Responsabilidad de intermediarios en entornos digitales

Derecho comparado. Australia, Brasil, España, Francia y la Unión Europea

Autora

Daniela Santana Silva
Email: dasantana@bcn.cl

Nº SUP: 1535400

Resumen

El presente informe examina modelos regulatorios aplicables a plataformas digitales, intermediarios en línea y servicios de redes sociales, considerando especialmente las tendencias recientes en materia de moderación de contenidos, obligaciones de diligencia, transparencia y supervisión administrativa. Para ello, se analizan experiencias regulatorias de la Unión Europea, Francia, España, Australia y Brasil, identificando sus principales características normativas e institucionales.

En este contexto, se revisa el Reglamento de Servicios Digitales de la Unión Europea (*Digital Services Act* - DSA) que establece obligaciones diferenciadas según el tipo y tamaño del prestador, mecanismos de notificación y retiro de contenidos ilícitos, deberes de transparencia algorítmica y sistemas reforzados de supervisión para plataformas de muy gran tamaño.

Asimismo, el informe da cuenta de cómo Francia y España han desarrollado institucionalidades nacionales destinadas a la implementación y supervisión del DSA, mediante autoridades competentes encargadas de fiscalización, coordinación y supervisión. En Francia destacan las funciones atribuidas a la Autoridad Reguladora de la Comunicación Audiovisual y Digital (ARCOM), mientras que en España la aplicación del Reglamento se articula mediante la Comisión Nacional de Mercados y Competencia (CNMC), pese a que la falta de normativa interna llevara al país ante el Tribunal de Justicia de la Unión Europea.

Por otra parte, Australia presenta un modelo centrado en la seguridad en línea, basado en facultades administrativas de remoción de contenidos, mecanismos regulatorios aplicables a servicios electrónicos y redes sociales, y categorías específicas de contenidos dañinos regulados por la *Online Safety Act*. Brasil, por su parte, mantiene un modelo en que la judicatura determina la responsabilidad de intermediarios y remoción de contenidos, especialmente a partir de las reglas contempladas en el Marco Civil de Internet.

En términos generales, las jurisdicciones analizadas se asemejan en su tendencia hacia el establecimiento de obligaciones de diligencia, mecanismos de remoción de contenidos y facultades de supervisión sobre plataformas digitales. Sin embargo, difieren en la intensidad de la intervención regulatoria, el rol de las autoridades administrativas y judiciales, y el alcance de las obligaciones de transparencia y responsabilidad impuestas a los prestadores de servicios digitales.

Introducción

A solicitud parlamentaria el presente informe tiene por objeto analizar la implementación del Reglamento de Servicios Digitales de la Unión Europea, con especial atención a su operatividad y su estructura normativa. Para ello, se examinan las principales categorías regulatorias contempladas en el modelo europeo y las implicancias jurídicas derivadas de dicha diferenciación funcional entre prestadores de servicios digitales.

Asimismo, el informe aborda las jurisdicciones de Francia, España, Australia y Brasil, definidas por el solicitante, en torno a los siguientes criterios: (i) marco normativo general; (ii) tipos de prestadores regulados; (iii) régimen de responsabilidad; (iv) regulación de contenidos y procedimientos de notificación; (v) debido proceso del usuario; (vi) transparencia algorítmica y sistemas de recomendación; y, (vii) autoridades y supervisión. Además, al final del informe se incorpora un anexo, que contiene una tabla que permite identificar semejanzas y diferencias en materia de responsabilidad de intermediarios, regulación de contenidos, supervisión administrativa y protección de usuarios en entornos digitales.

El tema abordado y los contenidos del presente informe se encuentran delimitados por los parámetros propios de la Asesoría Técnica Parlamentaria, por el plazo de entrega convenido y por la información normativa y doctrinaria disponible. No constituye un documento académico y se enmarca en criterios de neutralidad, pertinencia, síntesis y oportunidad en su elaboración. Lo destacado y las traducciones son propias.

I. Modelos de responsabilidad de intermediarios y regulación de contenidos digitales

La regulación comparada de los intermediarios digitales muestra una transición desde modelos centrados en la responsabilidad posterior por contenidos de terceros, hacia esquemas que imponen obligaciones preventivas, procedimentales y de transparencia a distintos tipos de prestadores de servicios en línea. Esta evolución se explica por el rol que cumplen las plataformas digitales en la circulación de información, en la organización del acceso a contenidos y en la amplificación de riesgos asociados a contenidos ilícitos, dañinos o inadecuados para ciertos grupos de usuarios.

Para efectos de este análisis, resulta relevante distinguir entre prestadores de infraestructura o mera transmisión, servicios de alojamiento o almacenamiento de contenidos, plataformas en línea, motores de búsqueda, redes sociales, tiendas de aplicaciones y grandes plataformas con capacidad de incidir estructuralmente en el entorno digital. La distinción no es solo conceptual, pues determina el nivel de responsabilidad, las obligaciones de diligencia, los mecanismos de notificación y retiro, el grado de supervisión estatal y los deberes de transparencia exigibles a cada tipo de actor.

En ese marco, la Unión Europea representa un modelo de regulación horizontal de intermediarios digitales, especialmente a través del Reglamento de Servicios Digitales, que clasifica los servicios según su función y escala. España y Francia deben ser entendidas como casos de implementación nacional de ese marco europeo, aunque con diferencias institucionales relevantes.

Brasil, en cambio, mantiene un modelo centrado en la libertad de expresión, la neutralidad de red y la responsabilidad condicionada a orden judicial. Australia, por su parte, adopta un enfoque de seguridad

en línea, basado en un regulador especializado, códigos y estándares sectoriales, gestión de riesgos y facultades administrativas de remoción o restricción de acceso.

A. Unión Europea

1. Marco normativo general

La Unión Europea (UE) regula la responsabilidad de intermediarios y la moderación de contenidos digitales principalmente a través del Reglamento de Servicios Digitales (DSA por sus siglas en inglés - *Digital Services Act*), que establece un marco horizontal aplicable a los servicios intermediarios ofrecidos en la Unión Europea, con independencia del lugar de establecimiento del prestador cuando exista una conexión sustancial con el mercado europeo (DSA, artículos 2 y 3).

El modelo europeo reconoce que los servicios intermediarios cumplen funciones distintas en la circulación de información en línea y, por tanto, no deben ser sometidos a un régimen uniforme de debida diligencia (DSA, considerando 41).

La regulación distingue entre servicios de mera transmisión, servicios de memoria caché, servicios de alojamiento de datos, plataformas en línea, motores de búsqueda en línea, plataformas en línea de muy gran tamaño y motores de búsqueda en línea de muy gran tamaño (DSA, artículo 3).

Esta clasificación determina qué obligaciones debe cumplir cada prestador y permite graduar la carga regulatoria según la función técnica, el tamaño del servicio y los riesgos asociados a su operación, de acuerdo con lo dispuesto en el capítulo III de DSA,

El mencionado Reglamento de la UE debe leerse junto con el Reglamento de Mercados Digitales (DMA por sus siglas en inglés – *Digital Markets Act*), que regula a los denominados "guardianes de acceso"[1] o *gatekeepers*. Mientras el DSA se orienta a crear un entorno digital seguro, predecible y transparente respecto de contenidos, servicios intermediarios y derechos de usuarios, el DMA se dirige a garantizar mercados digitales disputables y equitativos frente a empresas que controlan servicios básicos de plataforma (DSA, artículo 1; DMA, artículo 1).

Por ello, para efectos de un análisis de responsabilidad de intermediarios y regulación de contenidos, el DSA constituye la norma central, mientras que el DMA sirve para explicar la noción de *gatekeeper* y la dimensión económica del poder de ciertas plataformas digitales (DSA, artículo 1; DMA, artículos 1 y 3).

2. Tipos de prestadores regulados

El DSA define los servicios intermediarios en el artículo 3.g):

> uno de los siguientes servicios de la sociedad de la información:

[1] Se definen en el artículo 2. 1 del DMA como "una empresa prestadora de servicios básicos de plataforma, designada de conformidad con el artículo 3".

> i) un **servicio de "mera transmisión"**, consistente en transmitir, en una red de comunicaciones, información facilitada por el destinatario del servicio o en facilitar acceso a una red de comunicaciones,
>
> ii) un **servicio de "memoria caché",** consistente en transmitir por una red de comunicaciones información facilitada por el destinatario del servicio, que conlleve el almacenamiento automático, provisional y temporal de esta información, prestado con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio, a petición de estos,
>
> iii) un **servicio de "alojamiento de datos",** consistente en almacenar datos facilitados por el destinatario del servicio y a petición de este[.]

Dentro de los **servicios de alojamiento**, el Reglamento distingue a las plataformas en línea[2], que no solo almacenan información facilitada por usuarios, sino que además la difunden al público a petición de estos (DSA, artículo 3.i).

La noción de **plataforma en línea** excluye aquellos casos en que la difusión pública sea una característica menor o accesoria de otro servicio principal, lo que permite diferenciar entre infraestructura técnica y servicios cuyo objeto consiste en organizar y poner contenidos a disposición del público (DSA, artículo 3.i).

El Reglamento crea además la categoría de **plataformas en línea de muy gran tamaño**, aplicable a aquellas que alcanzan un promedio mensual de destinatarios activos en la Unión igual o superior a cuarenta y cinco millones de personas (DSA, artículo 33).

También se establece la categoría de **motores de búsqueda en línea de muy gran tamaño**, sujetos a obligaciones reforzadas cuando alcanzan el mismo umbral de destinatarios activos mensuales en la Unión (DSA, artículo 33).

El Reglamento contempla de manera diferenciada las obligaciones que se aplican a todos los servicios intermediarios (capítulo II), y aquellas que recaen sobre servicios de alojamiento, plataformas en línea y, especialmente, plataformas o motores de muy gran tamaño (capítulo III).

3. Régimen de responsabilidad

Las obligaciones contenidas en el DSA se adaptan a "la función, el tamaño y el impacto de cada servicio en línea en el ecosistema en línea" (Comisión Europea, 2026). Las micro y pequeñas empresas tienen requisitos de acuerdo con su tamaño, para mantenerlos responsables mientras crecen, mientras que las plataformas más grandes tienen más responsabilidades y, por lo tanto, obligaciones (Comisión Europea, 2026).

[2] El reglamento define "plataforma en línea" en el artículo 3.i) como "un servicio de alojamiento de datos que, a petición de un destinatario del servicio, almacena y difunde información al público, salvo que esa actividad sea una característica menor y puramente auxiliar de otro servicio o una funcionalidad menor del servicio principal y que no pueda utilizarse sin ese otro servicio por razones objetivas y técnicas, y que la integración de la característica o funcionalidad en el otro servicio no sea un medio para eludir la aplicabilidad del presente Reglamento".

Los **servicios de mera transmisión** no son responsables por la información transmitida o a la que dan acceso cuando: (i) no originan la transmisión, (ii) no seleccionan al destinatario y (iii) no seleccionan ni modifican la información transmitida (DSA, artículo 4).

Los **servicios de memoria caché** no son responsables por el almacenamiento automático, intermedio y temporal de información cuando: (i) no modifiquen la información, (ii) cumplan las condiciones de acceso, (iii) respeten las normas de actualización, (iv) no interfieran en tecnologías lícitas de obtención de datos y (v) actúen con prontitud para retirar o bloquear el acceso cuando corresponda (DSA, artículo 5).

Los **servicios de alojamiento** no son responsables por la información almacenada a petición de un destinatario cuando: (i) no tengan conocimiento efectivo de una actividad o contenido ilícito o, (ii) al obtenerlo, actúen con prontitud para retirar o bloquear el acceso a dicha información (DSA, artículo 6).

El DSA también incorpora una cláusula donde consta que la realización voluntaria y de buena fe de investigaciones propias o medidas para detectar, identificar o retirar contenidos ilícitos no priva automáticamente al prestador de las exenciones de responsabilidad (DSA, artículo 7).

El Reglamento contempla la prohibición de imponer obligaciones generales de supervisión o búsqueda activa de hechos o circunstancias que indiquen actividades ilícitas (DSA, artículo 8).

4. Regulación de contenidos y procedimientos de notificación

Los artículos 9 y 10 del DSA establecen mecanismos de cooperación entre autoridades y prestadores de servicios intermediarios respecto de contenidos ilícitos y acceso a información de usuarios. En ambos casos, cuando una autoridad judicial o administrativa competente emite una orden basada en el derecho de la Unión Europea o en normativa nacional compatible con este, los intermediarios deben informar sin dilación indebida las medidas adoptadas para dar cumplimiento a dicha orden, indicando si esta fue ejecutada y cuándo ocurrió (DSA, arts. 9.1 y 10.1).

Las **órdenes de actuación contra contenidos ilícitos** deben contener una referencia al fundamento jurídico que puede ser derecho comunitario europeo o derecho nacional. Además, debe contener: motivación, identificación de la autoridad emisora, indicación del contenido afectado, ubicación exacta del contenido y vías de recurso disponibles para el prestador y el destinatario del servicio (DSA, artículo 9.2.a).

Las **órdenes de entrega de información** deben estar suficientemente fundadas, identificar claramente la información requerida y respetar las garantías previstas por el Reglamento y el derecho aplicable (DSA, artículo 10).

Además, entre las obligaciones de debida diligencia el Reglamento dispone que los **prestadores de servicios intermediarios** deben establecer puntos únicos de contacto que permitan una comunicación directa y eficiente con las autoridades de los Estados miembros, la Comisión Europea y la Junta Europea de Servicios Digitales (DSA, artículo 11).

Los prestadores que no estén establecidos en la UE, pero que ofrezcan servicios en ella, deben designar un representante legal en un Estado miembro donde ofrezcan sus servicios (DSA, artículo 13).

Los **prestadores de servicios de alojamiento** deben establecer mecanismos de notificación y acción que permitan a cualquier persona o entidad notificar la presencia de contenidos que considere ilícitos (DSA, artículo 16). Estos mecanismos deben ser de fácil acceso, uso sencillo y permitir notificaciones[3] "suficientemente precisas y adecuadamente fundamentadas" para que el prestador pueda adoptar una decisión informada y diligente (DSA, artículo 16).

Cuando el prestador decida retirar, bloquear, limitar la visibilidad, desmonetizar, suspender o cerrar una cuenta o contenido por considerarlo ilegal o incompatible a sus condiciones, debe entregar una declaración de motivos al destinatario afectado (DSA, artículo 17).

Esta declaración debe explicar si la decisión se refiere a la retirada, bloqueo, degradación, restricción de visibilidad, suspensión o terminación del servicio, e indicar los hechos y circunstancias en que se basa la decisión (DSA, artículo 17.3). También debe indicar si se utilizaron medios automatizados para adoptar la decisión, el fundamento jurídico o contractual invocado y las vías de recurso disponibles para el usuario (DSA, artículo 17.3).

5. Debido proceso del usuario

El Reglamento establece que los **prestadores de servicios intermediarios** deben informar de manera clara las restricciones que pueden imponerse al uso del servicio, incluidas políticas, procedimientos, medidas y herramientas de moderación, así como el uso de toma de decisiones algorítmica y revisión humana (DSA, artículo 14.1).

Los prestadores deben aplicar sus condiciones generales de forma diligente, objetiva, proporcionada y teniendo debidamente en cuenta los derechos fundamentales de los destinatarios del servicio (DSA, artículo 14.4).

Los **prestadores de plataformas en línea** deben establecer sistemas internos de gestión de reclamaciones contra decisiones de moderación, suspensión, bloqueo, restricción de visibilidad, retirada de contenidos o suspensión de cuentas (DSA, artículo 20).

Estos sistemas deben ser gratuitos y permitir que los destinatarios impugnen por vía electrónica las decisiones durante al menos seis meses desde que fueron informados de ellas (DSA, artículo 20).

Las decisiones adoptadas en el marco del sistema interno de reclamaciones no pueden basarse exclusivamente en medios automatizados, lo que introduce un estándar mínimo de revisión humana (DSA, artículo 20).

El Reglamento también reconoce el derecho de los usuarios a acudir a órganos certificados de resolución extrajudicial de litigios para impugnar decisiones de plataformas en línea (DSA, artículo 21). La resolución extrajudicial no priva a los usuarios del derecho a recurrir ante los tribunales nacionales, preservando el derecho a tutela judicial efectiva (DSA, artículo 21).

[3] El artículo 16.3 del DSA dispone "Se considerará que las notificaciones a que se refiere el presente artículo proporcionan un conocimiento efectivo o permiten ser consciente (…) del elemento de información concreto de que se trate, cuando permitan a un prestador diligente de servicios de alojamiento de datos determinar, sin un examen jurídico detallado, que la información o la actividad pertinentes son ilícitas".

El DSA regula además a los alertadores fiables[4], cuyas notificaciones deben recibir tratamiento prioritario por las plataformas en línea, siempre que dichas entidades hayan sido certificadas por el Coordinador de Servicios Digitales competente (DSA, artículo 22).

Este mecanismo busca aumentar la eficacia del retiro de contenidos ilícitos, pero también introduce exigencias de competencia, independencia y objetividad para quienes reciben esa condición (DSA, artículo 22).

6. Transparencia algorítmica y sistemas de recomendación

La regulación europea reconoce que las plataformas no solo alojan contenidos, sino que también organizan su circulación mediante sistemas de recomendación, clasificación, priorización y personalización (DSA, considerando 70).

Las **plataformas en línea** que utilicen sistemas de recomendación deben establecer en sus condiciones generales, de forma clara y comprensible, los principales parámetros utilizados por dichos sistemas y las opciones disponibles para que los usuarios puedan modificarlos o influir en ellos (DSA, artículo 27.1). El Reglamento dispone en el párrafo 2 del artículo 27 que:

> Los parámetros principales (…) explicarán por qué se sugiere determinada información al destinatario del servicio. Estos parámetros incluirán, como mínimo:
>
> a) los criterios más significativos a la hora de determinar la información sugerida al destinatario del servicio, y
>
> b) las razones de la importancia relativa de dichos parámetros

Cuando existan varias opciones de sistemas de recomendación, la plataforma debe permitir a los usuarios seleccionar y modificar en cualquier momento la opción preferida de manera fácil y accesible (DSA, artículo 27.3).

Las **plataformas en línea de muy gran tamaño** y los **motores de búsqueda de muy gran tamaño** deben ofrecer “al menos una opción para cada uno de sus sistemas de recomendación que no se base en la elaboración de perfiles”, conforme a la normativa de protección de datos[5] (DSA, artículo 38).

Asimismo, deben evaluar riesgos sistémicos derivados del diseño, funcionamiento y uso de sus servicios, incluyendo la difusión de contenidos ilícitos, afectaciones a derechos fundamentales, violencia de género, salud pública, procesos electorales, discurso cívico y protección de menores (DSA, artículo 34.1).

---

[4] De acuerdo con lo dispuesto en el número 2 del artículo 22 del DSA, “2. La condición de «alertador fiable» en virtud del presente Reglamento será otorgada, previa solicitud de cualquier entidad que lo desee, por el coordinador de servicios digitales del Estado miembro donde el solicitante esté establecido, a un solicitante que haya demostrado que cumple todas las condiciones siguientes:
a) poseer conocimientos y competencias específicos para detectar, identificar y notificar contenidos ilícitos;
b) no depender de ningún prestador de plataformas en línea;
c) realizar sus actividades con el fin de enviar notificaciones de manera diligente, precisa y objetiva.”

[5] Reglamento de la UE 2016/679, artículo 4.4.

Estas entidades deben adoptar medidas de mitigación “razonables, proporcionadas y efectivas” frente a los riesgos sistémicos detectados, incluyendo adaptaciones de diseño, sistemas de moderación, condiciones generales, sistemas algorítmicos y publicidad (DSA, artículo 35.1).

El DSA también exige auditorías independientes para **plataformas y motores de búsqueda de muy gran tamaño**, con el fin de evaluar el cumplimiento de las obligaciones reforzadas (DSA, artículo 37). Además, estas entidades deben proporcionar acceso a datos a la Comisión Europea y a los Coordinadores de Servicios Digitales para supervisar y evaluar el cumplimiento del Reglamento (DSA, artículo 40).

7. Autoridad y supervisión

El DSA exige que cada Estado miembro designe al menos una autoridad competente para supervisar la aplicación del Reglamento, debiendo designar además un Coordinador de Servicios Digitales responsable de todas las materias relacionadas con la supervisión y ejecución del Reglamento en ese Estado (DSA, artículo 49.2).

Los Coordinadores de Servicios Digitales deben actuar con imparcialidad, transparencia y oportunidad, sin solicitar ni aceptar instrucciones de otras autoridades públicas o privadas (DSA, artículo 50).

Estas autoridades cuentan con facultades de investigación, incluyendo requerir información, realizar inspecciones y solicitar explicaciones a prestadores de servicios intermediarios (DSA, artículo 51). También pueden ordenar el cese de infracciones, imponer medidas correctivas y aplicar sanciones pecuniarias conforme al régimen nacional establecido en cumplimiento del Reglamento (DSA, artículos 51 y 52).

Las sanciones por incumplimiento del DSA pueden alcanzar hasta el 6% del volumen de negocios anual mundial del prestador infractor, según la naturaleza de la infracción y el régimen establecido por cada Estado miembro (DSA, artículo 52).

La Comisión Europea conserva competencias directas respecto de **plataformas en línea de muy gran tamaño** y **motores de búsqueda en línea de muy gran tamaño** en materia de supervisión (DSA artículo 56.2 y 56.3).

B. España

1. Marco normativo general

España regula la responsabilidad de intermediarios digitales mediante una combinación de normas internas previas al DSA y la aplicación directa del Reglamento Europeo de Servicios Digitales (Ley 34/2002, artículo 1; DSA, artículo 2).

El Reglamento (UE) 2022/2065 sobre Servicios Digitales (DSA) resulta directamente aplicable en España por tratarse de un reglamento europeo, conforme al artículo 288 del Tratado de Funcionamiento de la Unión Europea, que establece que los reglamentos son obligatorios en todos sus elementos y directamente aplicables en cada Estado miembro (TFUE, artículo 288).

En consecuencia, las obligaciones contenidas en el DSA son exigibles en España aun cuando no exista una ley nacional de transposición[6].

Sin embargo, el propio DSA reserva ciertas materias a los Estados miembros, especialmente la designación del Coordinador de Servicios Digitales, la definición de autoridades competentes, los procedimientos sancionatorios y las reglas nacionales de fiscalización y cooperación administrativa (DSA, artículos 49 a 51).

Así, en España resulta aplicable la Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico (LSSI), que incorporó al ordenamiento jurídico interno la Directiva 2000/31/CE y constituye la base del régimen aplicable a los prestadores de servicios intermediarios (Ley 34/2002, exposición de motivos y artículo 1).

La Ley 34/2002 regula el régimen jurídico de los servicios de la sociedad de la información, las obligaciones de los prestadores, los servicios de intermediación, las comunicaciones comerciales, la contratación electrónica, la solución de conflictos, la supervisión y el régimen sancionador (Ley 34/2002, artículo 1).

En materia audiovisual, España cuenta además con la Ley 13/2022, General de Comunicación Audiovisual, que regula los servicios de comunicación audiovisual y los servicios de intercambio de vídeos a través de plataforma (Ley 13/2022, artículo 1).

Por último, también es relevante la Ley 13/2022 porque incorpora al derecho español la regulación europea sobre servicios de intercambio de vídeos a través de plataforma[7], especialmente respecto de contenidos generados por usuarios, protección de menores, incitación al odio, publicidad y obligaciones de transparencia (Ley 13/2022, artículos 2.13)

2. Implementación del Reglamento DSA en España

En diciembre de 2024, España adoptó el Real Decreto ley 9/2024 que modificó la Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI) y la Ley 3/2013 que crea la Comisión Nacional de los Mercados y la Competencia (CNMC). Este Real Decreto fue derogado el 22 de enero de 2025 por Resolución del Congreso de los Diputados.

La reforma tenía como eje central designar a la CNMC como Coordinador de Servicios Digitales, conforme a las exigencias del artículo 49 del DSA.

[6] El Reglamento es directamente aplicable en todos los Estados miembros de la UE. Esto significa que: (i) se aplica de manera inmediata como norma en todos los Estados miembros de la UE, sin necesidad de ser transpuesto al Derecho nacional; (ii) atribuye derechos y obligaciones a los particulares y, por tanto, puede ser invocado directamente ante los tribunales nacionales; y, (iii) los particulares pueden utilizarlos como referencia en sus relaciones con otros particulares, con los Estados miembros de la UE o con las autoridades de la UE (EUR-lex, s.f.)

[7] Definidos en la ley como "[s]ervicio cuya finalidad principal propia o de una de sus partes disociables o cuya funcionalidad esencial consiste en proporcionar, al público en general, a través de redes de comunicaciones electrónicas, programas, vídeos generados por usuarios o ambas cosas, sobre los que no tiene responsabilidad editorial el prestador de la plataforma, con objeto de informar, entretener o educar, así como emitir comunicaciones comerciales, y cuya organización determina el prestador, entre otros medios, con algoritmos automáticos, en particular mediante la presentación, el etiquetado y la secuenciación" (artículo 2.13).

En enero de 2024 el Ministerio para la Transformación Digital anunció oficialmente dicha designación, señalando que la CNMC sería la autoridad responsable de supervisar y garantizar el cumplimiento del Reglamento europeo de Servicios Digitales en España (CNMC, 2024).

La propuesta buscaba dotar a la CNMC de facultades de investigación, inspección y sanción respecto de intermediarios digitales, incluyendo acceso a información sobre sistemas algorítmicos, medidas de moderación y mecanismos de publicidad digital (Real Decreto-ley 9/2024, disp. final quinta).

Asimismo, la reforma modificaba el régimen español de responsabilidad de intermediarios, derogando los antiguos artículos 14 a 17 de la LSSI, que contenían las reglas tradicionales de *safe harbour*, para sustituirlas por la remisión directa al sistema europeo del DSA.

La reforma también ampliaba significativamente el catálogo de infracciones y sanciones administrativas, incorporando incumplimientos relativos a obligaciones de diligencia debida, transparencia, publicidad dirigida y cooperación con autoridades (Ley 34/2002, artículo 38 modificado por RDL 9/2024).

Especial relevancia tenía el reconocimiento de facultades de inspección respecto de plataformas y motores de búsqueda, incluyendo acceso a algoritmos, sistemas informáticos y modelos de gestión de datos, en línea con el enfoque europeo de supervisión reforzada sobre plataformas de gran tamaño (Ley 34/2002, artículo 35 modificado por RDL 9/2024; DSA, artículos 34 y 40).

Cabe destacar que el DSA sigue siendo plenamente aplicable por efecto directo del derecho europeo, pero debido a la falta de desarrollo normativo la Comisión Europea ha decidido llevar a España ante el Tribunal de Justicia de la Unión Europea (TJUE). En particular, la Comisión ha indicado que, si bien España ha designado coordinador de servicios digitales, no posee las competencias necesarias para llevar a cabo sus tareas. Además, no ha establecido el régimen de sanciones que deriven de la infracción del Reglamento (Comisión Europea, 2025).

3. Tipos de prestadores regulados

La Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico, adopta un concepto amplio sobre la materia, que incluye contratación electrónica, suministro de información en línea, provisión de acceso a internet, transmisión de datos, copia temporal, alojamiento de datos, motores de búsqueda y enlaces a otros sitios de internet (Ley 34/2002, considerando II).

Desde el punto de vista de la responsabilidad, la ley distingue entre **operadores de redes y proveedores de acceso** (artículo 14), **prestadores que realizan copia temporal de datos** (artículo 15), **prestadores de alojamiento o almacenamiento** (artículo 16), y **prestadores que facilitan enlaces o instrumentos de búsqueda** (artículo 17). A continuación, se entrega una definición de cada una de ellas:

- Los **operadores de redes y proveedores de acceso** cumplen una función equivalente a la mera transmisión, pues transmiten datos facilitados por el destinatario del servicio o facilitan acceso a una red de telecomunicaciones (artículo 14).
- Los **prestadores que realizan copia temporal** almacenan datos de forma automática, provisional y temporal con la única finalidad de hacer más eficaz la transmisión ulterior a otros destinatarios (artículo 15).

- Los **prestadores de alojamiento o almacenamiento** albergan datos proporcionados por el destinatario del servicio, lo que los sitúa en la categoría funcional de hosting (artículo 16).
- Los **prestadores que facilitan enlaces o instrumentos de búsqueda** cumplen una función distinta, pues no alojan necesariamente el contenido, sino que dirigen o recomiendan al usuario información disponible en otros sitios o servicios (artículo 17).

Por su parte, la Ley 13/2022, general de comunicación audiovisual, agrega una categoría relevante para la regulación de contenidos audiovisuales: el **servicio de intercambio de vídeos a través de plataforma**. Este servicio se define como

> Servicio cuya finalidad principal propia o de una de sus partes disociables o cuya funcionalidad esencial consiste en proporcionar, al público en general, a través de redes de comunicaciones electrónicas, programas, vídeos generados por usuarios o ambas cosas, sobre los que no tiene responsabilidad editorial el prestador de la plataforma, con objeto de informar, entretener o educar, así como emitir comunicaciones comerciales, y cuya organización determina el prestador, entre otros medios, con algoritmos automáticos, en particular mediante la presentación, el etiquetado y la secuenciación (artículo 2.13).

La misma ley define además **al prestador del servicio de intercambio de vídeos** como la persona física o jurídica que presta dicho servicio (artículo 2.17). También define el **vídeo generado por usuarios** como el

> conjunto de imágenes en movimiento, con o sin sonido, que constituye un elemento unitario, con independencia de su duración, creado por un usuario y puesto a disposición del público a través de una plataforma de intercambio de vídeos por dicho usuario o por cualquier otro (artículo 2.20).

Con la aplicación del DSA, estas categorías nacionales deben complementarse con las categorías europeas de **servicios intermediarios**, **plataformas en línea**, **motores de búsqueda**, **plataformas de muy gran tamaño** y **motores de búsqueda de muy gran tamaño** (DSA, artículos 3 y 33).

4. Régimen de responsabilidad

El régimen español de responsabilidad de intermediarios se regula en la Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico, y se estructura sobre la responsabilidad general de los prestadores de servicios de la sociedad de la información y sobre exenciones específicas para actividades de intermediación (artículo 13).

Los **prestadores de servicios de la sociedad de la información** "están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico", sin perjuicio de las reglas específicas de la Ley 34/2002 (artículo 13.1).

Para determinar la responsabilidad por actividades de intermediación debe atenderse a las reglas especiales sobre acceso, transmisión, copia temporal, alojamiento, enlaces y búsqueda (artículo 13.2).

Los **operadores de redes y proveedores de acceso** no son responsables por la información transmitida cuando no originan la transmisión, no modifican los datos y no seleccionan los datos ni a sus destinatarios (artículo 14.1).

La manipulación estrictamente técnica de archivos durante la transmisión no constituye modificación de datos para efectos de la exención de responsabilidad (artículo 14.1).

El almacenamiento automático, provisional y transitorio realizado como parte de la transmisión también queda cubierto por la exención cuando sirve exclusivamente para permitir la transmisión por la red y no supera el tiempo razonablemente necesario para ello (artículo 14.2).

Los **prestadores que realizan copia temporal** no son responsables por el contenido de los datos ni por su reproducción temporal si no modifican la información, cumplen las condiciones de acceso, respetan normas de actualización, no interfieren con tecnologías lícitas y retiran o bloquean la información al tener conocimiento efectivo de determinados supuestos (artículo 15).

Los **prestadores de alojamiento o almacenamiento** no son responsables por la información almacenada a petición del destinatario si no tienen conocimiento efectivo de que la actividad o información es ilícita o lesiona bienes o derechos de terceros susceptibles de indemnización (artículo 16.1.a). Si tienen conocimiento efectivo, los prestadores de alojamiento deben actuar con diligencia para retirar los datos o hacer imposible el acceso a ellos (artículo 16.1.b).

La ley entiende que existe conocimiento efectivo

> cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse (artículo 16.1).

La exención de responsabilidad del alojamiento no opera cuando el destinatario del servicio actúa bajo la dirección, autoridad o control del prestador (artículo 16.2).

Los **prestadores que facilitan enlaces o instrumentos de búsqueda** no son responsables por la información a la que dirigen si no tienen conocimiento efectivo de su ilicitud o lesión, o si, al tenerlo, actúan con diligencia para suprimir o inutilizar el enlace correspondiente (artículo 17.1). La exención para enlaces o búsqueda tampoco opera cuando el proveedor de contenidos enlazado actúa bajo la dirección, autoridad o control del prestador que facilita la localización de esos contenidos (artículo 17.2).

5. Regulación de contenidos y procedimientos

La Ley 34/2002 permite adoptar restricciones frente a servicios de la sociedad de la información que atenten o puedan atentar contra determinados principios, tales como orden público, investigación penal, seguridad pública, defensa nacional, salud pública, protección de consumidores, dignidad humana, no discriminación, protección de la juventud e infancia y propiedad intelectual (artículo 8.1).

Estas medidas pueden consistir en la interrupción del servicio o en la retirada de datos que vulneren dichos principios (artículo 8.1).

La adopción de restricciones debe respetar las garantías, normas y procedimientos previstos para proteger “los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información” (artículo 8.1). Cuando la Constitución o las leyes

exijan intervención judicial excluyente, solo la autoridad judicial competente puede adoptar medidas que afecten derechos como libertad de expresión, creación, cátedra o información (artículo 8.1).

La ley también establece un deber de colaboración de los prestadores de servicios de intermediación cuando un órgano competente ordena interrumpir un servicio o retirar contenidos y para ello sea necesaria la intervención de intermediarios (artículo 11.1).

Si se trata de servicios o contenidos procedentes de prestadores establecidos fuera de la Unión Europea o del Espacio Económico Europeo, el órgano competente puede ordenar a intermediarios establecidos en España que suspendan el servicio de intermediación necesario para impedir el acceso desde España (artículo 11.2). En la adopción de estas medidas deben respetarse los derechos a la intimidad personal y familiar, protección de datos personales, libertad de expresión y libertad de información (artículo 11.3).

El secuestro de páginas de internet o la restricción de acceso que afecte derechos del artículo 20 de la Constitución española solo puede ser decidido por órganos jurisdiccionales competentes (artículo 11.3).

Las medidas de restricción deben ser “objetivas, proporcionadas y no discriminatorias y se adoptarán de forma cautelar o en ejecución de las resoluciones que se dicten” de acuerdo con las normas procesales (artículo 11.4).

En materia audiovisual, la Ley 13/2022 impone a los **servicios de comunicación audiovisual** la prohibición de incitar a la violencia, odio o discriminación por razones como edad, sexo, discapacidad, orientación sexual, identidad de género, raza, origen étnico, religión, opiniones políticas, nacionalidad o nacimiento (artículo 4.2).

La comunicación audiovisual tampoco puede contener provocación pública a la comisión de delitos, especialmente terrorismo, pornografía infantil o incitación al odio, hostilidad, discriminación o violencia (artículo 4.4).

Los **servicios de intercambio de vídeos** a través de plataforma quedan sometidos a obligaciones destinadas a proteger a menores y al público general frente a contenidos perjudiciales, incitación al odio, violencia o provocación a la comisión de delitos de terrorismo (título V, artículos 86 al 94).

6. Debido proceso del usuario

La Ley 34/2002 contempla garantías frente a restricciones de servicios o contenidos, especialmente cuando pueden verse afectados derechos fundamentales.

En particular, la exigencia de intervención judicial para medidas que afecten la libertad de expresión o información constituye una garantía institucional fuerte frente a la remoción o bloqueo de contenidos en línea (artículos 8.1 y 11.3).

La ley también reconoce la posibilidad de acudir a mecanismos de solución extrajudicial de conflictos, incluyendo arbitraje y procedimientos instaurados por códigos de conducta u otros instrumentos de autorregulación (artículo 32). Estos procedimientos pueden tramitarse por medios electrónicos conforme a su normativa específica (artículo 32.2).

La LSSI no contiene un sistema general de reclamación interna frente a decisiones de moderación de plataformas equivalente al previsto por el DSA (DSA, artículos 20 y 21).

La Ley 13/2022 prevé mecanismos de reclamaciones de usuarios en el contexto de códigos de conducta de autorregulación y corregulación (artículo 15.2.e). Los códigos de conducta también pueden prever sistemas de resolución extrajudicial de conflictos ante entidades acreditadas de resolución alternativa de litigios (artículo 15.2.f).

7. Transparencia algorítmica y sistemas de recomendación

La Ley 13/2022 reconoce el uso de algoritmos en la organización de contenidos por parte de **servicios de intercambio de vídeos a través de plataforma**, al señalar que la organización del contenido puede determinarse mediante algoritmos automáticos, presentación, etiquetado y secuenciación (artículo 2.13).

Sin embargo, esta ley no establece un régimen general de transparencia de sistemas de recomendación equivalente al del DSA (DSA, artículo 27).

La transparencia audiovisual se expresa principalmente en obligaciones de registro (artículo 39), acceso al registro (artículo 40) y publicidad del régimen de propiedad (artículo 42).

Los **prestadores del servicio de comunicación audiovisual y de intercambio de vídeos** deben hacer accesible en sus sitios web información sobre denominación, domicilio social, datos de contacto, establecimiento en España, autoridad de supervisión, responsables editoriales y titulares de participaciones significativas (artículo 42).

La Ley 34/2002 también obliga a los **prestadores de servicios de la sociedad de la información** a poner a disposición de usuarios y órganos competentes información general como nombre o denominación social, domicilio, correo electrónico, datos registrales, autorización administrativa cuando corresponda, número de identificación fiscal y precios (artículo 10).

La dimensión algorítmica queda, por tanto, principalmente cubierta por el DSA, que obliga a las **plataformas en línea** a informar los principales parámetros de sus sistemas de recomendación y las opciones para que los usuarios puedan modificarlos o influir en ellos (DSA, artículo 27).

Las **plataformas de muy gran tamaño** y **motores de búsqueda de muy gran tamaño** deben, además, evaluar y mitigar riesgos sistémicos asociados al diseño y funcionamiento de sus servicios, incluidos sus sistemas algorítmicos (DSA, artículos 34 y 35).

8. Autoridad y supervisión

La Ley 34/2002 atribuye funciones de control al Ministerio de Asuntos Económicos y Transformación Digital respecto del cumplimiento de las obligaciones de los prestadores de servicios de la sociedad de la información, sin perjuicio de las competencias de órganos sectoriales según la materia (artículo 35).

Los órganos competentes pueden realizar actuaciones inspectoras para el ejercicio de sus funciones de control, y los funcionarios que ejerzan inspección tienen la consideración de autoridad pública (artículo 35.2).

Los prestadores tienen la obligación de facilitar la información y colaboración necesarias para el ejercicio de las funciones de control, supervisión e inspección (artículo 36).

La ley contempla un régimen de infracciones y sanciones para los **prestadores de servicios de la sociedad de la información**, incluyendo infracciones muy graves, graves y leves (artículos 37 a 43).

Entre las infracciones muy graves se encuentra el incumplimiento de la obligación de suspender transmisión, alojamiento, acceso a la red u otro servicio equivalente de intermediación cuando lo ordene un órgano administrativo competente (artículo 38.2.b).

En materia audiovisual, la Ley 13/2022 reconoce a la CNMC un rol central como autoridad audiovisual estatal competente para supervisión y control del mercado audiovisual (Ley 13/2022, preámbulo III y título IX).

La Ley 13/2022 también establece un régimen sancionador para infracciones vinculadas a la **prestación de servicios de comunicación audiovisual** y **servicios de intercambio de vídeos** a través de plataforma (Ley 13/2022, título X).

Respecto del DSA, España debe contar con un Coordinador de Servicios Digitales dotado de independencia y facultades de investigación y ejecución para aplicar el Reglamento en el territorio nacional (DSA, artículos 49 a 51).

La Comisión Nacional de los Mercados y la Competencia (CNMC) actúa como Coordinador de Servicios Digitales supervisando que los prestadores de servicios cumplan sus obligaciones y protejan los derechos de los usuarios, especialmente de los menores (CNMC, s.f.). En el sitio web de dicha entidad, solo se lista como normativa aplicable el Reglamento de servicios digitales de la UE.

C. Francia

1. Marco normativo general

Este país regula la responsabilidad de intermediarios digitales y la moderación de contenidos combinando el marco europeo que proporciona el Reglamento de Servicios Digitales (DSA) y una regulación nacional propia, principalmente contenida en la Ley Nº2004-575 sobre la confianza en la economía digital (*pour la confiance dans l'économie numérique*), conocida como LCEN, y en la Ley Nº2024-449 destinada a garantizar y regular el espacio digital (*visant à sécuriser et à réguler l'espace numérique*), conocida como SREN.

La LCEN reconoce como principio general que la comunicación pública por vía electrónica es libre, pero admite limitaciones necesarias para proteger la dignidad humana, la libertad y propiedad ajenas, el pluralismo de las corrientes de pensamiento y opinión, el orden público, la defensa nacional, las exigencias de servicio público y las limitaciones técnicas de los medios de comunicación (artículo 1).

La misma ley define la **comunicación pública por vía electrónica** (*communication au public par voie électronique*) como

> cualquier puesta a disposición del público o de categorías del público, mediante un proceso de comunicación electrónica, de signos, señales, escritos, imágenes, sonidos o mensajes de cualquier tipo que no tengan el carácter de correspondencia privada (LCEN, artículo 1).

También define la **comunicación pública en línea** (*communication au public en ligne*) como

> cualquier transmisión, a petición individual, de datos digitales que no sean de carácter de correspondencia privada, mediante un proceso de comunicación electrónica que permita un intercambio recíproco de información entre el remitente y el receptor (LCEN, artículo 1).

Tras las modificaciones introducidas por la SREN, la LCEN incorporó una sección específica sobre **proveedores de servicios intermediarios** (*fournisseurs de services intermédiaires*), conectando expresamente las instituciones contempladas en el derecho francés con las categorías del Reglamento de Servicios Digitales de la Unión Europea (LCEN, artículos 5-1 y 6).

La LCEN entiende por **servicios de la sociedad de la información** (*services de la société de l'information*) aquellos definidos por la Directiva (UE) 2015/1535, y por servicios intermediarios aquellos definidos por el artículo 3.g del DSA (LCEN, artículo 5-1).

La SREN refuerza este marco mediante normas sobre protección de menores de edad en línea, verificación de edad, retiro de contenidos ilícitos especialmente graves, bloqueo, desreferenciación, tiendas de aplicaciones y suspensión de cuentas utilizadas para cometer ciertos delitos en línea (SREN, artículos 1 al 6 y 16).

El caso francés debe entenderse, por tanto, como una implementación nacional reforzada del modelo europeo, en la cual el DSA opera como marco y la legislación interna introduce mecanismos sectoriales de protección frente a determinados contenidos.

2. Tipos de prestadores regulados

La LCEN distingue entre distintos tipos de actores digitales, siguiendo tanto las categorías europeas del DSA como las categorías que existían en la regulación francesa antes de su adopción. En primer lugar, la ley define al **proveedor de servicio de acceso a internet** (*fournisseur d'un service d'accès à internet*) como

> cualquier persona que preste un servicio de transporte simple, tal como se define en el punto (i) del apartado (g) del artículo 3 del Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, por el que se establece un mercado único de servicios digitales y se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales), cuya actividad consista en ofrecer acceso a servicios de comunicaciones públicas en línea (artículo 6.I.1).

En segundo lugar, define al **proveedor de servicios de alojamiento** (*fournisseur de services d'hébergement)* como "toda persona que presta servicios de alojamiento conforme al artículo 3.g.iii del DSA[8]" (artículo 6.I.2).

En tercer lugar, define al **motor de búsqueda en línea** (*moteur de recherche en ligne)* mediante remisión al artículo 3.j del DSA[9] (artículo 6.I.3).

[8] "consistente en almacenar datos facilitados por el destinatario del servicio y a petición de este".
[9] "un servicio intermediario que permite a los usuarios introducir consultas para hacer búsquedas de, en principio, todos los sitios web, o de sitios web en un idioma concreto, mediante una consulta sobre un tema cualquiera en forma de palabra clave, consulta de voz, frase u otro tipo de entrada, y que en respuesta muestra resultados en cualquier formato en los que puede encontrarse información relacionada con el contenido que es objeto de la consulta".

En cuarto lugar, define la **plataforma en línea** (*plateforme en ligne*) mediante remisión al artículo 3.i del DSA[10] (artículo 6.I.4).

La ley incorpora además la noción de **servicio de red social en línea** (*service de réseaux sociaux en ligne*) mediante remisión al Reglamento de Mercados Digitales, que define las redes sociales como servicios básicos de plataforma en el ecosistema digital europeo (LCEN, artículo 6.I.5; DMA, artículo 2.7).

También reconoce la categoría de **tienda de aplicaciones informáticas** (*boutique d'applications logicielles*) mediante remisión al DMA, así como la categoría de **aplicación informática** (*application logicielle*) (LCEN, artículo 6.I.6 y 6.I.7; DMA, artículo 2.14 y 2.15).

Se destacan estas definiciones porque deja patente que Francia no ha creado categorías paralelas al DSA, sino que ha adaptado su derecho interno para operar con las definiciones europeas de intermediarios, plataformas, motores de búsqueda, redes sociales y tiendas de aplicaciones (LCEN, artículos 5-1 y 6).

La LCEN aclara además que las personas cuya actividad consiste en prestar un **servicio intermediario** (*service intermédiaire*) conforme al artículo 3.g del DSA no son productores en el sentido de la ley francesa sobre comunicación audiovisual, lo que contribuye a separar la responsabilidad editorial de la responsabilidad propia de los intermediarios técnicos (LCEN, artículo 6.II).

3. Régimen de responsabilidad

El régimen francés consagra en la LCEN el mecanismo de responsabilidad de intermediarios, construyéndose sobre la distinción entre **editores de contenido** y **prestadores técnicos de servicios intermediarios** (artículos 1-1, 5-1 y 6).

Los **editores de servicios de comunicación pública en línea** (*editer un service de communication au public en ligne*) deben poner a disposición del público información de identificación, incluyendo nombre o razón social, domicilio o sede, datos de contacto, nombre del director de publicación y datos del proveedor de alojamiento (artículo 1-1.I).

Las **personas que editan servicios de comunicación pública en línea de manera no profesional** pueden preservar su anonimato frente al público, siempre que comuniquen sus datos de identificación al proveedor de alojamiento (artículo 1-1.II).

Los **proveedores de alojamiento** quedan sujetos a secreto profesional respecto de los datos de identificación personal recibidos de editores no profesionales, sin que dicho secreto sea oponible a la autoridad judicial (artículo 1-1.II).

La LCEN impone a los proveedores de alojamiento obligaciones específicas de cooperación frente a contenidos que constituyen determinadas infracciones penales graves, como provocación a actos terroristas, pornografía infantil, acoso, trata, proxenetismo, delitos de odio y otros contenidos especialmente sensibles (artículo 6.IV.A). Estos proveedores deben informar prontamente a las

[10] "un servicio de alojamiento de datos que, a petición de un destinatario del servicio, almacena y difunde información al público, salvo que esa actividad sea una característica menor y puramente auxiliar de otro servicio o una funcionalidad menor del servicio principal y que no pueda utilizarse sin ese otro servicio por razones objetivas y técnicas, y que la integración de la característica o funcionalidad en el otro servicio no sea un medio para eludir la aplicabilidad del presente Reglamento".

autoridades competentes de las actividades ilícitas que les sean señaladas y que ejerzan los destinatarios de sus servicios (artículo 6.IV.A).

El incumplimiento de esta obligación de información puede ser sancionado con pena de prisión y multa de 250.000 euros; y las personas jurídicas pueden ser declaradas penalmente responsables conforme a las reglas del Código Penal francés (artículo 6.IV.A).

La ley también sanciona el incumplimiento de la obligación de informar inmediatamente a las autoridades competentes prevista en el artículo 18 del DSA, que se refiere a la sospecha de delitos que impliquen amenaza para la vida o seguridad de las personas (artículo 6.IV.C). Cuando la infracción de esta obligación sea cometida habitualmente por una persona jurídica, la multa puede alcanzar hasta el 6% de su volumen de negocios mundial (artículo 6.IV.C).

Además, los **proveedores de acceso y de alojamiento** deben conservar datos que permitan identificar a quienes contribuyeron a la creación de contenidos alojados en los servicios que prestan (artículo 6.V.A).

El incumplimiento de estas obligaciones de conservación o la negativa a entregar los datos requeridos por autoridad judicial puede dar lugar a sanciones penales consistentes en un año de prisión y multa de 250.000 euros (artículo 6.V.B).

4. Regulación de contenidos y procedimientos

La LCEN establece procedimientos específicos para el retiro y bloqueo de contenidos de especial gravedad, particularmente vinculados al terrorismo, material sexual infantil y tráfico de drogas (artículo 6-1).

Cuando las necesidades de lucha contra la provocación o apología del terrorismo, la difusión de imágenes o representaciones de menores de carácter pornográfico o la oferta de estupefacientes lo justifiquen, la autoridad administrativa puede solicitar a editores o proveedores de alojamiento el retiro de contenidos contrarios a las disposiciones penales correspondientes (artículo 6-1.I).

Si el contenido no es retirado dentro del plazo de 24 horas, la autoridad administrativa puede notificar a los proveedores de acceso a internet la lista de direcciones electrónicas que deben ser bloqueadas sin demora (artículo 6-1.I).

La autoridad administrativa también puede notificar dichas direcciones a motores de búsqueda o directorios, que deben adoptar medidas útiles para hacer cesar la referenciación del servicio de comunicación pública en línea (artículo 6-1.I).

Estas solicitudes y listas se transmiten a una personalidad calificada designada por la Autoridad Reguladora de las Comunicaciones Audiovisuales y Digitales (ARCOM por sus siglas en francés - *Autorité de régulation de la communication audiovisuelle et numérique*), encargada de controlar la regularidad de las solicitudes de retiro y de las condiciones de elaboración, actualización, comunicación y uso de la lista (artículo 6-1.I).

Si la personalidad calificada constata una irregularidad, puede recomendar a la autoridad administrativa ponerle término, y, si la autoridad no sigue esa recomendación, puede acudir a la jurisdicción administrativa competente (artículo 6-1.I).

La personalidad calificada debe publicar anualmente un informe de actividad sobre las condiciones de ejercicio y resultados de su actividad, indicando el número de solicitudes de retiro, contenidos retirados, motivos de retiro y recomendaciones formuladas a la autoridad administrativa (artículo 6-1.I).

La LCEN contempla además procedimientos específicos para contenidos terroristas en línea bajo el Reglamento (UE) 2021/784[11], asignando competencias a la autoridad administrativa y a ARCOM para emitir órdenes, supervisar medidas específicas y recibir notificaciones de representantes legales (artículo 6-1-1).

El incumplimiento de obligaciones de retirar contenido terrorista o bloquear el acceso dentro del plazo de una hora puede dar lugar a prisión de un año y multa de 250.000 euros. Si la infracción la comete una persona jurídica, la multa puede incrementarse hasta el 4% del volumen de negocios mundial (LCEN, artículo 6-1-3).

La SREN refuerza estos instrumentos en materia de protección de menores frente a contenidos pornográficos, otorgando a ARCOM la potestad de verificar que dichos contenidos no sean accesibles a menores (artículo 1).

ARCOM debe establecer y publicar un referente técnico que determine exigencias mínimas aplicables a los sistemas de verificación de edad, incluyendo fiabilidad del control de edad y respeto a la vida privada (artículo 1). Los **editores de servicios de comunicación pública en línea** y los **proveedores de plataformas de intercambio de vídeos** deben desplegar una pantalla sin contenido pornográfico mientras la edad del usuario no haya sido verificada (artículo 1).

ARCOM puede requerir auditorías independientes de los sistemas de verificación de edad implementados por los servicios concernidos (artículo 1). Si un servicio permite el acceso de menores a contenido pornográfico, ARCOM puede formular observaciones motivadas, poner en mora al prestador, ordenar medidas para impedir el acceso de menores, aplicar sanciones, ordenar bloqueo a proveedores de acceso y solicitar desreferenciación a motores de búsqueda (artículo 2).

ARCOM también puede solicitar a **tiendas de aplicaciones** que impidan la descarga de aplicaciones que den acceso a contenidos pornográficos cuando el servicio incumpla sus obligaciones de verificación o bloqueo (artículo 3).

5. Debido proceso del usuario y garantías de revisión

El sistema francés combina mecanismos previstos tanto en la LCEN como en la SREN.

La LCEN establece que los **proveedores de alojamiento** (*fournisseurs de services d'hébergement*) y los **proveedores de contenidos afectados por una solicitud de retiro** (*fournisseurs de contenus concernés par une demande de retrait)* pueden pedir al presidente del tribunal administrativo o al magistrado delegado la anulación de la solicitud dentro del plazo de 48 horas desde su recepción o desde que el proveedor de contenidos fue informado del retiro (artículo 6-1.II).

La jurisdicción administrativa debe pronunciarse sobre la legalidad de la orden de retiro dentro del plazo de setenta y dos horas desde su presentación, y la audiencia es pública (artículo 6-1.II). La sentencia

[11] Reglamento (UE) 2021/784 del Parlamento Europeo y del Consejo, de 29 de abril de 2021, sobre la lucha contra la difusión de contenidos terroristas en línea.

puede ser apelada dentro de 10 días desde su notificación, y la jurisdicción de apelación debe resolver dentro de un mes desde su intervención (artículo 6-1.II).

En el caso de órdenes vinculadas al Reglamento sobre contenidos terroristas en línea, **proveedores de alojamiento** y **proveedores de contenidos** también pueden solicitar la anulación de la orden o de la decisión motivada dentro de plazos breves ante la jurisdicción administrativa (artículo 6-1-5).

La SREN, por su parte, contempla que las personas afectadas por medidas de bloqueo, desreferenciación o medidas contra tiendas de aplicaciones pueden solicitar la anulación de dichas medidas ante la jurisdicción administrativa dentro de cinco días desde su recepción (artículo 2).

La jurisdicción administrativa debe resolver sobre la legalidad de la medida de bloqueo o desreferenciación dentro del plazo de un mes desde su presentación, y sus decisiones pueden ser apeladas dentro de diez días (artículo 2).

En materia de retiro de contenidos pedopornográficos[12], la SREN exige que, cuando un **proveedor de alojamiento** retire contenido, informe al **proveedor de contenidos** los motivos del retiro, la posibilidad de solicitar copia de la orden y los derechos disponibles para impugnar la solicitud ante la jurisdicción administrativa (artículo 4).

Esta obligación de información puede suspenderse cuando la autoridad competente estime necesario y proporcionado no divulgar información para no obstaculizar acciones de prevención, detección, investigación y persecución penal (SREN, artículo 4).

6. Transparencia algorítmica y sistemas de recomendación

La regulación francesa de intermediarios no contiene una regla nacional general de transparencia de sistemas de recomendación equivalente al artículo 27 del DSA, por lo que esa materia se rige principalmente por el Reglamento europeo.

No obstante, la LCEN y la SREN incorporan obligaciones de transparencia e identificación relevantes para el entorno digital. Los **editores de servicios de comunicación pública en línea** deben poner a disposición del público información de identificación y contacto en un estándar abierto, incluyendo información sobre el proveedor de alojamiento (LCEN, artículo 1-1.I).

Las personas nombradas o designadas en un servicio de comunicación pública en línea tienen derecho de respuesta, sin perjuicio de solicitudes de corrección o eliminación del mensaje dirigidas al servicio (LCEN, artículo 1-1.III).

En materia de contenidos pornográficos, la SREN, modifica la LCEN, exigiendo que los **sistemas de verificación de edad** (*systèmes de vérification de l'âge*) cumplan estándares técnicos mínimos fijados por ARCOM y evaluados con intervención de la autoridad de protección de datos (artículo 10-I).

La SREN también regula ciertos contenidos generados por tratamiento algorítmico, al modificar el Código Penal para sancionar la difusión de contenidos visuales o sonoros generados algorítmicamente que representen la imagen o palabras de una persona sin consentimiento cuando no sea evidente que

[12] pornografía infantil.

se trata de contenido generado algorítmicamente o no se indique expresamente (SREN, artículo 15; artículo 226-8 del Código Penal).

En materia de *deepfakes* sexuales, la SREN modifica el Código Penal, cuyo artículo 226-8-1 sanciona la difusión de montajes de carácter sexual realizados con la imagen o palabras de una persona sin consentimiento, incluyendo contenidos generados por tratamiento algorítmico (SREN, artículo 21).

La dimensión de **sistemas de recomendación**, sin embargo, queda principalmente cubierta por el DSA, que obliga a las plataformas a informar los principales parámetros de sus recomendadores y a las **plataformas de muy gran tamaño** a evaluar riesgos sistémicos asociados a sus sistemas algorítmicos (DSA, artículos 27, 34 y 35).

7. Autoridad y supervisión

En Francia, la supervisión y aplicación del Reglamento de Servicios Digitales (DSA) corresponde principalmente a la Autoridad Reguladora de las Comunicaciones Audiovisuales y Digitales (ARCOM por sus siglas en francés - *Autorité de régulation de la communication audiovisuelle et numérique*), en su calidad de Coordinador de Servicios Digitales (Arcom, s.f.).

En ejercicio de estas funciones, Arcom puede investigar a los prestadores de servicios establecidos en Francia, requerir el cese de infracciones, imponer multas y sanciones pecuniarias coercitivas, e incluso ordenar, como medida de último recurso, restricciones temporales de acceso al servicio. Asimismo, determinadas competencias son compartidas con otros organismos especializados, como la Comisión Nacional de Tecnologías de la Información y Libertades (*Commission nationale de l'informatique et des libertés* - CNIL), en materia de protección de datos personales, y la Dirección General de Competencia, Asuntos del Consumidor y Control del Fraude (*Direction générale de la concurrence, de la consommation et de la répression des fraudes* - DGCCRF), en el ámbito de la protección de los consumidores y del derecho del consumo en línea (Arcom, s.f.).

De acuerdo con LCEN, ARCOM puede supervisar el cumplimiento de obligaciones bajo el Reglamento (UE) 2021/784 respecto de **proveedores de alojamiento** establecidos en Francia o con representante legal residente en Francia (artículo 6-1-4). Asimismo, también puede requerir información necesaria para el seguimiento de obligaciones, poner en mora a proveedores, imponer sanciones pecuniarias y hacer públicas sus decisiones de puesta en mora y sanción (artículo 6-1-4).

Las sanciones pueden considerar la naturaleza, gravedad y duración del incumplimiento, el carácter intencional o negligente, antecedentes de incumplimiento, situación financiera, cooperación con autoridades, naturaleza y tamaño del proveedor y grado de responsabilidad asociado a medidas técnicas y organizativas (artículo 6-1-4).

En cuanto a la protección de menores de edad frente a contenidos pornográficos, ARCOM puede establecer estándares técnicos, exigir auditorías, emitir observaciones motivadas, imponer medidas de cumplimiento, ordenar bloqueos y desreferenciaciones, y aplicar sanciones económicas (SREN, artículos 1 y 2).

La SREN prevé además reportes anuales de actividad de ARCOM sobre decisiones de requerimiento, medidas adoptadas, decisiones judiciales relacionadas y número de direcciones electrónicas bloqueadas o desreferenciadas (artículo 2).

D. Brasil

1. Marco normativo general

Brasil regula la responsabilidad de intermediarios y los contenidos digitales principalmente mediante la Ley Nº12.965 de 2014, que establece principios, garantías, derechos y deberes para el uso de internet en Brasil (*estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil),* que establece principios, garantías, derechos y deberes para el uso de internet en Brasil conocida como Marco de Derechos Civiles para Internet o Marco Civil (artículo 1).

Este Marco Civil se funda expresamente en el respeto a la libertad de expresión y en otros fundamentos como el reconocimiento de la escala mundial de la red, los derechos humanos, el desarrollo de la personalidad, la ciudadanía en medios digitales, la pluralidad, la diversidad, la apertura, la colaboración, la libre iniciativa, la libre competencia, la defensa del consumidor y la finalidad social de la red (artículo 2).

Los principios de la disciplina brasileña de internet incluyen la garantía de libertad de expresión, comunicación y manifestación del pensamiento, la protección de la privacidad, la protección de datos personales, la neutralidad de red, la estabilidad y funcionalidad de la red, la responsabilidad de los agentes según sus actividades, la naturaleza participativa de la red y la libertad de modelos de negocio que no contradigan la ley (artículo 3).

Por su parte, la Ley N°13.709 de 2018, General de Datos Personales (*Lei Geral de Proteção de Dados Pessoais* - LGPD), complementa este marco al regular el tratamiento de datos personales, incluso en medios digitales, con el objeto de proteger derechos fundamentales de libertad, privacidad y libre desarrollo de la personalidad (artículo 1).

La LGPD reconoce derechos del titular frente a decisiones basadas únicamente en tratamiento automatizado de datos personales que afecten sus intereses (artículo 20).

En septiembre de 2025, Brasil incorporó además la Ley Nº15.211, estatuto digital para niños y adolescentes (*Estatuto Digital da Criança e do Adolescente*), que regula la protección de niños, niñas y adolescentes en ambientes digitales y se aplica a productos o servicios de tecnología de la información dirigidos a ellos o de acceso probable por ellos en el país (artículo 1).

2. Tipos de prestadores regulados

El Marco Civil distingue entre conexión a internet, aplicaciones de internet, registros de conexión y registros de acceso a aplicaciones de internet (artículo 5). A continuación, se presentan las correspondientes definiciones:

- La **conexión a internet** (*conexão à internet*) se define como “la habilitación de un terminal para enviar y recibir paquetes de datos mediante la atribución o autenticación de una dirección IP” (artículo 5.V).
- Las **aplicaciones de internet** (*aplicações de internet*) se definen como “el conjunto de funcionalidades que pueden ser accedidas mediante un terminal conectado a internet” (artículo 5.VII).

- El **registro de conexión** (*registro de conexão*) corresponde al "conjunto de información relativa a la fecha y hora de inicio y finalización de una conexión a Internet, su duración y la dirección IP utilizada por el terminal para enviar y recibir paquetes de datos" (artículo 5.VI).
- El **registro de acceso a aplicaciones de internet** (*registros de acesso a aplicações de internet*) corresponde al "conjunto de informaciones referentes a la fecha y hora de uso de una determinada aplicación de internet desde una determinada dirección IP" (artículo 5.VIII).

La Ley N° 15.211/2025, introduce categorías más específicas para el ámbito de niños, niñas y adolescentes, incluyendo **producto o servicio de tecnología de la información** (*produto ou serviço de tecnologia da informação)*, **producto o servicio de monitoreo infantil** (*produto ou serviço de monitoramento infantil*), **red social** (*rede social*), **perfilamiento** (*perfilamento*), **tienda de aplicaciones de internet** *(loja de aplicações de internet),* **sistema operacional** *(sistema operacional)* **mecanismo de supervisión parental** (*mecanismo de supervisão parental*), **servicio con control editorial** (*serviço com controle editorial*), **monetización** (*monetização*) **impulsionamiento** (*impulsionamento*) (artículo 2).

Esta ley define **red social** (*rede social*) como

> aplicación de internet cuyo objetivo principal es compartir y difundir, por parte de los usuarios, opiniones e información transmitidas a través de textos o imágenes, sonidos o archivos audiovisuales, en una única plataforma, mediante cuentas conectadas o articuladas, permitiendo la conexión entre usuarios (artículo 2.III).

Define **perfilamiento** (*perfilamento*) como

> cualquier forma de tratamiento de datos personales, automatizado o no, para evaluar determinados aspectos de una persona física, con el fin de clasificarla en un grupo o perfil para inferir su comportamiento, situación económica, salud, preferencias personales, intereses, deseos de consumo, ubicación geográfica, movimientos, posiciones políticas u otras características similares (artículo 2.V).

También, define **tienda de aplicaciones** *(loja de aplicações de internet)* como una "aplicación de internet que distribuye y facilita la descarga, para usuarios terminales, de aplicaciones de internet disponibles o accesibles a través de su plataforma" (artículo 2.VI) y al **sistema operacional** *(sistema operacional)* como "software de sistema que controla las funciones básicas del hardware o software y permite que las aplicaciones de Internet, los programas informáticos, las aplicaciones u otro software se ejecuten a través de él" (artículo 2.VII).

3. Régimen de responsabilidad

La regla es que "el proveedor de conexión a internet no será responsable civilmente por daños derivados de contenidos generados por terceros" (artículo 18).

En el caso del **proveedor de aplicaciones de internet,** el Marco Civil establece una regla general de responsabilidad condicionada al incumplimiento de una orden judicial específica de retiro (Marco Civil, artículo 19). Dicha regla establece que el proveedor de aplicaciones solo puede ser responsabilizado civilmente por daños derivados de contenido generado por terceros si, después de una orden judicial

específica, no adopta las medidas necesarias para hacer indisponible el contenido señalado dentro del plazo y límites técnicos del servicio (artículo 19).

La orden judicial debe identificar de manera clara y específica el contenido señalado como infractor, permitiendo su localización inequívoca, bajo pena de nulidad (artículo 19, §1).

Se exceptúan de esa regla los contenidos que involucren desnudez o actos sexuales de carácter privado difundidos sin autorización de sus participantes (artículo 21). En ese caso, el proveedor de aplicaciones que aloje el contenido puede ser responsable subsidiariamente si, tras recibir notificación del participante o su representante legal, deja de promover diligentemente la indisponibilidad del contenido dentro del ámbito y límites técnicos de su servicio (artículo 21).

La notificación debe contener elementos que permitan la identificación específica del material señalado como violatorio de la intimidad del participante y la verificación de legitimidad para presentar el requerimiento (artículo 21, parágrafo único).

4. Regulación de contenidos y procedimientos

El Marco Civil dispone como regla general que el retiro de contenidos de terceros que pueda generar responsabilidad del proveedor de aplicaciones requiere una orden judicial específica (artículo 19).

La ley permite que las causas sobre resarcimiento por daños derivados de contenidos disponibles en internet relacionados con honra, reputación o derechos de personalidad, así como la indisponibilidad de esos contenidos, puedan ser presentadas ante juzgados especiales (artículo 19, §3).

El juez puede anticipar total o parcialmente los efectos de la tutela solicitada cuando exista prueba inequívoca del hecho y, considerado el interés de la colectividad en la disponibilidad del contenido, se verifique verosimilitud de la alegación del autor y temor fundado de daño irreparable o de difícil reparación (artículo 19, §4).

La excepción de contenidos íntimos no consentidos opera sin necesidad de orden judicial previa, pues basta la notificación del participante o su representante legal para activar el deber de indisponibilidad diligente del proveedor de aplicaciones (artículo 21).

En materia de neutralidad de red, el responsable de transmisión, conmutación o enrutamiento debe tratar de forma isonómica cualquier paquete de datos, sin distinción por contenido, origen, destino, servicio, terminal o aplicación (artículo 9).

La discriminación o degradación del tráfico solo puede derivar de requisitos técnicos indispensables para la prestación adecuada de servicios y aplicaciones o de la priorización de servicios de emergencia (artículo 9, §1).

En esos casos, el responsable debe abstenerse de causar daño a los usuarios, actuar con proporcionalidad, transparencia e isonomía, informar previamente de manera transparente y abstenerse de conductas anticompetitivas (artículo 9, §2).

En el ámbito de niños, niñas y adolescentes, la Ley N° 15.211/2025 exige que los proveedores adopten medidas razonables desde la concepción y durante la operación de sus productos o servicios para prevenir y mitigar riesgos de acceso, exposición, recomendación o facilitación de contacto con

contenidos de explotación sexual, violencia, acoso, autolesión, apuestas, productos prohibidos, prácticas publicitarias predatorias y pornografía (artículo 6).

Los **proveedores de productos o servicios dirigidos a niños, niñas y adolescentes** o de acceso probable por ellos deben realizar gestión de riesgos de sus recursos, funcionalidades y sistemas, evaluar contenidos según edad, impedir acceso a contenidos ilegales, pornográficos o manifiestamente inadecuados, evitar diseños de uso compulsivo e informar la clasificación etaria del producto o servicio (artículo 8).

Cuando se trate de contenido, producto o servicio impropio, inadecuado o prohibido para menores de dieciocho años, los proveedores deben adoptar medidas eficaces para impedir el acceso de niños, niñas y adolescentes, incluyendo mecanismos confiables de verificación de edad en cada acceso y prohibición de autodeclaración (artículo 9).

5. Debido proceso del usuario

La Ley que establece principios, garantías, derechos y deberes para el uso de internet, dispone que el acceso a internet se reconoce como esencial para el ejercicio de la ciudadanía, y se aseguran derechos como inviolabilidad de intimidad y vida privada, secreto del flujo de comunicaciones, secreto de comunicaciones privadas almacenadas y no suspensión de conexión salvo por deuda directa derivada de su uso (artículo 7.I - IV).

El usuario tiene derecho a información clara y completa en contratos de prestación de servicios, incluyendo régimen de protección de registros, prácticas de gestión de red que puedan afectar su calidad y políticas de uso de proveedores de conexión y aplicaciones (artículo 7.VI y XI).

También tiene derecho a no entrega de datos personales a terceros salvo consentimiento libre, expreso e informado o hipótesis legales (artículo 7.VII), y a información clara sobre recolección, uso, almacenamiento, tratamiento y protección de datos personales (artículo 7 VIII).

Además, la ley reconoce la aplicación de normas de protección y defensa del consumidor en las relaciones de consumo realizadas en internet (artículo 7.XIII).

La privacidad y la libertad de expresión son declaradas condiciones para el pleno ejercicio del derecho de acceso a internet (artículo 8).

En materia de remoción de contenidos, el debido proceso se canaliza principalmente por vía judicial, ya que la responsabilidad del proveedor de aplicaciones depende de una orden judicial específica, identificable y acotada al contenido infractor (artículo 19).

Por su parte, la LGPD introduce una dimensión de debido proceso algorítmico al reconocer al titular el derecho a solicitar revisión de decisiones tomadas únicamente sobre la base de tratamiento automatizado de datos personales que afecten sus intereses (artículo 20).

El titular también puede obtener información clara y adecuada sobre los criterios y procedimientos utilizados para la decisión automatizada, observados los secretos comercial e industrial (LGPD, artículo 20, §1).

6. Transparencia algorítmica y sistemas de recomendación

La transparencia en el Marco Civil se concentra en información contractual, políticas de uso, tratamiento de datos personales y prácticas de gestión de red que puedan afectar la calidad del servicio (Marco Civil, artículo 7.VI, VIII y XI).

Por su parte, la LGPD reconoce el derecho a solicitar revisión de decisiones adoptadas únicamente con base en tratamiento automatizado de datos personales (artículo 20). El derecho de revisión comprende decisiones destinadas a definir perfil personal, profesional, de consumo, de crédito o aspectos de la personalidad del titular (artículo 20).

El controlador debe proporcionar, cuando sea solicitado, información clara y adecuada sobre los criterios y procedimientos utilizados en la decisión automatizada, observados los secretos comercial e industrial (artículo 20, §1).

La autoridad nacional puede realizar auditoría para verificar aspectos discriminatorios en el tratamiento automatizado de datos personales cuando el controlador no entregue información amparándose en secreto comercial o industrial (artículo 20, §2).

La LGPD también considera como datos personales aquellos utilizados para la formación de perfil comportamental de una persona natural determinada, si esta es identificada (artículo 12, §2).

En el ámbito de niños, niñas y adolescentes, la Ley N°15.211/2025 establece que los proveedores deben prevenir y mitigar riesgos de recomendación o facilitación de contacto con contenidos dañinos para niños, niñas y adolescentes, incluyendo autolesión, suicidio, pornografía, explotación sexual, violencia y prácticas publicitarias predatorias (artículo 6).

Además, las herramientas de supervisión parental deben incluir control sobre sistemas de recomendación personalizados, incluida la opción de desactivación (artículo 17, §4.V).

Finalmente, los proveedores no pueden diseñar, modificar o manipular interfaces con el objetivo o efecto de comprometer la autonomía, toma de decisión o elección del usuario, especialmente si ello debilita herramientas de supervisión parental o salvaguardas (artículo 18, §2).

7. Autoridad y supervisión

El Marco de Derechos Civiles distribuye el *enforcement* entre autoridad judicial, autoridades administrativas competentes y órganos de protección de datos, consumo y telecomunicaciones.

Especificamente, la orden judicial cumple un rol central en la remoción de contenidos de terceros, tanto para activar la responsabilidad del proveedor de aplicaciones como para obtener registros necesarios para identificar usuarios o responsables (artículos 19, 22 y 23).

La parte interesada puede solicitar judicialmente registros de conexión o registros de acceso a aplicaciones para formar un conjunto probatorio en procesos civiles o penales, siempre que existan indicios fundados del ilícito, justificación motivada de utilidad de los registros y período específico al que se refieren (artículo 22).

El juez debe adoptar medidas necesarias para garantizar la confidencialidad de la información recibida y preservar la intimidad, vida privada, honra e imagen del usuario (artículo 23).

La LGPD crea o reconoce una autoridad nacional encargada de velar, implementar y fiscalizar el cumplimiento de la normativa de protección de datos en todo el territorio nacional (artículo 5.XIX). Se trata de la Autoridad Nacional de Protección de Datos (*Autoridade Nacional de Proteção de Dados* – ANPD), que ofrece canales de comunicación para las solicitudes en materia de datos personales de las personas, de los encargados del tratamiento, las empresas de impresión y la sociedad en general (Gobierno de Brasil, s.f.)

En decisiones automatizadas y tratamiento de datos, la autoridad nacional puede solicitar informes de impacto y fiscalizar tratamientos que puedan generar riesgos para derechos y libertades del titular (artículos 10, §3 y 20, §2).

La Ley N°15.211/2025 prevé la existencia de una autoridad administrativa autónoma de protección de derechos de niños, niñas y adolescentes en ambiente digital, encargada de aplicar la ley, fiscalizar su cumplimiento y dictar reglamentos y procedimientos para su ejecución (artículo 2.X).

Esta autoridad puede emitir recomendaciones y orientaciones sobre prácticas relevantes para cumplir las obligaciones de protección infantil digital, considerando asimetrías regulatorias, funcionalidades, nivel de riesgo del producto o servicio, evolución tecnológica y patrones técnicos aplicables (artículo 5, §3).

E. Australia

1. Marco normativo general

Australia regula la responsabilidad de intermediarios y la moderación de contenidos desde un enfoque de seguridad en línea, cuyo eje normativo principal es la Ley de Seguridad en Línea (*Online Safety Act)* de 2021.

Dicha ley tiene por objeto mejorar y promover la seguridad en línea de las personas en Australia (sección 3).

El modelo australiano se organiza en torno al Comisionado de Seguridad en Línea (*eSafety Commissioner*) (sección 26), autoridad independiente con funciones de promoción de seguridad en línea, administración de sistemas de quejas, gestión del esquema de contenidos en línea, monitoreo de cumplimiento y formulación de orientaciones o buenas prácticas (sección 27).

Específicamente, la ley contempla mecanismos específicos para el ciber acoso (*cyberbullying)* contra niños (sección 6), ciber abuso (*cyber-abuse*) contra adultos (sección 7), difusión no consentida de imágenes íntimas, material violento extremo (sección 8), contenidos clasificados como clase 1[13] o clase 2[14] (sección 9) códigos de industria y estándares obligatorios (*Online Safety Codes and Standards*).

El sistema se complementa con las Expectativas básicas de seguridad en línea (*Basic Online Safety Expectations* – BOSE), que fijan expectativas gubernamentales respecto de las medidas que deben adoptar ciertos servicios para mantener seguros a sus usuarios, aunque dichas expectativas no constituyen por sí mismas un deber exigible judicialmente (secciones 45 y 46).

[13] De acuerdo con la sección 106.
[14] De acuerdo con la sección 107.

También se complementa con los Códigos y normas de seguridad en línea (*Online Safety Codes and Standards*), que imponen obligaciones obligatorias y exigibles a distintas secciones de la industria en línea, según el tipo de servicio y el riesgo que presentan respecto de contenidos ilícitos o restringidos por edad (Online Safety Act, ss. 132 a 150).

La guía regulatoria de Comisionado de Seguridad en Línea de abril de 2026 señala que estos códigos y estándares buscan abordar riesgos sistémicos y promover cambios proactivos, más que limitarse a incidentes aislados de contenido (eSafety Commissioner, 2026 a: 4).

2. Tipos de prestadores regulados

La *Online Safety Act* distingue categorías de servicios digitales y de actores de la industria en línea, entre ellos **servicios de redes sociales** (*social media service*) (sección 13), **servicios electrónicos relevantes** (*relevant electronic service*) (sección 13A), **servicios de internet designados** (*designated internet service*) (sección 14), **servicios de hosting** (*hosting service*) (sección 17), **proveedores de internet** (*internet service providers*) (sección 19). A continuación, se presentan las correspondientes definiciones:

- Un **servicio de red social** (*social media service*) es un servicio electrónico cuya finalidad principal sea permitir la interacción social en línea entre dos o más usuarios finales; que permita a dichos usuarios conectarse o interactuar entre sí, total o parcialmente; y que posibilite la publicación de contenidos en la plataforma, además de cumplir las demás condiciones que puedan establecer las reglas legislativas aplicables. Se excluyen de esta definición los servicios expresamente exceptuados por la normativa correspondiente (sección 13).
- Un **servicio electrónico relevante** (*relevant electronic service*) incluye servicios que permiten comunicación por correo electrónico, mensajería instantánea, SMS, MMS, chat, juegos en línea entre usuarios u otros servicios especificados por reglas legislativas (sección 13A).
- Un **servicio de internet designado** (*designated internet service*) es un servicio que permite a los usuarios acceder a material mediante un servicio de transporte de internet o que entrega material a personas con equipos aptos para recibirlo, excluyendo servicios de redes sociales, servicios electrónicos relevantes, servicios de programas a demanda y otros servicios exceptuados (sección 14).
- El **servicio de hosting** (*hosting service*) se configura cuando una persona aloja material almacenado que ha sido proporcionado en un servicio de red social, servicio electrónico relevante o servicio de internet designado (sección 17).
- Un **proveedor de servicios de internet** (*internet service providers*) es quien suministra o propone suministrar al público un servicio de transporte de internet (sección 19).

La ley también contempla **servicios de distribución de aplicaciones** (*app distribution service*), definidos como “servicios que permiten a los usuarios descargar aplicaciones mediante un servicio de transporte” (sección 5).

La guía del Comisionado en Línea, indica que los códigos y estándares cubren ocho secciones de la industria en línea: **servicios de redes sociales**, **servicios electrónicos relevantes**, **servicios de**

internet designados, **motores de búsqueda**, **tiendas de aplicaciones**, **hosting**, **servicios de transporte de internet** y **servicios de equipamiento** (eSafety Commissioner a, 2026: 8).

3. Régimen de responsabilidad y deberes de actuación

La ley permite al *eSafety Commissioner* recibir e investigar quejas sobre ciber acoso (*cyberbullying*) dirigido a niños australianos, ciber abuso (*cyber-abuse*) dirigido a adultos australianos, difusión no consentida de imágenes íntimas y contenidos clase 1[15] o clase 2[16] accesibles para usuarios en Australia.

[15] La sección 106 de la ley dispone que:
(1) Para los efectos de esta ley, se entiende por material de clase 1:
(a) material respecto del cual se cumplen las siguientes condiciones:
(i) el material es una película o el contenido de una película;
(ii) la película ha sido clasificada como RC por la Junta de Clasificación conforme a la *Classification (Publications, Films and Computer Games) Act 1995*; o
(b) material respecto del cual se cumplen las siguientes condiciones:
(i) el material es una película o el contenido de una película;
(ii) la película no ha sido clasificada por la Junta de Clasificación conforme a la *Classification (Publications, Films and Computer Games) Act 1995*;
(iii) si la película fuese clasificada por la Junta de Clasificación conforme a dicha ley, probablemente sería clasificada como RC; o
(c) material respecto del cual se cumplen las siguientes condiciones:
(i) el material es una publicación o el contenido de una publicación;
(ii) la publicación ha sido clasificada como RC por la Junta de Clasificación conforme a la *Classification (Publications, Films and Computer Games) Act 1995*; o
(d) material respecto del cual se cumplen las siguientes condiciones:
(i) el material es una publicación o el contenido de una publicación;
(ii) la publicación no ha sido clasificada por la Junta de Clasificación conforme a la *Classification (Publications, Films and Computer Games) Act 1995*;
(iii) si la publicación fuese clasificada por la Junta de Clasificación conforme a dicha ley, probablemente sería clasificada como RC; o
(e) material respecto del cual se cumplen las siguientes condiciones:
(i) el material es un videojuego;
(ii) el videojuego ha sido clasificado como RC por la Junta de Clasificación conforme a la *Classification (Publications, Films and Computer Games) Act 1995*; o
(f) material respecto del cual se cumplen las siguientes condiciones:
(i) el material es un videojuego;
(ii) el videojuego no ha sido clasificado por la Junta de Clasificación conforme a la *Classification (Publications, Films and Computer Games) Act 1995*;
(iii) si el videojuego fuese clasificado por la Junta de Clasificación conforme a dicha ley, probablemente sería clasificado como RC; o
(g) material respecto del cual se cumplen las siguientes condiciones:
(i) el material no es una película, ni el contenido de una película, ni un videojuego, ni una publicación, ni el contenido de una publicación;
(ii) si el material fuese clasificado por la Junta de Clasificación de manera equivalente a la forma en que se clasificaría una película conforme a la *Classification (Publications, Films and Computer Games) Act 1995*, probablemente sería clasificado como RC.
Nota: Véase también la sección 160 (el Comisionado puede obtener asesoría de la Junta de Clasificación).
(2) La sección 22CF de la *Classification (Publications, Films and Computer Games) Act 1995* (relativa a la clasificación mediante una herramienta de clasificación aprobada) se aplica para los efectos de esta sección de manera equivalente a la forma en que se aplica para los efectos de dicha ley.

[16] De acuerdo con la sección 107: (1) Para los efectos de esta ley, se entiende por material de clase 2:
(a) material respecto del cual se cumplen las siguientes condiciones:
(i) el material es una película o el contenido de una película;
(ii) la película ha sido clasificada como X 18+ por la Junta de Clasificación conforme a la *Classification (Publications, Films and Computer Games) Act 1995*; o
(b) material respecto del cual se cumplen las siguientes condiciones:
(i) el material es una película o el contenido de una película;

(ii) la película no ha sido clasificada por la Junta de Clasificación conforme a la *Classification (Publications, Films and Computer Games) Act 1995*;
(iii) si la película fuese clasificada por la Junta de Clasificación conforme a dicha ley, probablemente sería clasificada como X 18+; o
(c) material respecto del cual se cumplen las siguientes condiciones:
(i) el material es una publicación o el contenido de una publicación;
(ii) la publicación ha sido clasificada como Categoría 2 restringida por la Junta de Clasificación conforme a la *Classification (Publications, Films and Computer Games) Act 1995*; o
(d) material respecto del cual se cumplen las siguientes condiciones:
(i) el material es una publicación o el contenido de una publicación;
(ii) la publicación no ha sido clasificada por la Junta de Clasificación conforme a la *Classification (Publications, Films and Computer Games) Act 1995*;
(iii) si la publicación fuese clasificada por la Junta de Clasificación conforme a dicha ley, probablemente sería clasificada como Categoría 2 restringida; o
(e) material respecto del cual se cumplen las siguientes condiciones:
(i) el material no es una película, ni el contenido de una película, ni un videojuego, ni una publicación, ni el contenido de una publicación;
(ii) si el material fuese clasificado por la Junta de Clasificación de manera equivalente a la forma en que se clasificaría una película conforme a la *Classification (Publications, Films and Computer Games) Act 1995*, probablemente sería clasificado como X 18+; o
(f) material respecto del cual se cumplen las siguientes condiciones:
(i) el material es una película o el contenido de una película;
(ii) la película ha sido clasificada como R 18+ por la Junta de Clasificación conforme a la *Classification (Publications, Films and Computer Games) Act 1995*; o
(g) material respecto del cual se cumplen las siguientes condiciones:
(i) el material es una película o el contenido de una película;
(ii) la película no ha sido clasificada por la Junta de Clasificación conforme a la *Classification (Publications, Films and Computer Games) Act 1995*;
(iii) si la película fuese clasificada por la Junta de Clasificación conforme a dicha ley, probablemente sería clasificada como R 18+; o
(h) material respecto del cual se cumplen las siguientes condiciones:
(i) el material es una publicación o el contenido de una publicación;
(ii) la publicación ha sido clasificada como Categoría 1 restringida por la Junta de Clasificación conforme a la *Classification (Publications, Films and Computer Games) Act 1995*; o
(i) material respecto del cual se cumplen las siguientes condiciones:
(i) el material es una publicación o el contenido de una publicación;
(ii) la publicación no ha sido clasificada por la Junta de Clasificación conforme a la *Classification (Publications, Films and Computer Games) Act 1995*;
(iii) si la publicación fuese clasificada por la Junta de Clasificación conforme a dicha ley, probablemente sería clasificada como Categoría 1 restringida; o
(j) material respecto del cual se cumplen las siguientes condiciones:
(i) el material es un videojuego;
(ii) el videojuego ha sido clasificado como R 18+ por la Junta de Clasificación conforme a la *Classification (Publications, Films and Computer Games) Act 1995*; o
(k) material respecto del cual se cumplen las siguientes condiciones:
(i) el material es un videojuego;
(ii) el videojuego no ha sido clasificado por la Junta de Clasificación conforme a la *Classification (Publications, Films and Computer Games) Act 1995*;
(iii) si el videojuego fuese clasificado por la Junta de Clasificación conforme a dicha ley, probablemente sería clasificado como R 18+; o
(l) material respecto del cual se cumplen las siguientes condiciones:
(i) el material no es una película, ni el contenido de una película, ni un videojuego, ni una publicación, ni el contenido de una publicación;
(ii) si el material fuese clasificado por la Junta de Clasificación de manera equivalente a la forma en que se clasificaría una película conforme a la *Classification (Publications, Films and Computer Games) Act 1995*, probablemente sería clasificado como R 18+.
Nota: Véase también la sección 160 (el Comisionado puede obtener asesoría de la Junta de Clasificación).
(2) La sección 22CF de la *Classification (Publications, Films and Computer Games) Act 1995* (relativa a la clasificación mediante una herramienta de clasificación aprobada) se aplica para los efectos de esta sección de manera equivalente a la forma en que se aplica para los efectos de dicha ley.

En materia de **ciber acoso (*cyberbullying*) contra niños**, el regulador puede investigar quejas y emitir avisos de remoción dirigidos al proveedor de un servicio de red social, servicio electrónico relevante o servicio de internet designado (secciones 30 y 31).

También puede emitir avisos de remoción a proveedores de hosting que alojen cyberbullying dirigido a un niño australiano (sección 66).

Respecto a la materia de **ciber abuso (*cyber-abuse*) contra adultos**, el regulador puede recibir quejas, investigar y emitir avisos de remoción dirigidos a plataformas, servicios electrónicos relevantes, servicios de internet designados o proveedores de hosting (secciones 36 y 37).

En relación a la materia de **imágenes íntimas no consentidas,** la ley permite que la persona afectada o quien actúe autorizadamente presente queja u objeción ante el Comisionado, y este puede considerar la emisión de un aviso de remoción (secciones 32 y 33).

En materia de ciber abuso (*cyber-abuse*), cualquier persona residente en Australia, persona jurídica que opere en Australia o entidad pública australiana puede presentar quejas sobre material clase 1 o cierto material clase 2 accesible para usuarios australianos (sección 38).

El Comisionado puede investigar de oficio o en respuesta a quejas si usuarios australianos pueden acceder a material clase 1 o clase 2, si un prestador incumplió una regla de servicio o si un participante de la industria incumplió un código o estándar aplicable (sección 42).

Para material clase 1, el regulador puede emitir avisos de remoción dirigidos a **proveedores de redes sociales**, **servicios electrónicos relevantes**, **servicios de internet designados** o **proveedores de hosting** (secciones 109 y 110).

Para material clase 2, el regulador puede emitir avisos de remoción y avisos remediales que exijan remover el material o sujetar su acceso a un sistema de acceso restringido de **servicio de redes sociales**, **servicio electrónico relevante**, **servicio de internet designado** o **proveedor de servicios de alojamiento** (secciones 114, 115, 119 y 120).

También puede emitir avisos de eliminación de enlaces dirigidos a **motores de búsqueda** y avisos de retiro de aplicaciones dirigidos a **servicios de distribución de aplicaciones** (secciones 124 y 128).

4. Regulación de contenidos y procedimientos

Como se ha descrito, la *Online Safety Act* regula diferentes tipos de contenidos y daños, entre ellos ciber acoso contra niños, ciber abuso contra adultos, imágenes íntimas no consentidas, material que representa conducta violenta aborrecible, material *class 1* y material *class 2*.

El ciber acoso (*cyberbullying*) dirigido a un niño australiano se configura cuando el material está disponible en un servicio cubierto y una persona razonable concluiría que probablemente fue destinado a afectar a un niño australiano y tendría el efecto de amenazarlo, intimidarlo, acosarlo o humillarlo gravemente (sección 6).

El ciber abuso (*cyber-abuse*) dirigido a un adulto australiano se configura cuando el material está disponible en un servicio cubierto, probablemente fue destinado a causar daño grave a un adulto australiano y una persona razonable en su posición lo consideraría amenazante, acosador u ofensivo (sección 7).

El daño grave (*serious harm*) incluye daño físico grave o daño grave a la salud mental, incluyendo daño psicológico grave o angustia grave, pero no meras reacciones emocionales ordinarias como angustia, pena, miedo o enojo (sección 5).

El material que representa conducta violenta aborrecible (*material that depicts abhorrent violent conduct*) incluye material de audio, visual o audiovisual que registra o transmite dicha conducta, siendo irrelevante si el material fue alterado (sección 9).

El material se considera proporcionado (*provided*) en un servicio de red social, servicio electrónico relevante o servicio de internet designado cuando es accesible o entregado a uno o más usuarios mediante dicho servicio (sección 10).

Asimismo, el material se considera publicado (*posted*) en un servicio de red social, servicio electrónico relevante o servicio de internet designado cuando un usuario final provoca que dicho material sea accesible o entregado a uno o más usuarios finales mediante el uso del servicio (sección 11).

Finalmente, se considera removido (*removed*) cuando ya no es accesible ni entregado a ningún usuario en Australia mediante el servicio respectivo (sección 12).

El esquema de contenidos en línea distingue entre *class 1 material* y *class 2 material*, definidos por referencia al sistema australiano de clasificación (secciones 106 y 107).

La guía regulatoria de *eSafety Commissioner* explica que los códigos y estándares cubren material *class 1* y *class 2*, desde contenidos de explotación sexual infantil y material proterrorista hasta pornografía en línea y material inadecuado para niños (eSafety Commissioner a, 2026: 8).

La guía también distingue entre material *class 1A*, *class 1B* (eSafety Commissioner a, 2026: 9) *class 1C*, *class 2A* y *class 2B* (eSafety Commissioner a, 2026: 10), lo que permite graduar las obligaciones regulatorias según la gravedad y tipo de material.

El material *class 1A* incluye explotación sexual infantil, material proterrorista y material de crimen y violencia extrema, mientras que el material *class 2* incluye pornografía en línea y otro material de alto impacto, como violencia, drogas, lenguaje o temas sensibles (eSafety Commissioner a, 2026: 9)

Los códigos y estándares se aplican a cada sección de la industria y pueden exigir medidas de prevención, detección, reporte, remoción, restricción de acceso, evaluación de riesgo y cooperación con el Comisionado de Seguridad (secciones 132 a 150).

5. Debido proceso del usuario y mecanismos de queja

Australia incorpora un sistema escalonado de quejas que, en algunos casos, exige que el usuario haya reclamado previamente ante el proveedor antes de acudir al *eSafety Commissioner* (secciones 30.4 -niños- y 36.3 -adultos-).

En ciber acoso (*cyberbullying*) contra niños, cuando se busca que el Comisionado emita un aviso de remoción dirigido al proveedor del servicio, la queja debe acompañarse de evidencia de que el material fue previamente objeto de una queja ante dicho proveedor (sección 30.4).

Si el servicio emite un número de recibo o referencia como parte de sus procesos ordinarios de quejas, el Comisionado puede exigir que la evidencia adopte esa forma (sección 30.6).

Si el servicio no emite número de referencia, el Comisionado puede exigir evidencia mediante captura de pantalla, declaración estatutaria u otra forma especificada (sección 30.7).

En ciber abuso (*cyber-abuse*) contra adultos, también se exige que la queja ante el Comisionado vaya acompañada de evidencia de que el material fue previamente reclamado ante el proveedor cuando se busca una orden de remoción contra el servicio (sección 36.3).

La guía regulatoria del *eSafety Commissioner* indica que ciertos prestadores deben derivar a eSafety las quejas no resueltas sobre incumplimiento de códigos o estándares, cuando sepan que el reclamante está insatisfecho con la forma en que se tramitó la queja o con su resultado (eSafety Commissioner a, 2026: 40)

La guía precisa que esta obligación no se satisface simplemente remitiendo al reclamante al formulario de quejas de *eSafety*, sino que el proveedor debe notificar al regulador los detalles de la queja y, en la medida de lo conocido, la razón de la insatisfacción (eSafety Commissioner a, 2026: 27)

En materia de imágenes íntimas, la persona afectada puede presentar una objeción incluso si previamente consintió la difusión de la imagen, lo que refuerza la capacidad del usuario de recuperar control sobre contenidos íntimos (sección 33.2).

La ley también permite que padres, tutores o personas autorizadas presenten quejas u objeciones en representación de niños o personas que no puedan gestionar sus propios asuntos (secciones 30.2, 32.3 y 33.3).

6. Transparencia algorítmica, recomendadores y gestión de riesgos

La guía regulatoria de *eSafety Commissioner* señala que algunos códigos y estándares diferencian los niveles de riesgo que distintos servicios pueden presentar frente a material clase 1 y clase 2, con obligaciones proporcionales al riesgo de que dicho material sea generado, accedido, distribuido o almacenado mediante el servicio (eSafety Commissioner a, 2026: 27)

Los servicios no preclasificados o definidos deben realizar su propia evaluación de riesgos o asignarse por defecto al nivel de riesgo más alto, lo que incentiva una gestión preventiva del diseño y funcionamiento del servicio (eSafety Commissioner a, 2026: 15)

Cuando un servicio realiza cambios materiales en su funcionalidad, ciertos proveedores deben reevaluar riesgos y considerar funciones o configuraciones que minimicen la posibilidad de que material clase 1 y clase 2 sea accedido, distribuido o almacenado por usuarios en Australia (eSafety Commissioner a, 2026: 19)

El documento que presenta los resultados de la consulta del *eSafety Commissioner* sobre material de autolesión destaca que los algoritmos de recomendación pueden contribuir a la proliferación de contenidos dañinos, incluso cuando los usuarios no los buscan activamente o solo han tenido una interacción mínima con ese tipo de material (eSafety Commissioner b, 2026: 14)

La misma consulta advierte que, por la naturaleza personalizada de los recomendadores, los contenidos dañinos pueden ser servidos precisamente a quienes son más susceptibles de verse afectados por ellos (eSafety Commissioner b, 2026: 15).

Respecto de IA generativa, la consulta advierte que *chatbots* u otros servicios de IA pueden contribuir a la producción y exposición de niños a material de autolesión restringido por edad, por ejemplo, mediante interacciones que validen conductas dañinas o entreguen instrucciones (eSafety Commissioner b, 2026: 15).

La guía regulatoria de eSafety incorpora además un apéndice específico (apéndice E) sobre servicios de IA generativa, incluidos motores de búsqueda integrados con IA y servicios de IA generativa de alto impacto (eSafety Commissioner, 2026 a: 69).

7. Autoridad y supervisión

De acuerdo con la Ley de Seguridad en Línea, el *eSafety Commissioner* es el eje institucional del modelo australiano, que cuenta con funciones amplias de promoción, educación, investigación, monitoreo, asesoría, elaboración de guías, cumplimiento y coordinación interinstitucional en materia de seguridad en línea (secciones 26 y 27).

El *Commissioner* puede investigar quejas presentadas por usuarios o actuar de oficio en materias del esquema de contenidos en línea, incumplimiento de reglas de servicio, incumplimiento de disposiciones sancionables e incumplimiento de códigos o estándares de industria (secciones 31, 37, 42 y 146).

La ley reconoce potestades de obtención de información, investigación y requerimiento de comparecencia o producción de documentos, lo que entrega al regulador herramientas prácticas de fiscalización (secciones 13 y 14).

En materia de contenidos, el *Commissioner* puede emitir avisos de remoción (sección 65), avisos remediales (sección 66), avisos de eliminación de enlaces (sección 88), avisos de retiro de aplicaciones (sección 128), solicitudes de bloqueo (sección 95) y avisos de bloqueo (sección 99), según el tipo de contenido y servicio involucrado.

El incumplimiento de avisos u obligaciones puede dar lugar a advertencias formales, procedimientos de sanción civil, avisos de infracción y compromisos exigibles ante tribunales (Online Safety Act, parte 10, secciones 166 y siguientes).

La guía de *eSafety Commissiner* señala que el regulador cuenta con un rango de respuestas frente al incumplimiento de códigos y estándares, desde resoluciones administrativas hasta procedimientos de sanción civil, con multas que pueden alcanzar 30.000 unidades de penalidad para individuos y cinco veces esa cifra para corporaciones (eSafety Commissioner a, 2026: 69).

Los códigos de industria pueden ser elaborados por asociaciones representativas de prestadores y registrados por el *eSafety Commissioner* cuando cumplen requisitos procedimentales y sustantivos, incluyendo salvaguardas comunitarias apropiadas (sección 140).

Si no se registra un código adecuado o concurren otras condiciones, el *Commissioner* puede dictar un estándar de industria aplicable a una sección de la industria en línea (sección 145). Los estándares prevalecen sobre códigos incompatibles, lo que permite al regulador imponer una regla pública obligatoria cuando la autorregulación sectorial es insuficiente (sección 150).

Los códigos y estándares son obligatorios y exigibles desde su entrada en vigor, salvo cuando una medida sea expresamente opcional o el prestador esté exento por su perfil de riesgo o categoría (eSafety Commissioner a, 2026: 5).

II. Principales hallazgos del análisis comparado de los modelos

Los sistemas examinados muestran una tendencia hacia el fortalecimiento de deberes de diligencia y capacidades regulatorias sobre intermediarios digitales, aunque lo hacen desde tradiciones jurídicas y modelos institucionales distintos.

Tanto la Unión Europea y sus implementaciones nacionales (España y Francia), como Brasil y Australia, reconocen que determinadas plataformas y servicios digitales no operan únicamente como intermediarios técnicos neutrales, sino como actores con capacidad efectiva de organizar, priorizar, recomendar, amplificar y restringir contenidos a gran escala. Esto explica la progresiva expansión de obligaciones relativas a moderación, cooperación con autoridades, gestión de riesgos, trazabilidad y protección reforzada frente a determinados contenidos ilícitos o dañinos.

La experiencia europea constituye un modelo estructurado de regulación de servicios digitales. El Reglamento de Servicios Digitales (DSA) establece una arquitectura basada en categorías funcionales de **intermediarios**, **plataformas**, **motores de búsqueda** y **plataformas de muy gran tamaño**, incorporando obligaciones escalonadas según el nivel de riesgo y alcance del servicio. Este modelo combina reglas de responsabilidad limitada para intermediarios con deberes de diligencia reforzada, transparencia algorítmica, sistemas de notificación y acción, gestión de riesgos sistémicos y supervisión coordinada entre autoridades nacionales y la Comisión Europea.

España y Francia representan formas distintas de implementación y adaptación de este marco común. España ha avanzado principalmente mediante mecanismos institucionales, manteniendo como base interna la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico. España tiene pendiente la implementación del Reglamento DSA, situación por la que la Comisión Europea llevó este asunto al Tribunal de Justicia de la Unión Europea. Francia, por otra parte, ha desarrollado una estrategia de integración normativa entre el Reglamento DSA y legislación nacional específica, particularmente a través de la LCEN y la SREN. El caso francés destaca por reforzar mecanismos administrativos de retiro, bloqueo y desreferenciación respecto de contenidos vinculados a terrorismo, explotación sexual infantil y pornografía accesible a menores, además de ampliar competencias regulatorias de ARCOM y establecer estándares técnicos en materias como verificación de edad. En ambos casos, sin embargo, el núcleo regulatorio continúa siendo europeo y responde a una lógica de mercado digital integrado y supervisión multinivel.

Por su parte, Brasil presenta un modelo comparativamente más garantista respecto de la libertad de expresión y la intervención estatal sobre contenidos generados por terceros. El Marco Civil de Internet mantiene como regla central que los proveedores de aplicaciones solo responden civilmente cuando incumplen una orden judicial específica de remoción, solución que busca evitar incentivos para la eliminación privada excesiva de contenidos. A diferencia del modelo europeo y australiano, la intervención judicial ocupa una posición central en el equilibrio entre libertad de expresión y responsabilidad de plataformas. No obstante, el sistema brasileño también muestra una evolución hacia mayores exigencias regulatorias, especialmente en materia de protección de niños, niñas y

adolescentes, perfilamiento, sistemas de recomendación y diseño seguro de servicios digitales. Asimismo, la Ley General de Protección de Datos introduce mecanismos de revisión de decisiones automatizadas y control sobre tratamiento algorítmico de datos personales, incorporando una dimensión de debido proceso algorítmico menos desarrollada en otros modelos examinados.

Australia, por su parte, representa un modelo orientado a seguridad digital y gestión administrativa de riesgos. Su modelo se estructura sobre potestades regulatorias amplias del *eSafety Commissioner* para investigar, emitir avisos de remoción, ordenar bloqueos, exigir medidas preventivas y supervisar códigos y estándares obligatorios para distintos sectores de la industria digital. El sistema australiano, a diferencia de los anteriores, regula categorías de daño (ciberacoso, abuso, explotación sexual, material violento extremo o contenidos restringidos por edad) e incorpora una lógica de gestión de riesgos sistémicos, particularmente respecto de sistemas de recomendación, funcionalidades algorítmicas y servicios de inteligencia artificial generativa.

Desde una perspectiva comparada, existen diferencias relevantes en el equilibrio entre intervención administrativa y control judicial. El modelo brasileño privilegia una autorización judicial previa para la remoción de contenidos, mientras que el modelo europeo -especialmente en Francia- y el australiano permiten actuaciones administrativas inmediatas frente a determinadas categorías de contenido consideradas especialmente graves. En contrapartida, Francia y Australia contemplan mecanismos posteriores de revisión judicial y procedimientos relativamente expeditos de reclamación o impugnación.

Asimismo, los modelos difieren en el nivel de institucionalización de la supervisión digital. La Unión Europea ha construido un esquema de coordinación entre autoridades nacionales y Comisión Europea. Francia y Australia cuentan con reguladores especializados con potestades claras y capacidades sancionatorias; mientras que Brasil mantiene un sistema fragmentado entre tribunales, autoridades de protección de datos, órganos de consumo e institucionalidades sectoriales.

Los casos examinados evidencian una preocupación transversal por los efectos de los sistemas algorítmicos y de recomendación en la exposición a contenidos dañinos, especialmente respecto de niños, niñas y adolescentes. Sin embargo, el tratamiento varía considerablemente. El DSA europeo aborda esta cuestión mediante obligaciones de transparencia y gestión de riesgos sistémicos; Francia complementa esas obligaciones con regulaciones sectoriales sobre verificación de edad; Brasil conecta el problema con protección de datos, perfilamiento y diseño seguro; y, Australia lo aborda desde una lógica de seguridad digital y prevención de daños, incluyendo referencias a inteligencia artificial generativa y recomendaciones automatizadas.

ANEXO: Tabla comparativa de modelos regulatorios de plataformas digitales

Jurisdicción	Modelo regulatorio	Tipos de prestadores regulados	Régimen de responsabilidad	Regulación de contenidos y procedimientos de notificación	Debido proceso del usuario	Transparencia algorítmica y sistemas de recomendación	Autoridades y supervisión
Unión Europea	Modelo horizontal basado en obligaciones de diligencia debida y gestión de riesgos	Servicios intermediarios, hosting, plataformas en línea y motores de búsqueda	Exenciones condicionadas y obligaciones diferenciadas según el tipo de servicio	Sistemas de notice and action, remoción de contenidos ilícitos y mitigación de riesgos sistémicos	Derechos de reclamación y mecanismos de recurso frente a decisiones de plataformas	Obligaciones de transparencia respecto de publicidad, algoritmos y sistemas de recomendación	Coordinadores de Servicios Digitales y Comisión Europea
Francia	Implementación nacional del DSA complementada con institucionalidad sectorial	Prestadores de servicios digitales y plataformas en línea	Aplicación del régimen de responsabilidad previsto en el DSA	Facultades de investigación, requerimientos de cese y restricciones temporales de acceso	Aplicación de garantías procedimentales derivadas del DSA	Supervisión vinculada a obligaciones del DSA y protección de usuarios	Arcom, CNIL y DGCCRF
España	Implementación nacional del DSA mediante autoridades administrativas competentes	Prestadores intermediarios y plataformas digitales	Régimen previsto en el DSA	Mecanismos de cumplimiento y coordinación institucional para remoción y supervisión	Garantías derivadas del DSA	Aplicación del régimen europeo de transparencia	Autoridades nacionales competentes y Coordinador de Servicios Digitales

Australia	Modelo de seguridad en línea basado en riesgos y categorías de contenidos dañinos	Redes sociales, servicios electrónicos relevantes y servicios de internet designados	Régimen regulatorio basado en obligaciones de remoción y cumplimiento	Procedimientos de notice y take down; regulación de material class 1 y class 2	Mecanismos administrativos y revisión regulatoria	Menor desarrollo de obligaciones generales de transparencia algorítmica	eSafety Commissioner
Brasil	Modelo centrado en responsabilidad posterior y control judicial	Aplicaciones de internet y plataformas digitales	Responsabilidad condicionada principalmente a orden judicial	Remoción de contenidos en casos específicos y protección de libertad de expresión	Centralidad del control judicial y garantías procesales	Desarrollo limitado en transparencia algorítmica	Poder Judicial y autoridades sectoriales

Referencias

Referencias generales

Arcom (s.f.). 5 informations à retenir sur le Règlement sur les services numériques (RSN) ou Digital Services Act (DSA). Disponible en: https://c.bcn.cl/5Kkorv (mayo, 2026).

CNMC (2024). El Ministerio para la Transformación Digital y de la Función Pública designa a la CNMC como Coordinador de Servicios Digitales de España. Disponible en: https://c.bcn.cl/YpftvE (mayo, 2026).

- (s.f.) Servicios digitales. Disponible en: https://c.bcn.cl/K2Jh7n (mayo, 2026).

Comisión Europea (2026). La Ley de Servicios Digitales. Disponible en: https://c.bcn.cl/NtPBm7 (mayo, 2026).

- (s.f.). Decisiones sobre infracciones. Disponible en: https://c.bcn.cl/JqxlTU (mayo, 2026).
- (2025). La Comisión decide llevar a CHEQUIA, ESPAÑA, CHIPRE, POLONIA y PORTUGAL ante el Tribunal de Justicia de la Unión Europea debido a la falta de aplicación efectiva del Reglamento de Servicios Digitales. Disponible en: https://c.bcn.cl/AtDmv6 (mayo, 2026).

eSafety Commissioner (2026 a). Online Safety Codes and Standards. Regulatory Guidance. Disponible en: https://c.bcn.cl/vAQbmZ (mayo, 2026).

- (2026 b). Self-harm material consultation summary. Age-Restricted Material Codes. Disponible en: https://c.bcn.cl/UDn5r5 (mayo, 2026).

EUR-lex (s.f.). Reglamento. Disponible en: https://c.bcn.cl/nK62Eo (mayo, 2026).

Europa press (2026). El Congreso decide este martes si tramita una ley para habilitar a la CNMC como coordinador de servicios digitales. Disponible en: https://c.bcn.cl/WTbu4S (mayo, 2026)

Gobierno de Brasil (2026). *Governo do Brasil regulamenta o ECA Digital: novo marco na proteção de crianças e adolescentes na internet*. Disponible en: https://c.bcn.cl/nHWn4X (mayo, 2026).

- (s.f.). Fale conozco Agência Nacional de Proteção de Dados. Disponible en: https://c.bcn.cl/r05F8E (mayo, 2026).

Referencias normativas

Australia

- Online Safety Act (2021). Disponible en: https://c.bcn.cl/wusQOe (mayo, 2026).

Brasil

- Ley N° 12.965 (2014). Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponible en: https://c.bcn.cl/U5NKOa (mayo, 2026).
- Ley N° 13.709 (2018). Lei Geral de Proteção de Dados Pessoais (LGPD). Disponible en: https://c.bcn.cl/XsiTLK (mayo, 2026).
- Ley N° 15.211 (2025). Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Disponible en: https://c.bcn.cl/C4n7Em (mayo, 2026).

España

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Disponible en: https://c.bcn.cl/YG36BA (mayo, 2026).
- Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual. Disponible en: https://c.bcn.cl/XplaCm (mayo, 2026).
- Resolución de 22 de enero de 2025, del Congreso de los Diputados, por la que se ordena la publicación del Acuerdo de derogación del Real Decreto-ley 9/2024, de 23 de diciembre, por el que se adoptan medidas urgentes en materia económica, tributaria, de transporte, y de Seguridad Social, y se prorrogan determinadas medidas para hacer frente a situaciones de vulnerabilidad social. Disponible en: https://c.bcn.cl/eYK6Dx (mayo, 2026).

Francia

- LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique. Disponible en: https://c.bcn.cl/51YCCC (mayo, 2026).
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Disponible en: https://c.bcn.cl/PvkqOj (mayo, 2026).

Unión Europea

Parlamento Europeo y del Consejo

- (2000), Directiva 2000/31/CE del Parlamento 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). Disponible en: https://c.bcn.cl/439hMf (mayo, 2026).
- (2022). Reglamento (UE) 2022/2065 del relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) Disponible en: https://c.bcn.cl/IbK7E6 (mayo, 2026).
- (2022). Reglamento (UE) 2022/1925 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). Disponible en: https://c.bcn.cl/SHRVIP (mayo, 2026).

Nota aclaratoria

Asesoría Técnica Parlamentaria, está enfocada en apoyar preferentemente el trabajo de las Comisiones Legislativas de ambas Cámaras, con especial atención al seguimiento de los proyectos de ley. Con lo cual se pretende contribuir a la certeza legislativa y a disminuir la brecha de disponibilidad de información y análisis entre Legislativo y Ejecutivo.

Creative Commons Atribución 3.0 (CC BY 3.0 CL)