ARI 34/2023
20 de abril de 2023

El cumplimiento basado en el riesgo o *risk-based compliance*, pieza cardinal del nuevo Derecho digital europeo

Moisés Barrio Andrés | Letrado del Consejo de Estado, profesor de Derecho digital y 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 | @moisesbarrioa

Tema

Los reguladores del Derecho digital europeo han utilizado cada vez con más frecuencia la herramienta del riesgo para fomentar una mayor responsabilidad de los agentes públicos y privados. El enfoque de cumplimiento basado en el riesgo (*risk-based approach*) consiste en adaptar los derechos y obligaciones a los riesgos concretos derivados de una actividad específica.

Resumen

En el mundo digital, el cumplimiento normativo o *compliance* ha sido poco frecuente hasta fechas recientes, ya que las directivas y reglamentos no obligaban a las empresas a someterse a numerosas obligaciones. Sin embargo, la situación ha cambiado con la aprobación del nuevo Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Reglamento de Servicios Digitales o DSA por sus siglas inglesas) y la nueva Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI2 o NIS2). Este análisis expone las principales novedades en materia de cumplimiento normativo derivadas de los nuevos Reglamentos europeos DSA, DMA y de IA, así como la nueva Directiva NIS2, que han modificado de forma significativa la forma en que se aborda la propia regulación del riesgo y la relación entre el regulador y el regulado.

Análisis

Aunque la evaluación y gestión del riesgo siempre ha sido parte integrante de la toma de decisiones de los Estados y los sujetos privados, ha adquirido especial importancia en las políticas contemporáneas. Múltiples factores, como la transformación de las sociedades democráticas, la competencia de los mercados, el esfuerzo constante por innovar, la globalización y las tecnologías digitales, han incrementado los tipos y la diversidad de los riesgos, así como la magnitud potencial de sus efectos indeseables. Además, también ha aumentado la concienciación sobre los riesgos y, con ella, la lucha por prepararse, anticiparse y afrontarlos.

Por eso, los legisladores cada vez recurren más a un paradigma de la regulación basado en el riesgo como respuesta al desarrollo de lo que, tras la obra del profesor Beck publicada en 1986 primero en lengua alemana, se define como "sociedad del riesgo". Así, como advirtió este autor,[1] mientras que "la base de la sociedad de clases consiste en conflictos que propugnan por la supresión de la carencia, la sociedad del riesgo se define como la lucha por la supresión del riesgo, de la riqueza o de la igualdad; es decir, como consigna normativa del estado ideal de las cosas se hace un tránsito a la seguridad". En síntesis, se ha producido el cambio a una sociedad de minimización de males.

Este modelo normativo fue pronto adoptado, entre otros, por la UE, primero en ámbitos como el Derecho medioambiental, el sanitario, el financiero o el agroalimentario, y ahora también en el Derecho digital. Desde la publicación en 2015 de la Comunicación de la Comisión titulada *Una Estrategia para el Mercado Único Digital de Europa*,[2] los reguladores de la UE han utilizado cada vez con más frecuencia la herramienta del riesgo para fomentar una mayor responsabilidad de los agentes públicos y privados sobre los posibles efectos colaterales relacionados con el uso de las tecnologías digitales o el tratamiento de datos personales.

El enfoque basado en el riesgo o *risk-based approach* consiste en la promulgación de un marco normativo en el que los deberes y obligaciones se escalonan y adaptan a los riesgos concretos derivados de una actividad específica. Se supera así la lógica binaria de cumplimiento/incumplimiento en términos clásicos kelsenianos por una nueva forma de "cumplimiento 2.0" habitualmente denominada cumplimiento normativo o *compliance*.

Esta nueva forma impone a los sujetos obligados un modelo de organización y gestión[3] que incluya medidas de vigilancia y control idóneas para prevenir incumplimientos normativos, entre las que se engloban destacadamente un sistema de gestión de riesgos, un programa de conducta (o de prevención de riesgos corporativos: en inglés, *compliance programme*) y un responsable de cumplimiento normativo o *Compliance Officer*.

[1] "... en el fondo, aquí ya no se trata de alcanzar algo bueno sino sólo ya de evitar lo peor. El sueño de la sociedad de clases significa que todos quieren y deben participar en el pastel. El objetivo de la sociedad de riesgo es que todos han de ser protegidos del veneno". Véase Ulrich Beck (1998), *La sociedad del riesgo: hacia una nueva modernidad*, Editorial Paidós Ibérica.

[2] COM(2015) 192 final.

[3] Véase, por ejemplo, Concepción Campos Acuña (dir.) (2020), *Guía práctica de compliance en el sector público*, Editorial El Consultor de los Ayuntamientos; Dino Carlos Caro Coria (2020), *Derecho penal económico y de la empresa*, Editorial Gaceta Jurídica; Íñigo Gómez Berruezo (2021); y Stewart Room (ed.) (2022), *Data protection and compliance*, Editorial BCS, 2.ª edición.

El “compliance” en el nuevo Derecho digital europeo

En el mundo digital, el *compliance* como fenómeno ha sido poco frecuente hasta fechas recientes, ya que las directivas y reglamentos no obligaban a las empresas a someterse a numerosas normas. La carga regulatoria[4] ha sido mínima, como ocurre con el marco general que introdujo la 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, o DCE).

Ciertamente, el *compliance* siempre ha tenido innegable importancia, especialmente en grandes corporaciones del mundo digital, pero con la oleada de regulación del Derecho digital europeo posterior a 2015 se ha instaurado una nueva forma de cumplimiento, el cumplimiento basado en el riesgo o *risk-based compliance*.

En efecto, el cumplimiento basado en el riesgo se consagró de forma rudimentaria en el propio Reglamento europeo de Protección de Datos,[5] el RGPD. Concretamente, su art. 35 exige[6] a los responsables del tratamiento que realicen un examen del riesgo a través de la previa evaluación de impacto relativa a la protección de datos “cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas”.

A partir de entonces, el cumplimiento basado en el riesgo se ha convertido en un método regulador dominante en los instrumentos normativo más recientes del Derecho digital europeo,[7] tanto para las directivas marco como para los reglamentos sectoriales.

El nuevo Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales o DSA por sus siglas inglesas) introduce el cumplimiento basado en el riesgo para plataformas muy grandes y motores de búsqueda. El art. 34 del Reglamento DSA obliga a los prestadores de plataformas en línea de muy gran tamaño (VLOP por sus siglas en inglés) y los motores de búsqueda en línea de muy gran tamaño (VLSE) a detectar, analizar y evaluar con diligencia “cualquier riesgo sistémico en la Unión que se derive del diseño o del funcionamiento de su servicio y los sistemas relacionados con este, incluidos los sistemas algorítmicos, o del uso que se haga de sus servicios”. Las plataformas designadas por la Comisión están obligadas a realizar una evaluación de riesgos que, como mínimo, debe incluir el riesgo de:

[4] Lo he analizado *in extenso* en Moisés Barrio Andrés (2020), *Fundamentos del Derecho de Internet*, Editorial Centro de Estudios Políticos y Constitucionales, 2.ª edición, cap. V.

[5] 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).

[6] Véase José López Calvo (coord.) (2019), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Editorial Wolters Kluwer, en especial su cap. 19.

[7] Véase Moisés Barrio Andrés (2022), *Manual de Derecho digital*, Editorial Tirant lo Blanch, 2.ª edición.

- difusión de contenidos ilícitos;
- cualquier efecto negativo sobre los derechos fundamentales (enumerados específicamente en el precepto);
- cualquier efecto negativo sobre el discurso cívico y los procesos electorales y la seguridad pública; y
- cualquier efecto negativo sobre la violencia de género, la protección de la salud pública y de los menores y las consecuencias negativas graves para el bienestar físico y mental de la persona.

Al realizar la evaluación de riesgos, estos sujetos deben tener en cuenta (art. 34.2 Reglamento DSA):

- el diseño de sus sistemas de recomendación y de cualquier otro sistema algorítmico pertinente;
- sus sistemas de moderación de contenidos;
- los términos y condiciones aplicables y su ejecución;
- los sistemas de selección y presentación de anuncios;
- las prácticas del prestador en relación con los datos; y
- la manipulación intencionada del servicio.

A la identificación del riesgo le sigue la obligación de mitigarlo (art. 35). Las medidas de reducción de riesgos incluyen medidas específicas como:

- adaptar el diseño, las características o el funcionamiento de sus servicios;
- adaptar los términos y condiciones;
- adaptar los procesos de moderación de contenidos;
- probar y adaptar los sistemas de inteligencia artificial;
- probar y adaptar los sistemas de publicidad; y
- reforzar los procesos internos, los recursos, la realización de pruebas, la documentación o la supervisión de cualquiera de sus actividades.

De conformidad con el art. 36, la Comisión podrá poner en marcha un mecanismo de respuesta a las crisis que requiera acciones específicas.

Asimismo, los prestadores de plataformas en línea de muy gran tamaño (VLOP) y los motores de búsqueda en línea de muy gran tamaño (VLSE) están sometidos a auditorías independientes, como mínimo cada año (art. 37). El art. 41 del Reglamento DSA les impone además una función especial de comprobación del cumplimiento (art. 41), que sea independiente de la operativa, que dependa directamente del órgano de dirección y se encargue directamente de supervisar los riesgos. Existe una función similar en el nuevo Reglamento de Mercados Digitales[8] (art. 28).

[8] Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales o DMA).

El cumplimiento basado en el riesgo también se incorpora a los instrumentos sectoriales.

La nueva 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 SRI2 o NIS2), por ejemplo, se basa en la gestión del riesgo de ciberseguridad y las obligaciones de información (arts. 20 a 25).

Su art. 20 encomienda a los Estados miembros garantizar el cumplimiento basado en el riesgo. En virtud del art. 21, las medidas de gestión de riesgos son técnicas, operativas y organizativas, y tienen por objeto gestionar el riesgo, así como prevenir y minimizar su impacto. A la hora de tomar en consideración los distintos factores, siempre se tendrá en cuenta el estado de la técnica y, en su caso, las normas europeas e internacionales y los costes de aplicación. Las medidas adoptadas deben ser siempre proporcionales al riesgo en relación con la exposición, el tamaño, la probabilidad y el impacto. En cuanto a las obligaciones, el apartado 2 del art. 21 adopta el enfoque de "todos los peligros", exigiendo que las medidas incluyan como mínimo el análisis de riesgos, la gestión de incidentes, la continuidad y la seguridad de la cadena de suministro, entre otras. La gestión del riesgo en la cadena de suministro es especialmente interesante en este caso, ya que significa que las entidades deben gestionar a terceros (proveedores directos y vendedores).

El futuro Reglamento europeo regulador de determinados usos de la IA[9] también se basa en el cumplimiento basado en el riesgo, aunque de forma diferente a las normas anteriores. Mientras que éstas dejan la evaluación del riesgo y las medidas de mitigación a los sujetos obligados, el Reglamento de IA las impone directamente.[10] Este reglamento opera con cuatro categorías: riesgo inaceptable; riesgo elevado; riesgo limitado; y riesgo mínimo.

Los sistemas pertenecientes al primer grupo (por ejemplo, los de reconocimiento biométrico a distancia en tiempo real en espacios de acceso público) están prohibidos por el art. 5 de la propuesta. El segundo grupo, que incluye una lista de sistemas de IA identificados por el anexo III, modificable por la Comisión (arts. 6-7), se enfrenta a una larga lista de requisitos de calidad y transparencia, mientras que los proveedores y usuarios de esos sistemas deben cumplir obligaciones y deberes de control (arts. 8 y siguientes). Por último, mientras que los sistemas de riesgo limitado (como los *chatbots*) deben limitarse a cumplir los requisitos de transparencia previstos en el art. 52, el resto de los sistemas, considerados de riesgo mínimo, no están regulados en absoluto (aunque se fomenta la adopción de códigos de conducta).

[9] Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21 de abril de 2021, 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)0206).

[10] Sobre ello, véanse Carlos Fernández Hernández (2022), "La futura regulación europea de la inteligencia artificial: objetivos, principios y pautas", en Pablo García Mexía (dir.), *Claves de Inteligencia Artificial y Derecho*, Editorial Wolters Kluwer; y José Manuel Muñoz Vela (2022), *Retos, riesgos, responsabilidad y regulación de la inteligencia artificial*, Editorial Aranzadi.

Conclusión

La nueva regulación del Derecho digital europeo pretende lograr un equilibrio entre los diversos intereses en presencia: por un lado, el interés orientado a la economía hacia la innovación y la creación de un mercado único digital competitivo a escala internacional; por otro, el interés tuitivo de los valores democráticos y los derechos y libertades de las personas. El riesgo, en otras palabras, funciona como presupuesto de una nueva modalidad regulatoria, la del equilibrio de intereses y valores, que es intrínsecamente constitucional por su propia naturaleza.

Ahora bien, los 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 de la Unión 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.

En fin, resulta muy significativo que la nueva legislación basada en el riesgo ha aumentado la carga de cumplimiento para un amplio abanico de empresas. 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.