo, al llevar a cabo las evaluaciones de riesgos, los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño tendrán en cuenta, en particular, si los siguientes factores influyen, y de qué manera, en cualquiera de los riesgos sistémicos precitados:

- el diseño de sus sistemas de recomendación y de cualquier otro sistema algorítmico pertinente;
- sus sistemas de moderación de contenidos;
- las condiciones generales aplicables y su ejecución;
- los sistemas de selección y presentación de anuncios;
- las prácticas relacionadas con los datos.

Al igual que la Directiva NIS2, el Reglamento DSA impone obligaciones especiales de gobernanza a la dirección de la empresa. Su artículo 41 obliga a los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño a establecer una función de cumplimiento, independiente de sus funciones operativas y compuesta por responsables de cumplimiento. Este *compliance officer* debe tener «autoridad, rango y recursos suficientes, así como acceso al órgano de dirección». Los órganos de dirección tienen obligaciones específicas a este respecto.

El Reglamento DSA es fundamental por dos razones. En primer lugar, impone requisitos estrictos a las plataformas más grandes, intentando crear un espacio más seguro para los usuarios y unas condiciones equitativas para las empresas. Esto significa que tanto las empresas como los usuarios pueden confiar más en las plataformas, ya que ahora éstas se ven obligadas a actuar de forma jurídicamente más responsable. Esto debería reducir el riesgo para todos ahora que un competidor de las grandes tecnológicas debe pagar una sanción si impone un coste adicional a otros agentes del mercado a través del comportamiento desleal o poco competitivo del competidor de las grandes tecnológicas (RIORDAN, 2016, p. 388). En segundo lugar, incluso en los casos en que el cumplimiento basado en el riesgo no es obligatorio en virtud de la propia norma (debido al bajo umbral), los mecanismos de identificación y mitigación de riesgos prescritos en el Reglamento son, *de*

facto, modelos de cumplimiento basado en el riesgo que las empresas más pequeñas deben adoptar.

3. Inteligencia artificial

El desarrollo y la aplicación de soluciones basadas en la IA en las empresas modernas se está extendiendo rápidamente. Los legisladores de la UE, entre los primeros a escala mundial, propusieron en abril de 2021 una norma jurídica autónoma sobre IA. El futuro Reglamento europeo de IA (RIA) adopta un enfoque basado en el riesgo al positivizar normas sobre la comercialización de productos y herramientas basados en IA, así como sobre el uso de sistemas de IA. La norma se aplica no sólo a los proveedores y usuarios de sistemas de IA ubicados en la UE, sino también a los productos y servicios cuyo resultado producido por el sistema se utilice en la Unión, lo que amplía considerablemente su ámbito de aplicación (FERNÁNDEZ HERNÁNDEZ, 2022, pp. 131-135).

El RIA prohíbe de plano determinadas tecnologías. Entre ellas, se encuentran los sistemas que despliegan técnicas subliminales para manipular a las personas, los que explotan vulnerabilidades de grupo y los sistemas que utilizan una puntuación social por parte de Estados no democráticos. Otros sistemas clasificados como de alto riesgo incluyen:

- identificación y categorización biométricas;
- gestión y funcionamiento de infraestructuras esenciales (como el tráfico rodado y el suministro de agua, gas, calefacción y electricidad);
- educación y formación profesional;
- empleo;
- acceso y disfrute de servicios públicos y privados esenciales, y sus beneficios; y
- Administración de justicia.

A diferencia del enfoque ascendente del RGPD, el RIA crea una lista descendente de obligaci ones que deben cumplirse.

El artículo 9 del RIA exige el establecimiento de un sistema de gestión basado en el riesgo. Se trata de un «proceso iterativo continuo que se llevará a cabo durante todo el ciclo de vida de un sistema de IA de alto riesgo, el cual requerirá actualizaciones sistemáticas periódicas», que incluye la identificación y estimación del riesgo y la adopción de medidas de gestión del riesgo. Este grupo de sistemas está sujeto a un amplio espectro de obligaciones que incluyen la supervisión humana, la transparencia, la ciberseguridad, la gestión de riesgos, la calidad de los datos, la supervisión pública y las obligaciones de información. El artículo 10 del RIA impone requisitos de gobernanza de datos para las técnicas que implican el entrenamiento de modelos con datos. Las sanciones son

elevadas: multas de hasta 30 millones de euros o el 6 % de los ingresos globales, lo que sea mayor.

Aunque el alcance de las obligaciones impuestas a los usuarios es algo más reducido que aquellas a las que están sujetos los productores de IA o quienes comercializan sistemas de IA, la gestión de riesgos que exige el artículo 9 del RIA es imposible sin la participación del usuario y sin una cooperación más estrecha del productor y la empresa usuaria.

4. Ciberseguridad

Los gobiernos y el sector privado necesitan proteger sus infraestructuras más que nunca. Los ciberataques son cada vez más frecuentes y cada vez más tienen como objetivo infraestructuras clave de la sociedad. Las tendencias actuales muestran que los ciberdelincuentes están motivados por la monetización, con el *ransomware* como principal amenaza y un aumento de los ciberataques perpetrados contra infraestructuras del sector público (BARRIO ANDRÉS, 2018; DELGADO MARTÍN, 2023, pp. 211-216).

Por eso, la nueva Directiva NIS2 de 2022 es una continuación de los esfuerzos de la primera Directiva NIS de 2016[7], que obligaba a determinados operadores de servicios esenciales y proveedores de servicios digitales a introducir obligaciones de seguridad y sistemas de notificación de incidentes de ciberseguridad. Fue un paso limitado pero significativo en la mejora de la ciberseguridad europea (ARTEAGA MARTÍN, 2021). La nueva Directiva NIS2 sigue las líneas maestras de su predecesora, pero exige una mejor formación y una efectiva notificación de incidentes, y, sobre todo, una mejora general de la ciberseguridad.

La Directiva NIS2 se aplica a las entidades esenciales e importantes (enumeradas en los anexos I y II) que realicen actividades en la Unión Europea y cumplan los requisitos de umbral para medianas empresas.[8] Independientemente del tamaño, la norma se aplica a las telecomunicaciones, a los proveedores exclusivos de servicios críticos y, en otras situaciones, a las Administraciones Públicas centrales y regionales. Los sectores de alta criticidad son la energía, el transporte, la banca, las infraestructuras de los mercados financieros, la sanidad, el agua potable, las aguas residuales, las infraestructuras digitales, la gestión de servicios TIC y la administración pública (anexo I). Otros sectores críticos son los servicios postales y de mensa-

7. Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

8. El número exacto de entidades incluidas no está cerrado en este momento, ya que los Estados miembros tienen un pequeño margen de discrecionalidad en algunos casos enumerados, pero también porque se incluye a los proveedores directos de la cadena de suministro.

jería, gestión de residuos, productos químicos, producción alimentaria, fabricación, proveedores de servicios digitales e investigación (anexo II).

El artículo 21 de la Directiva NIS2 obliga a las entidades a considerar el estado de la técnica y las normas comunitarias e internacionales para garantizar un nivel de seguridad de la red adecuado a los riesgos planteados. Hay que tener en cuenta la exposición al riesgo, el tamaño de la entidad y la probabilidad de que se produzca una incidencia. Se adopta el enfoque de «todos los peligros» (art. 21), que exige que se tenga en cuenta todo el alcance de las posibles emergencias o catástrofes a la hora de preparar y desarrollar las respuestas, lo que incluye:

- gestión de incidentes;
- continuidad de las actividades;
- seguridad de la cadena de suministro;
- seguridad de la red;
- gestión de riesgos;
- seguridad de los recursos humanos;
- criptografía; y
- autenticación multifactor (AMF).

Un aspecto único de la nueva directiva es la gestión de riesgos en la cadena de suministro. No sólo la empresa está obligada a evaluar los riesgos de sus propias operaciones, sino también los de sus proveedores directos o prestadores de servicios en la cadena de suministro. Deben tenerse en cuenta las vulnerabilidades específicas de cada proveedor directo, así como la «calidad general de los productos y las prácticas de ciberseguridad de sus proveedores y prestadores de servicios».

La supervisión pública nacional consiste en inspecciones *in situ*, controles aleatorios y auditorías de seguridad independientes. Pueden ordenarse auditorías *ad hoc* en caso de infracciones de ciberseguridad o incumplimiento, pero las autoridades nacionales también pueden imponer multas o suspender o inhabilitar a entidades o a sus directivos. Las multas para las entidades esenciales pueden ser de hasta 10 millones de euros o el 2 % del volumen de negocios mundial, el mayor de los dos, y de hasta 7 millones de euros o el 1,4 % del volumen de negocios mundial, el mayor de los dos, para las entidades importantes.

Como parte del nuevo interés de la UE por la gobernanza de los asuntos digitales, la Directiva NIS2 ordena a los Estados miembros de la UE que garanticen que los órganos de dirección de las empresas, como los consejos de administración, aprueben las medidas de gestión de riesgos de ciberseguridad adoptadas por esas entidades en materia de cumplimiento de riesgos, que supervisen su aplicación y que los órganos de dirección puedan ser considerados responsables de las infracciones.

Así pues, el abogado interno es responsable de las complejas evaluaciones de riesgos de las operaciones de su propia empresa, así como de las de sus proveedores

directos. La asunción de riesgos se sitúa en el nivel de dirección de la empresa y se reconocen como estándar las medidas a nivel de vanguardia. Aunque las importantes multas deberían servir de disuasión, a mi juicio la motivación principal debe ser que una sólida ciberseguridad es un elemento clave de la organización.

V. CONCLUSIONES

Las nuevas coordenadas del Derecho digital europeo suponen un señalado cambio de paradigma, que lleva aparejado una cierta complejidad. Los nuevos instrumentos normativos son bastante extensos, como también el potencial cuerpo de actos delegados de seguimiento y otro material interpretativo que está dictando la Comisión Europea.

Y lo que es más significativo, la interacción entre los instrumentos arroja dosis notables de inseguridad jurídica. Sus nuevas normas estructurales establecen que su aplicación es «sin perjuicio de» las reglas de otras normas de la UE. Pero esto sólo establece el orden en el que hay que buscar las respuestas. Si un asunto concreto está regulado, por ejemplo, en las directivas sobre derechos de autor, el Reglamento DSA no las deroga, pero sus numerosas normas sobre contenidos ilícitos, evaluación de riesgos, etc. cambian el panorama de forma significativa. La complejidad a nivel normativo se une a las incertidumbres del cumplimiento basado en el riesgo.

Asimismo, los nuevos Reglamentos europeos DSA, DMA y de IA, así como la nueva Directiva NIS2, han modificado la forma en que se aborda la propia regulación del riesgo y la relación entre el regulador y el regulado: si en el marco del RGPD el regulado es el responsable de lograr ese equilibrio, la decisión adoptada en estas últimas normas del Derecho digital europeo es trasladar progresivamente esa competencia del regulado al regulador. La razón de ser de este cambio radica en la necesidad de abandonar un enfoque liberal y abstencionista a otro más democrático, donde es el legislador quien toma las riendas de la regulación.

Por otra parte, resulta muy significativo que la nueva legislación digital europea basada en el riesgo ha aumentado la carga de cumplimiento para un amplio abanico de empresas y Administraciones Públicas. Es flexible en el sentido de que sólo hay que tomar medidas si el riesgo existe o si está por encima de un nivel determinable, pero la carga global es mayor que en el marco jurídico anterior a 2015. Se potencia así otra línea de trabajo para todos los operadores jurídicos del Derecho digital.

Ahora bien, a mi juicio no es cierto que más regulación signifique siempre menos innovación. Mirando al pasado, la economía digital apenas estaba regulada antes de 2018 en el Derecho de la Unión Europea (ese año entró en vigor el RGPD de 2016). La Directiva de comercio electrónico de 2000[9] —la predecesora del

9. 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).

Reglamento DSA— se asemeja mucho a la Sección 230 de la Ley de Decencia en las Comunicaciones de Estados Unidos de 1996 (la señalada CDA), protegiendo a las plataformas de cualquier obligación de supervisión general y estableciendo para ellas un generoso régimen de exclusión de responsabilidad. La única otra norma tecnológica notable de la UE en vigor antes de 2018 fue la Directiva de Protección de Datos de 1995[10], que era considerablemente bastante menos protectora de los derechos fundamentales que el nuevo RGPD de 2016.

Por lo tanto, aunque no existía en la UE una regulación tecnológica sustancial durante los años en que se fundaron empresas como Google y Facebook (1998 y 2004, respectivamente), no se fundaron empresas comparables en Europa. Del mismo modo, las *startups* europeas de IA van a la zaga de las estadounidenses y chinas, a pesar de que en la UE, a fecha de escribir estas líneas, no se ha aprobado el RIA. Por eso, no puede decirse que el Derecho digital europeo haya frenado el progreso tecnológico y el potencial innovador del sector digital. Al contrario, y gracias a la regulación *ex ante* del Derecho de las telecomunicaciones vigente desde varias décadas, Europa cuenta con una cobertura de fibra óptica y 5G inédita en otras regiones del mundo.

Por eso, la nueva regulación del Derecho digital europeo atiende al principio de proporcionalidad y es asimétrica. Ello se plasma en que el nuevo Reglamento DMA sólo se dirige a los mayores gigantes tecnológicos capaces de actuar como guardianes digitales[11], y el Reglamento DSA impone más exigencias reguladoras a las plataformas y motores de búsqueda de muy gran tamaño —los señalados VLOP y VLSE— que tienen el mayor potencial de causar daños, pero también más recursos para evitar que se produzcan.

VI. BIBLIOGRAFÍA

ARTEAGA MARTÍN, F., «La evaluación y la revisión de la Directiva NIS», en *ARI Real Instituto Elcano*, núm. 19, 2021.

BARRIO ANDRÉS, M., «El cumplimiento basado en el riesgo o risk-based compliance, pieza cardinal del nuevo Derecho digital europeo», en *ARI Real Instituto Elcano*, núm. 34/2023.

BARRIO ANDRÉS, M., «El nuevo Reglamento europeo de servicios digitales», en RECUERDA GIRELA, M. A. (dir.), *Anuario de Derecho Administrativo 2023*, Aranzadi, Pamplona, 2023.

BARRIO ANDRÉS, M., «Inteligencia artificial: origen, concepto, mito y realidad», en *El Cronista del Estado Social y Democrático de Derecho*, núm. 100, 2022.

10. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.

11. Los llamados *gatekeepers* o plataformas digitales que ejercen como guardianes de acceso.

BARRIO ANDRÉS, M., «La ciberseguridad en el Derecho digital europeo: novedades de la Directiva NIS2», en *Indret*, núm. 1, 2024.

BARRIO ANDRÉS, M., «La regulación del derecho a la protección de datos en los Estados Unidos», en *Cuadernos de Derecho transnacional*, vol. 14, núm. 2, 2022.

BARRIO ANDRÉS, M., *Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos*, Wolters Kluwer, Madrid, 2018.

BARRIO ANDRÉS, M., *Fundamentos del Derecho de Internet*, Centro de Estudios Políticos y Constitucionales, Madrid, 2020, 2.ª edición.

BARRIO ANDRÉS, M., *Internet de las Cosas*, Reus, Madrid, 2022, 2.ª edición.

BARRIO ANDRÉS, M., *Los derechos digitales y su regulación en España, la Unión Europea e Iberoamérica*, Colex, A Coruña, 2023.

BARRIO ANDRÉS, M., *Manual de Derecho digital*, Tirant lo Blanch, Valencia, 2022, 2.ª edición.

BOIX PALOP, A., «Digital Platform Competition Regulatory Challenges», en *Revista General de Derecho de los Sectores Regulados: RSR*, núm. 8, 2021.

BRADFORD, A., *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, Nueva York, 2020.

CAMPOS ACUÑA, C., *Guía práctica de compliance en el sector público*, Wolters Kluwer, Madrid, 2020.

DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, T., «La regulación como modalidad genérica de intervención pública. La regulación en la sociedad digital (Transformaciones en el derecho público y privado)», en *Cuadernos de Derecho transnacional*, vol. 15, núm. 2, 2023.

DELGADO MARTÍN, J., «La regulación de la ciberseguridad», en MONTERO PASCUAL, J. J. (coord.), *Digitalización y Derecho*, Tirant lo Blanch, Valencia, 2023.

DOMÍNGUEZ ÁLVAREZ, J. L., «Derecho a la seguridad digital: génesis, evolución y perspectivas de futuro», en RODRÍGUEZ AYUSO, J. F. (coord.), *Nuevos retos en materia de derechos digitales en un contexto de pandemia: perspectiva multidisciplinar*, Aranzadi, Pamplona, 2022.

FERNÁNDEZ HERNÁNDEZ, C., «La futura regulación europea de la inteligencia artificial: objetivos, principios y pautas», en GARCÍA MEXÍA, P. (dir.), *Claves de Inteligencia Artificial y Derecho*, Wolters Kluwer, Madrid, 2022.

LÓPEZ CALVO, J. (coord.)., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Editorial BOSCH, Madrid, 2019.

MONTERO PASCUAL, J. J., «Digitalización y Derecho», en MONTERO PASCUAL, J. J. (coord.), *Digitalización y Derecho*, Tirant lo Blanch, Valencia, 2023.

MUÑOZ VELA, J. M., «Hacia un equilibrio entre ética, protección de los derechos fundamentales, seguridad, confianza, innovación, desarrollo y competitividad», en *Revista LA LEY de Derecho Digital e Innovación*, núm. 14, 2022.

NEMITZ, P., «Constitutional democracy and technology in the age of artificial intelligence», en *Philosophical Transactions of the Royal Society*, vol. 376, núm. 2133, 2018.

ORTEGA JIMÉNEZ, A. (coord.), *Derecho internacional privado, contratación internacional en internet y régimen jurídico del comercio electrónico*, Aranzadi, Pamplona, 2022.

RIORDAN, J., *The Liability of Internet Intermediaries*, Oxford University Press, Oxford, 2016.

RODRÍGUEZ AYUSO, J. F., «Obligaciones *ex ante* para promover la disputabilidad y la equidad en mercados digitales relevantes: el nuevo régimen jurídico de los gatekeepers», en *Revista General de Derecho Administrativo*, núm. 64, 2023.

ROMERO JÍMENEZ, G., «La Carta de Derechos Digitales y el ejercicio práctico de la abogacía», en *Revista LA LEY de Derecho Digital e Innovación*, núm. 9, 2021.

VIDA FERNÁNDEZ, J., «La gobernanza de los riesgos digitales: desafíos y avances en la regulación de la inteligencia artificial», en *Cuadernos de Derecho transnacional*, vol. 14, núm. 1, 2022.