GARRIGUES

Guía práctica de implementación del Reglamento de Servicios Digitales

El Reglamento de Servicios Digitales (DSA)

Presentamos nuestra "**Guía práctica de implementación del Reglamento de Servicios Digitales**" en la que explicamos cuáles son las principales novedades introducidas por dicha norma.

El Reglamento UE 2022/2065, relativo a un mercado único de servicios digitales ("Reglamento de Servicios Digitales" o "DSA") por el que se modifica la Directiva 2000/31/CE, tiene como principal objetivo contribuir a la creación de **un Internet más seguro, predecible y fiable y en el que se protejan los derechos fundamentales**.

La norma se centra en definir un marco unificado sobre cuál es la responsabilidad de los prestadores de servicios intermediarios (redes sociales, *marketplaces,* buscadores, etc.), a los que impone normas de diligencia debida dependiendo del tipo de servicios que prestan y su tamaño.

Nuestro objetivo es ayudar tanto a los prestadores de servicios intermediarios como a los titulares de contenidos a hacer uso de este nuevo marco para, entre todos, conseguir la eliminación de contenido ilícito en Internet sin afectar los derechos fundamentales de los ciudadanos y empresas.

Para ayudarte en la lectura de esta Guía, cada vez que encuentres un signo "**Q**" puedes hacer clic para moverte en el documento y obtener información adicional.

Índice

MÓDULO A

¿Qué servicios digitales están afectados por el Reglamento?

1. ¿Cuándo será aplicable el Reglamento de Servicios Digitales?

Ya. El Reglamento de Servicios Digitales será de aplicación general a partir del 17 de febrero de 2024.

Algunas normas vienen siendo exigibles desde agosto de 2023 en relación con determinadas obligaciones aplicables a “plataformas en línea de muy gran tamaño” (“**VLOP**”) y a los “motores de búsqueda en línea de muy gran tamaño” (“**VLOSE**”) **[Q4]**.

Se trata de un texto vivo y complejo que se complementa con normas adicionales publicadas por la Comisión Europea para hacer efectiva su aplicación.

Calendario

2022

23 abril
Acuerdo político sobre la DSA

27 octubre
Publicación DSA en DOUE

16 noviembre
Entrada en vigor

2023

17 Febrero
PL obligadas a publicar su número de usuarios activos

Marzo - abril
CE debe designar VLOP

Julio - Agosto
Son exigibles las normas aplicables VLOP (4 meses desde notificación de la designación)

31 Agosto
Comunicación a la CE de estados financieros para el cálculo de la tasa anual

20 octubre
Recomendación CE para la Red Informal de CSD

31 Diciembre
Pago tasa anual de supervisión VLOP/VLOSE

2024

8 febrero
Las VLOP/VLOSE deberán facilitar a la CE la información solicitada en relación con el cumplimiento de sus obligaciones y rendición de cuentas

17 febrero
Designación CSD por EE. MM.
Aplicación general de la norma

2025

17 febrero
KYC exigible para todos los comerciantes

2. ¿Cuáles son los objetivos del Reglamento de Servicios Digitales?

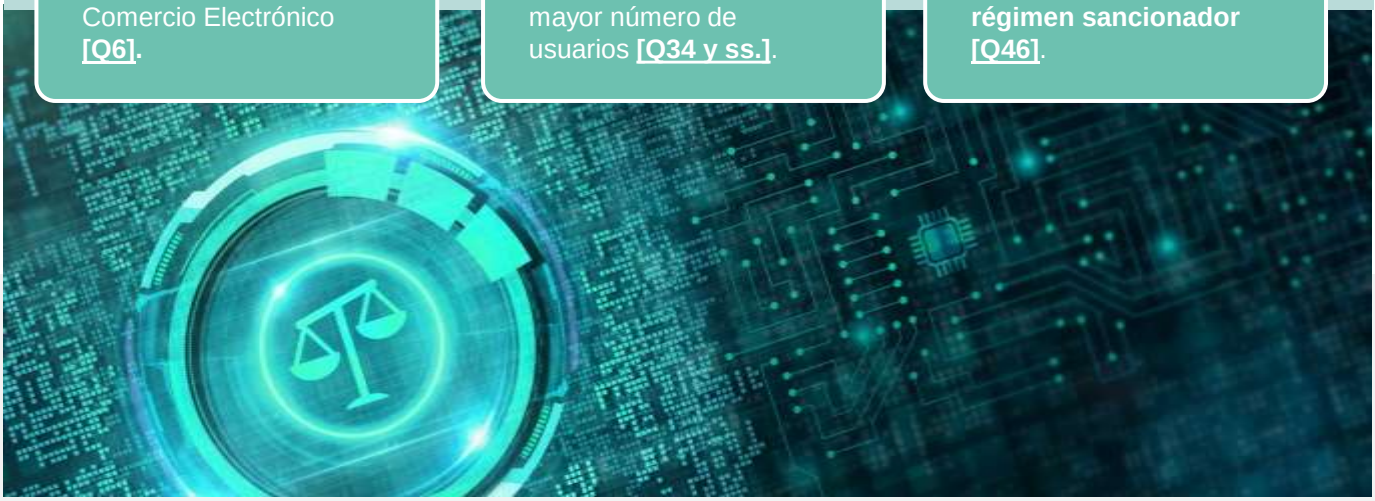
El objetivo principal del Reglamento es garantizar un entorno en línea seguro, predecible y fiable que proteja los derechos de los usuarios y, al mismo tiempo, contribuya al correcto funcionamiento del mercado interior y favorezca la innovación. Dicho de otro modo, **prevenir las actividades ilegales y nocivas en línea y la difusión de desinformación.**

Para cumplir con este objetivo se establecen normas armonizadas en los siguientes ámbitos:

1. Condiciones para la exención de responsabilidad de los prestadores de servicios intermediarios ("**PSSI**") que, en general, conserva los principios de la Directiva 2000/31/CE del Comercio Electrónico **[Q6]**.

2. Obligaciones de transparencia y diligencia debida de carácter progresivo. Esto significa que se imponen mayores obligaciones a los PSSI que están más cerca del usuario y a los que tienen mayor número de usuarios **[Q34 y ss.]**.

3. Reforzar la supervisión y ejecución de sus obligaciones mediante la designación de **nuevos organismos de supervisión y control [Q45]**, así como la creación de un **nuevo régimen sancionador [Q46]**.



Hay que tener en cuenta que la DSA no define qué es un contenido ilícito. Dependerá de la normativa aplicable a nivel nacional o de la UE. Esto implica que pueden existir diferencias entre Estados dependiendo de su normativa interna. Hay áreas en las que existe un consenso generalizado, como sucede con el contenido terrorista o la pornografía infantil. Otros contenidos pueden generar más dudas como sucede, por ejemplo, con el llamado "discurso del odio".

Cuando un contenido es ilegal solo en un Estado, la regla general es que solo deberá eliminarse o hacerse inaccesible en ese Estado de cara a reducir su impacto en otros derechos fundamentales.

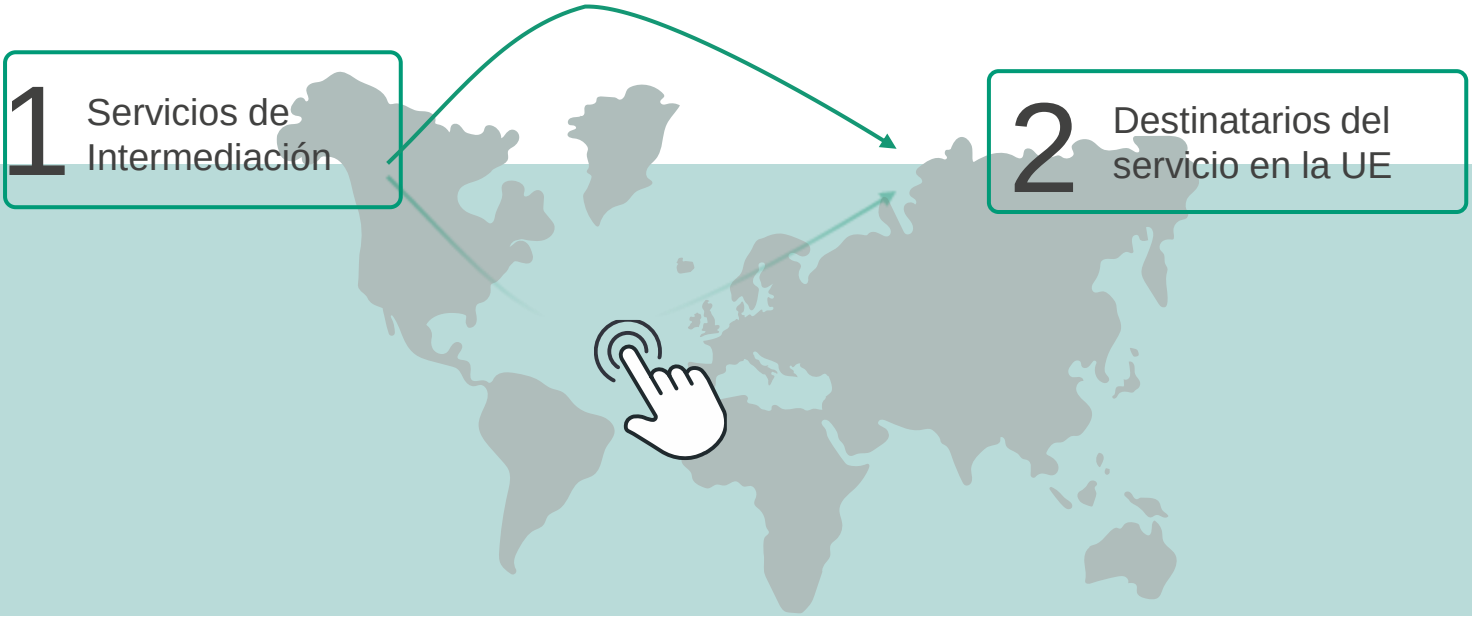
3. ¿Cuál es el ámbito territorial del Reglamento de Servicios Digitales?

La DSA se aplicará a todos los PSSI que tengan una **conexión sustancial** con la UE, independientemente del país en el que estén localizados.

¿Cuándo puede considerarse que existe una **conexión sustancial** con la UE?

1. Cuando el PSSI tenga un establecimiento en la UE; o
2. Cuando el número de destinatarios del servicio en uno o varios Estados sea significativo en relación con su población; o
3. Cuando se orienten actividades hacia uno o más Estados miembro lo que debe determinarse atendiendo a factores como el uso de una lengua o una moneda utilizados en ese Estado, la posibilidad de entrega de productos o servicios en ese Estado (p. ej. código postal) o el registro y uso de nombres de dominio de primer nivel (p. ej. *.es, .it,* etc.).

Por otro lado, y como viene siendo tradicional en materia de conflictos territoriales en Internet, la **mera accesibilidad al servicio** no es un factor de conexión suficiente para que la DSA resulte de aplicación.



Si el PSSI no tiene domicilio en un Estado miembro pero el Reglamento le resulta exigible por la aplicación de otros criterios, tiene que nombrar un **representante legal** [Q12], tal y como ya hacen muchas empresas como parte de sus obligaciones derivadas de otros instrumentos jurídicos.

4. ¿Qué servicios están afectados por el Reglamento? (ámbito objetivo)

El Reglamento de Servicios Digitales se aplica a los prestadores de servicios intermediarios, que se clasifican en tres categorías dependiendo del tipo de servicios de intermediación que prestan y de sus funcionalidades técnicas:

Servicios de "mera transmisión"

Se trata de servicio relacionados con la infraestructura de red, como los proveedores de acceso a Internet, los registradores de nombres de dominio, las autoridades de certificación, etc.

Servicios de "memoria chaché"

Son servicios que almacenan la información de forma temporal. Aquí se ubican, por ejemplo, los llamados proveedores de CDN (*Content Delivery Network*). Se trata de empresas que utilizan la memoria cache para almacenar contenido estático de sitios web en múltiples ubicaciones geográficas para acelerar su entrega a los usuarios.

Servicios de "alojamiento de datos"

Son servicios de almacenamiento de contenidos facilitados por el destinatario del servicio y a petición de éste, como la computación en nube o el alojamiento web. Dentro de estos, el Reglamento distingue entre:

a. **Plataformas en línea**: se trata de servicios que además de alojar los contenidos, los **difunden al público**, por lo que no se trata de mero almacenamiento —siempre que esa difusión no sea una característica menor o meramente accesoria y auxiliar al servicio principal—.
b. **Mercados digitales o en línea**: se trata de plataformas que, además, permiten que los consumidores celebren contratos a distancia con los comerciantes.
c. **Motores de búsqueda**: se trata de servicios que permiten a los usuarios introducir consultas para hacer búsquedas.

Además, las plataformas y motores de búsqueda también se clasifican atendiendo a su tamaño y, en aquellos casos en los que excedan de los 45 millones de destinatarios, pasan a ser plataformas en línea o buscadores de muy gran tamaño ("VLOP" y "VLOSE" por sus siglas en inglés), con las obligaciones que esto conlleva.

¿Qué significa difusión al público?

Que la información se ponga a disposición de un número **potencialmente ilimitado de personas**, es decir, que la información sea fácilmente accesible para los destinatarios del servicio en general, sin necesidad de que el destinatario del servicio que proporciona la información haga nada más, con independencia de si dichas personas acceden efectivamente a la información en cuestión. Por tanto, cuando el acceso a la información requiera la inscripción o la admisión en un grupo de destinatarios del servicio, solo debe considerarse que dicha información ha sido difundida al público cuando los destinatarios del servicio que deseen acceder a la información se inscriban o sean admitidos automáticamente sin que un ser humano decida o escoja a quién se concede el acceso.

El 25 de abril de 2023, la Comisión Europea designó 17 plataformas en línea como VLOP y 2 motores de búsqueda en línea como VLOSE (pulsa **aquí** para más información). Dichos servicios contaban con un plazo de 4 meses para su adaptación (25 de agosto de 2023). El 20 de diciembre, la Comisión adoptó un segundo conjunto de decisiones y designó otras tres plataformas en línea de muy gran tamaño (pulsar **aquí** para más información). La Comisión publicó el 18 de enero de 2024 un resumen sobre las plataformas designadas y las principales actividades de control (pulsa **aquí** para más información). Asimismo, están pendientes de resolución las demandas presentadas por **Zalando** y **Amazon** ante el Tribunal de Justicia de la Unión Europea ("**TJUE**") impugnando la clasificación de sus servicios como VLOP.

5. ¿Cómo se calcula el promedio mensual de destinatarios del servicio activos?

Para saber su una plataforma o un buscador exceden el umbral de 45 millones de usuarios que aplica la Comisión Europea para determinar que son “de muy gran tamaño” debe atenderse al “promedio mensual de destinatarios del servicio activos” o “AMAR” por sus siglas en inglés. Es importante tener en cuenta que **el AMAR debe calcularse para cada servicio considerado individualmente**, y no de forma global.

Para realizar este cálculo es importante tener en cuenta que el concepto de “destinatarios del servicio activos” no es el mismo que el de “destinatarios del servicio”, ya que exige cierto grado de involucración con el servicio incluyendo:

- Todos los destinatarios que participan en el servicio **al menos una vez en el periodo de 6 meses.**
- En las **plataformas con múltiples caras**, serán relevantes los destinatarios de todas ellas (consumidores, profesionales).
- **Acceden desde el territorio de la UE** (¿localizaciones ocultas?).
- **Expuestos a información difundida** en la interfaz de la plataforma en línea (viendo, escuchando, *scrolling over*), no solo usuarios activos.
- **¡No exige registro!** No coincide con usuario registrado y **no es necesario comprar** el producto/servicio.
- **¡No equivale a visitas!** Deberán ser, en la medida de lo posible, **usuarios únicos del servicio.**

Una vez que tenemos determinado el número de usuarios “activos” ya podemos aplicar la siguiente fórmula para calcular el AMAR:

AMAR = Usuarios únicos en el territorio UE - Visitas no auténticas

- El uso de diferentes interfaces por un mismo usuario (sitios web o *apps*), debe contarse una sola vez (desduplicar).
- El acceso desde distintas URL o dominios por un mismo usuario (.com, .es o .pt) debe contarse una sola vez (desduplicar).

- Deberán descontarse los usos incidentales por parte de destinatarios de servicios de terceros (indexación).
- Deberán descontarse los usuarios automatizados (*bots*, extractores de información).

Para más información sobre la identificación y contabilización de destinatarios del servicio activos, véase el informe de Preguntas y respuestas de la Comisión.

En esta web puedes confirmar los servicios ya designados por la Comisión Europea: **https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413**

Son los propios PSSI los que deben calcular su AMAR promedio de los últimos seis meses y publicarlo en una sección de su interfaz en línea accesible por el público. No obstante, es la Comisión Europea la encargada de designar qué prestadores deben ser considerados VLOP/VLOSE, pudiendo atender a otros datos además de los proporcionados por el PSSI.

MÓDULO B

Régimen de responsabilidad

6. ¿Cuál es el régimen de responsabilidad de los prestadores de servicios intermediarios bajo en nuevo Reglamento?

Se trata de una de las cuestiones clave del Reglamento, ya que se centra en determinar cuándo los PSSI pueden llegar a ser responsables por los contenidos de sus usuarios.

En líneas generales, el Reglamento mantiene el régimen de responsabilidad que la Directiva 2000/31/CE de Comercio Electrónico ya preveía para los prestadores intermediarios, que se basa en el establecimiento de un puerto seguro (*safe harbor*) para protegerlos de las consecuencias de transmitir y/o alojar contenido ilícito de sus usuarios.

Como **requisito previo**, el PSSI debe ser un **intermediario**, en el sentido de que no es responsable editorial del contenido. Es decir, su rol respecto de la información que le proporcionan sus usuarios debe ser **meramente técnico, neutral y automático** (pasivo).

No siempre es fácil determinar si un PSSI actúa o no como mero intermediario, pero el Reglamento nos da algunas pistas. Por ejemplo, el hecho de que el PSSI indexe automáticamente la información cargada en su servicio, ofrezca sistemas que impiden la identificación del usuario, tenga funciones de búsqueda o recomiende contenidos basándose en los perfiles de sus usuarios no le confiere un rol activo ni afecta a su puerto seguro.

¿Qué indicadores ha establecido la Comisión Europea para determinar si la plataforma actúa como un mero PSSI?

Indicador	Proveedor del servicio subyacente	Proveedor de servicios intermediario
Precio	Fija el precio final	Recomienda el precio final o deja libertad absoluta de elección.
Términos y condiciones	Establece los términos y condiciones del servicio	Establece los términos y condiciones de uso de la plataforma
Activos	Titular de los activos clave para la prestación del servicio	Activos propiedad o bajo el control de los usuarios
Gastos y riesgos	Sufraga los gastos y asume todos los riesgos	Los usuarios prestadores de servicios actúan por su propia cuenta y riesgo
Relación con el prestador del servicio	Relación laboral entre la plataforma y la persona que presta el servicio	Inexistencia de relación laboral
Gestión de calidad	Verificación y gestión directa de la calidad de los servicios subyacentes	Establecimiento de mecanismos de *rating* para la evaluación del servicio y servicios postventa.

- STJUE **Google France** de 23 de marzo de 2010 (asuntos C-236/08 y C-238/08)
- STJUE **eBay** de 12 de julio de 2011 (asunto C-324/09)
- SAP de Madrid **Youtube** n.º 5057/2014, de 14 de enero
- STJUE **Uber** de 20 de diciembre de 2017 (asunto C-434/15)
- STJUE **AirBnB**, de 19 de diciembre de 2019 (asunto C-390/18)
- STJUE **Coty v Amazon** de 2 de abril de 2020 (asunto C-567/18)

Cumplido este requisito previo, las condiciones para que los PSSI puedan mantener su exención de responsabilidad dependen del tipo de servicio que presten:

Servicios de "mera transmisión"

No serán responsable de la información transmitida si: (i) no han iniciado la transmisión; (ii) no han seleccionado al receptor; y (iii) no han seleccionado ni modificado la información.

Servicios de "memoria chaché"

No serán responsables por el almacenamiento automático, provisional y temporal de la información transmitida si: (i) no modifican la información; (ii) cumplen con las condiciones de acceso a la información; (iii) cumplan con las normas relativas a la actualización de la información; (iv) no interfieran en la utilización lícita de la tecnología; y (v) actúen con **prontitud [Q8]** para retirar el contenido ilícito cuando tenga **conocimiento efectivo [Q7]** de que la información contenida en la fuente inicial de transmisión ha sido retirado de la red; se ha bloqueado su acceso al mismo; o una autoridad judicial o administrativa ha ordenado retirarla o bloquearla.

Servicios de "alojamiento de datos"

No serán responsables por la información almacenada a petición de los usuarios si: (i) no tienen **conocimiento efectivo de una actividad ilícita o de un contenido ilícito [Q7]**; y (ii) en caso de tenerlo, actúen con **prontitud [Q8]** para retirar o bloquear el acceso al contenido ilícito.

La DSA sigue manteniendo la **prohibición de imponer a las plataformas una obligación general de monitorización** de los contenidos subidos por los usuarios, pilar fundamental para el desarrollo de los negocios digitales. Es decir, estas plataformas no tienen una obligación de verificar *ex ante* la legalidad de los contenidos subidos por los usuarios.

En el caso de los mercados digitales en los que el servicio consiste en facilitar la interacción directa entre compradores y vendedores, el *marketplace* debe dejar claro a los usuarios que el producto o servicio en cuestión está prestado por un tercero **[Q30]**. El objetivo es no inducir a error a los consumidores para que piensen que el servicio viene ofertado por la propia plataforma, dejando claro en todo momento quién es el vendedor del producto en cuestión. Si no se cumple con este requisito de información y transparencia, el *marketplace* podría acabar siendo responsable por el contenido alojado por sus usuarios.

7. ¿Cuándo tiene el PSSI "conocimiento efectivo de una actividad o contenido ilícito"?

Al no existir una obligación de supervisión de los contenidos alojados por los usuarios, los PSSI no estarán obligados a actuar contra un contenido ilícito hasta que no tengan **conocimiento efectivo** de que, en efecto, se trata de un contenido ilícito.

Determinar cuándo surge el conocimiento efectivo ha sido una de las cuestiones más debatidas por los tribunales de los distintos EE. MM. No siempre es fácil determinar cuándo un contenido denunciado es realmente ilícito. Por ejemplo, existe un consenso generalizado cuando lo que se solicita es que se retiren videos que contienen pornografía infantil o falsificaciones burdas. No sucede lo mismo con otros contenidos en los que la ilicitud no es obvia, como sucede, por ejemplo, con contenidos que vulneran el derecho al honor o la intimidad, que podrían estar protegidos por las libertades de expresión e información de la persona que los publica.

El Reglamento introduce una herramienta muy útil para determinar cuándo surge el conocimiento efectivo, ya que el PSSI deberá poder determinar que el contenido es **manifiestamente ilícito sin un examen jurídico detallado**.

Vías por las que el PSSI puede adquirir conocimiento efectivo de la existencia de un contenido ilícito

- Denuncias realizadas por los usuarios
- Recepción de una orden de una autoridad competente
- Investigaciones realizadas por el propio prestador

Lo que no es suficiente es el mero hecho de que (i) el prestador sea consciente, de manera general, de que su servicio se utiliza para almacenar contenidos ilícitos; (ii) el prestador indexe automáticamente la información cargada en su servicio; o (iii) el prestador tenga una función de búsqueda y recomiende información basándose en los perfiles o preferencias de los destinatarios del servicio.

Actuación ante una notificación de una autoridad para la retirada de contenido ilícito

1 Verificación

Verificar que la orden recibida (p. ej., oficios, requerimiento administrativo, etc.) cumple con los requisitos mínimos, que incluyen:

- ☐ Fundamento jurídico: norma que justifica la retirada.
- ☐ Motivación: razones por las que se solicita la retirada de ese contenido, y en qué norma se sustenta (p. ej., 248 Código Penal).
- ☐ Identificación: debe constar qué autoridad emite la orden; p. ej., Juzgado de Instrucción núm. 5 de Madrid.
- ☐ Territorio: la orden debe identificar el territorio afectado (p.ej., España).
- ☐ Localización: debe identificarse de forma clara el contenido cuya retirada se está solicitando; p. ej., dirección URL, referencia, etc.
- ☐ Recurso: debe informar al PSSI y al titular del contenido afectado de cuáles son sus posibilidades de recurrir la orden para no tener que quitar el contenido.
- ☐ Responsable: la orden también debe informar de cuál será la autoridad a la que debe trasladarse la información sobre el curso dado a las órdenes. Es decir, a quién debe informar el PSSI en relación con su decisión de retirar (o no retirar).

2 Recepción

Debe haberse recibido en el Punto de Contacto Único, y en una de las lenguas que el PSSI declara conocer.

3 Decisión

Decidir si se procede o no a la retirada.

4 Reporte

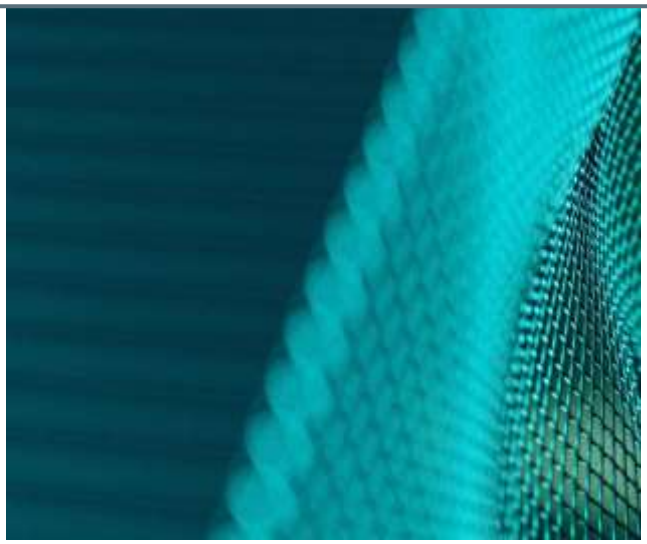
Tomada la decisión, informar al responsable indicado en la orden, **sin dilación indebida**, del curso dado a la solicitud de retirada.

5 Comunicación al usuario afectado

Informar al usuario afectado por la retirada del contenido, a menos que la orden lo impida. Puede informarse bien en el momento en el que se procede a la retirada, o bien en el momento en que indique la autoridad emisora de la orden. Deben indicarse: (i) los motivos, a menos que la orden lo prohíba; (ii) las vías de recurso, que serán las indicadas en la orden; y (iii) el ámbito territorial.

El **Código de Conducta para la Lucha contra la Incitación Ilegal al Odio en Internet** es una iniciativa conjunta de las empresas TI (YouTube, Microsoft, Twitter y Facebook) y la Comisión Europea que establece pautas y compromisos para las plataformas en línea con el propósito de luchar contra la propagación de la incitación ilegal al odio en Internet. Uno de sus aspectos clave es la obligación de las plataformas de eliminar contenido ilegal que incite al odio dentro de un **plazo máximo de 24 horas después de recibir una notificación**. Esta medida busca abordar de manera eficiente y rápida la presencia de contenido perjudicial en la red, promoviendo un entorno digital más seguro y respetuoso.

Otros tipos de contenidos ilícitos pueden requerir plazos más largos o más cortos para el tratamiento de las notificaciones, que dependerán de los hechos, las circunstancias y los tipos de contenidos ilícitos de que se trate.



8. ¿Qué significa actuar con “prontitud” en la retirada o bloqueo del contenido ilícito?

Una vez que el PSSI tiene conocimiento efectivo de la existencia de un contenido ilícito aún puede beneficiarse de su “puerto seguro” si actúa con “prontitud” para retirarlo o hacerlo inaccesible. El Reglamento no define qué es actuar con prontitud, pero sí ofrece ciertas orientaciones basadas en el tipo de contenido que se denuncia y la urgencia de tomar medidas. Por ejemplo:

1. Se espera una respuesta más rápida cuando se notifiquen contenidos que puedan suponer una amenaza para la vida o la seguridad de las personas lo que puede suceder, por ejemplo, en contextos como el vivido en la pandemia de la COVID-19 y la difusión de información falsa.

2. Se espera una respuesta más rápida en relación con contenidos pornográficos, especialmente los relacionados con la ciberviolencia, con el objetivo de proteger a las víctimas. Entre estos contenidos, estarían las relaciones no consentidas o la difusión de *deepfakes* de contenido sexual.

3. Se espera que la retirada de otro tipo de contenidos pueda exigir plazos más largos.

Existen además otras normas que sí establecen plazos recomendados para la retirada de ciertos tipos de contenido. Por ejemplo, el Código de Conducta para la lucha contra la incitación ilegal al odio en Internet de 2016 establece un plazo orientativo de 24 horas para tratar notificaciones válidas que solicitan la eliminación de este tipo de contenidos.

9. ¿Deben cooperar los PSSI con las autoridades nacionales?

Sí, los PSSI deberán cooperar con las autoridades nacionales para la retirada de contenidos ilícitos y/o para facilitar información sobre sus usuarios del servicio.

Es necesaria una orden válidamente emitida por las autoridades judiciales o administrativas competentes, en una lengua que el PSSI declare conocer, que debe contener al menos la siguiente información:

- Referencia al fundamento jurídico de la orden.
- Motivación de la retirada o de la solicitud de información.
- Identificación de la autoridad emisora de la orden.
- Territorio afectado.
- Identificación clara de dónde se encuentra el contenido, por ejemplo, la dirección URL o que permita identificar al destinatario del servicio.
- Posibles vías de recurso.
- Autoridades a las que trasladar la información.

La orden sólo será vinculante si se cumplen los requisitos anteriores y se limita a lo estrictamente necesario para alcanzar su objetivo, incluyendo su ámbito territorial.

El PSSI debe decidir si procede o no la retirada y en ese caso, informar al emisor de la orden, **sin dilación indebida**, del curso dado a la solicitud de retirada.

El PSSI también debe informar al usuario afectado y, a menos que la Ley lo impida, informarle de los motivos de la retirada, las vías de recursos de las que dispone y el ámbito territorial de la orden.

MÓDULO C

Obligaciones de diligencia debida

10. Mapa de obligaciones de diligencia debida

El Reglamento se sustenta en un régimen estratificado de responsabilidad en función del tipo de servicio y el tamaño del prestador. Se trata, además, de obligaciones cumulativas. En la siguiente tabla puedes navegar por las distintas obligaciones de diligencia debida aplicables a los PSSI.

	Art.	Obligaciones de diligencia debida	Intermediación	Alojamiento	Plataformas	VLOP
[Q11]	11-12	Puntos de contacto				
[Q12]	13	Designación de un representante legal				
[Q13]	14	Términos y condiciones de uso				
[Q14]	15, 24	Obligaciones de transparencia				
[Q15]	16	Mecanismos de notificación y acción e información a los usuarios (NTD)				
[Q19]	17	Declaración de motivos				
[Q20]	18	Notificación de sospechas de delitos				
[Q21]	20	Sistema interno de gestión de reclamaciones				
[Q21]	21	Resolución extrajudicial de litigios				
[Q23]	22	Canal de denuncias para alertados fiables				
[Q24]	23	Medidas de protección contra usos indebidos de los servicios				
[Q19]	24	Obligaciones de transparencia para plataformas				
[Q25]	25	Diseño y organización de interfaces en línea				
[Q26]	26	Publicidad en las plataformas en línea				
[Q28]	27	Transparencia de los sistemas de recomendación				
[Q29]	28	Medidas de protección a los menores				
[Q30]	30	Trazabilidad de vendedores				
[Q32]	31	Cumplimiento desde el diseño				
[Q33]	32	Obligaciones de información al consumidor sobre productos ilícitos				
[Q34]	34	Detección, análisis y evaluación de riesgos sistémicos				
[Q34]	35	Aplicación de medidas de reducción de riesgos				
[Q44]	36, 48	Mecanismos de respuesta a las crisis				
[Q38]	37	Auditorías independientes				
[Q40]	38	Sistemas de recomendación				
[Q40]	39	Requisitos de transparencia adicionales sobre la publicidad en línea				
[Q41]	40	Acceso a datos y escrutinio				
[Q42]	41	Función de comprobación del cumplimiento				
[Q14]	42	Obligaciones de transparencia informativa				
[Q43]	45-47	Códigos de conducta				

11.¿Cómo se establecen los puntos de contacto?

Los PSSI deberán designar un **punto único de contacto** que permita tanto las autoridades (judiciales o administrativas, incluyendo autoridades nacionales, Comisión Europea y Junta de Servicios Digitales) como a los usuarios comunicarse fácilmente con ellos por vía electrónica.

El objetivo es crear un auténtico canal de comunicación

- Se deben utilizar los **recursos necesarios** para que las comunicaciones tengan lugar de manera rápida y eficiente. Tratándose de conceptos jurídicos indeterminados, no podemos determinar, *a priori*, qué plazos se van a considerar rápidos, pero deberán emplearse medios razonables para atender a las comunicaciones teniendo en cuenta su volumen.
- **No pueden automatizarse** el 100 % de las respuestas.
- La información deberá ser **fácilmente accesible** y mantenerse **actualizada**.
- Se debe permitir el **acuse de recibo** (p. ej., con un *e-mail* automático de "recibido") a través del *e-mail* facilitado por el usuario o autoridad que ha contactado con el prestador. Es recomendable que el usuario o autoridad reciba dicha comunicación vía *e-mail*, para poder mantener un registro de estas a efectos probatorios.
- Se deberán indicar los **idiomas** disponibles para las comunicaciones. Deberá ser posible la comunicación al menos en los idiomas de los países de la Unión Europea a los que el PSSI dirija sus servicios, entendiendo como tales todos los países en cuyo idioma está disponible la página web.
- En el caso de que se utilicen ***chatbots* o herramientas similares de mensajería instantánea**, deberá indicarse expresamente. Si bien la DSA no especifica cómo debería articularse dicha indicación, entendemos que podría comunicarse al usuario a través del propio *chatbot* (p. ej, mandar un mensaje al iniciarse la conversación especificando que el destinatario de la conversación iniciada por el usuario es una herramienta automatizada) o articularse mediante etiquetas/diseños que permitan al usuario entender que está interactuando con una herramienta de mensajería instantánea (p. ej., utilizar el icono o dibujo de un robot).

12. La obligación de designar representantes legales para los PSSI que no estén establecidos en la UE

Los PSSI establecidos en un tercer país y que ofrezcan servicios en la UE deben designar a un representante legal para actuar en alguno de los Estados en los que ofrezca sus servicios y proporcionar información a las autoridades sobre el mismo.

El objetivo es facilitar la comunicación con los PSSI establecidos en terceros países

- Los representantes legales podrán ser personas físicas o jurídicas.
- Deberán disponer de los poderes y recursos necesarios para cooperar de manera eficiente con las autoridades (p. ej., el representante legal no podrá estar sujeto a procedimientos de quiebra o insolvencia).
- Un mismo representante legal podrá ser mandatado por más de un PSSI y funcionar como punto de contacto.
- La designación deberá realizarse por escrito.
- Los PSSI deberá notificar su: (i) nombre; (ii) domicilio postal; (iii) dirección de correo electrónico; y (iv) número de teléfono al Coordinador de Servicios Digitales **[Q45]** del Estado en el que resida. La información deberá estar a disposición del público de manera accesible, clara y actualizada.

13. Adaptación de los términos y condiciones de uso

El Reglamento busca transparencia en relación con las políticas de moderación de los PSSI. Ahora se trata no solo de cumplir con la Ley aplicable, sino también con las normas definidas por el PSSI. Como principio general, rige la autonomía de la voluntad, de modo que el PSSI podrá definir las pautas de comportamiento que deben seguir sus usuarios.

Todos los PSSI deben **explicar y publicar sus políticas de moderación de contenidos**, con un lenguaje claro, sencillo y, en su caso, adaptado a menores. Las políticas de moderación de contenidos deben ser fácilmente accesibles y publicarse en un formato legible por máquina.

1

Formales

- Detallar las políticas, procedimientos, medidas y herramientas de moderación de contenidos (incluyendo decisiones algorítmicas y revisión humana).
- Explicar el sistema interno de gestión de reclamaciones **[Q21]**.
- Explicar en qué consiste un uso inadecuado de los servicios (p. ej., publicación reiterada de contenidos ilícitos o denuncias infundadas de forma reiterada) y sus consecuencias: ¿retirada del contenido? ¿suspensión de la cuenta? ¿cierre definitivo?
- Informar sobre los “cambios significativos” de las condiciones generales.

2

Materiales

- Aplicación diligente, objetiva y proporcionada, **teniendo en cuenta los derechos e intereses legítimos de todas las partes**, incluyendo los derechos fundamentales de los destinatarios del servicio (libertad de expresión, libertad y pluralismo de los medios de comunicación y otros derechos y libertades fundamentales amparados por la Carta).

Como recomendación adicional, es necesaria la aceptación de los términos y condiciones por parte de los usuarios y deben implementarse mecanismos que permitan preservar prueba tanto de la aceptación como del contenido. Por ejemplo, pueden utilizarse **herramientas de sellado de tiempo cualificadas** que permitan acreditar de forma fehaciente el contenido.

En el caso de las VLOP/VLOSE existen obligaciones adicionales:

- Proporcionar un resumen claro y accesible de las condiciones de uso, incluyendo medidas correctivas y mecanismos de recurso.
- Publicar los términos y condiciones de uso en todas las lenguas oficiales de los EE. MM. donde se presten lo servicios.

14. Medidas de transparencia

Todos los PSSI deben publicar informes **anuales** sobre sus actividades de moderación:

Autoridades

Órdenes recibidas de los EE. MM. indicando: (i) tipo de ilícito; (ii) Estado Miembro emisor, y (iii) tiempo medio para informar a la autoridad y para dar curso a la orden.

Investigaciones propias

Medidas implementadas, incluyendo: (i) uso de herramientas automatizadas; (ii) medidas adoptadas para formar RR. HH. (p. ej., recursos destinados al diseño y revisión humana de algoritmos); (iii) medidas adoptadas que afectan a la visibilidad y disponibilidad de los contenidos, especificando el número; y (iv) cualquier otra restricción de los servicios.

Categorización cumulativa según: (i) contenido contrario a la Ley o a los T&C generales; (ii) método de detección; (iii) restricción aplicada; y (iv) descripción del uso de medios automatizados especificando su finalidad, tasa de error y precisión.

Notificación y acción

Número de N&A recibidas indicando: (i) tipo de ilícito; (ii) número de notificaciones enviadas por alertadores fiables; (iii) actuaciones llevadas a cabo dependiendo de si es contrario a la Ley o a los T&C generales; (iv) número de N&A tratados sólo con herramientas automatizadas; y (v) tiempo medio para la adopción de medidas.

Apelación

Número de reclamaciones recibidas, incluyendo: (i) base de las reclamaciones; (ii) decisiones adoptadas; (iii) tiempo medio de decisión; y (iv) número de revocaciones.

Las plataformas, además, tienen obligaciones adicionales:

Resolución extrajudicial

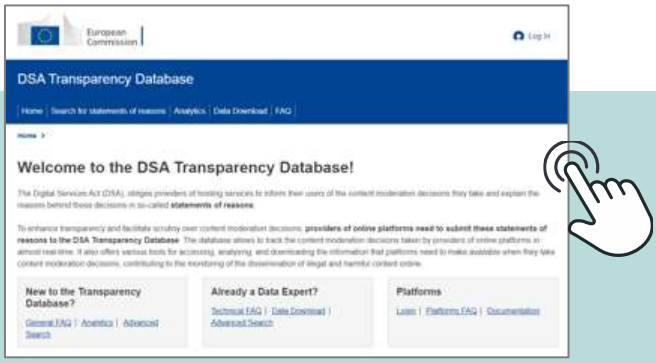
Número de disputas sometidas a órganos de resolución extrajudicial indicando: (i) los resultados de la resolución; (ii) el tiempo medio necesario para la resolución; y (iii) el porcentaje de disputas en las que se adoptó su decisión.

Suspensión de cuentas

Número de suspensiones impuestas por usos indebidos, distinguiendo entre suspensiones impuestas por: (i) proporcionar contenido manifiestamente ilegal; (ii) por enviar notificaciones manifiestamente infundadas; o (iii) por enviar reclamaciones manifiestamente infundadas.

Además, los informes deben publicarse en un formato legible por máquina y que sea fácilmente accesible y comprensible. En este momento, la Comisión Europea ha lanzado una consulta pública para definir qué formato deberán seguir estos informes (consultar aquí).

Tanto las plataformas en línea, como las VLOP y VLOSE deben, además, presentar a la Comisión Europea las declaraciones de motivos **[Q19]** relacionadas con la moderación de contenidos, para su inclusión en la Base de Datos de Transparencia de la DSA, en la que se pueden rastrear las decisiones de moderación de contenido que toman casi en tiempo real:



¿Qué obligaciones adicionales tienen las VLOP y VLOSE?

Las VLOP y VLOSE deberán publicar informes semestrales en una de las lenguas oficiales de los EE. MM. y que incluyan, junto con la información listada, la siguiente información adicional:

i. Recursos humanos que la plataforma dedica a la moderación de contenidos con respecto al servicio ofrecido, desglosados por cada lengua oficial aplicable.

ii. Cualificaciones y conocimientos lingüísticos de las personas que llevan a cabo dicha actividad de moderación de contenidos.

iii. Indicadores de precisión e información de los informes desglosada por cada lengua oficial.

iv. Información sobre el promedio mensual de destinatarios del servicio para cada EM.

15. ¿Qué es un mecanismo de notificación y acción? (N&A)

Se trata de mecanismos que permitan denunciar contenidos ilícitos directamente a los PSSI que los alojan. Una vez recibida la notificación de la denuncia, y si esta se ha formulado correctamente **[Q16]**, el PSSI estará obligado a responder **[Q17]**. Por eso se llaman mecanismos de notificación y acción.

Notificación

1. Explicación suficientemente motivada de la ilicitud
2. Localización precisa (URL)
3. Identificación del notificante (incluyendo *e-mail*)
4. Declaración de buena fe de que la información es precisa y completa

Permite determinar, **sin un examen jurídico detallado**, que el contenido es manifiestamente ilícito

Acción

1. Acuse de recibo (sin dilación indebida) **(Prioridad alertadores fiables [Q23])**
2. **Decisión motivada** incluyendo vías de recurso (sin dilación indebida)
3. Utilización de medios automatizados (cuando proceda)

16. Requisitos que deben cumplir los formularios de notificación

En realidad, el Reglamento recoge en gran medida las prácticas que ya están asentadas en el mercado, principalmente por influencia estadounidense, y las hace obligatorias. En concreto, los formularios deben diseñarse para cumplir con los siguientes requisitos:

Ser fácilmente accesibles y manejables, permitiendo el envío de notificaciones exclusivamente por vía electrónica.

Deben contener campos que permitan que el denunciante pueda proporcionar la información necesaria, incluyendo:

- una explicación motivada de por qué considera que un contenido es ilícito;
- la ubicación del contenido (p. ej., URL, referencia, etc.);
- su nombre y dirección de correo electrónico; y
- una declaración de actuación de buena fe.

En la descripción debe ser posible que el denunciante notifique múltiples elementos de contenidos presuntamente ilícitos por medio de una única notificación.

Debe permitir, pero no exigir, la identificación de la persona física o entidad que envía la notificación (salvo en los casos en los que sea necesaria la identidad para determinar si la información supone un contenido ilícito). Por lo tanto, debe permitirse al usuario continuar con el formulario en caso de que no rellene las casillas de “Nombre” y “Apellidos”.

17. ¿Cómo deben actuar los PSSI cuándo reciben una denuncia?

1

Acuse recibo

Deberá acusar recibo de la notificación al denunciante, **sin dilación indebida**. En el caso de las VLOP y VLOSE, deberá darse preferencia a las notificaciones formuladas por los **alertadores fiables [Q23]**.

2

Decisión motivada

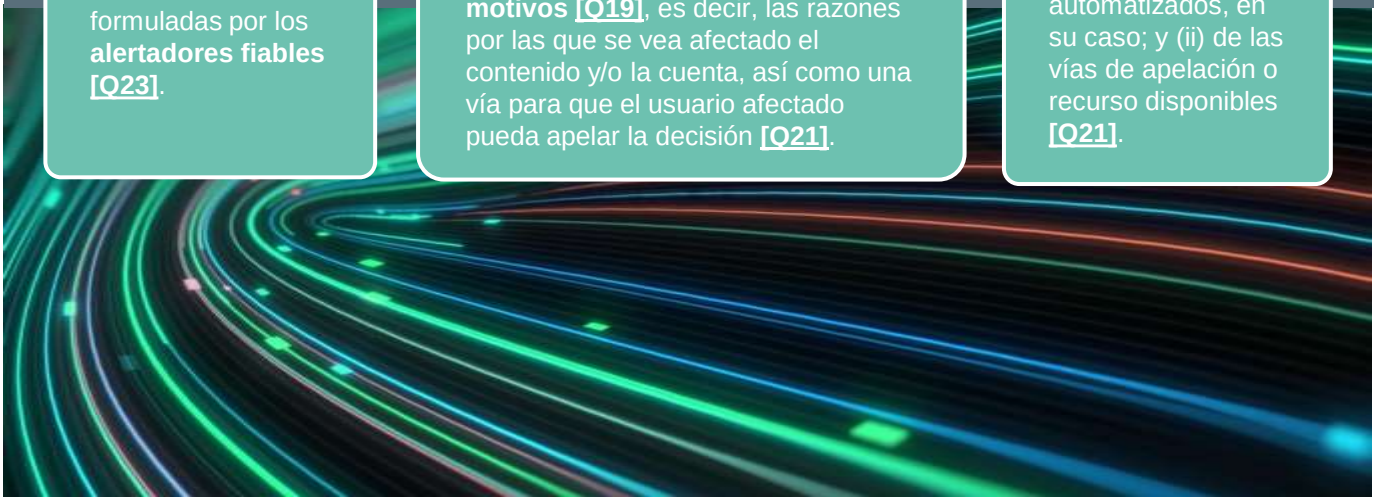
Las decisiones sobre el contenido o cuenta denunciada deben tomarse **en tiempo oportuno** y de manera diligente, no arbitraria y objetiva.

En caso de que el PSSI decida afectar una cuenta de usuario **[Q18]** deberá comunicarlo al afectado, incluyendo una **declaración de motivos [Q19]**, es decir, las razones por las que se vea afectado el contenido y/o la cuenta, así como una vía para que el usuario afectado pueda apelar la decisión **[Q21]**.

3

Comunicación de la decisión al denunciante

Deberá informarse, además de la decisión tomada al usuario que efectuó la denuncia, incluyendo: (i) el uso de medios automatizados, en su caso; y (ii) de las vías de apelación o recurso disponibles **[Q21]**.



18. ¿Qué significa “afectar” una cuenta?

Se entenderá que el PSSI está afectando una cuenta si se producen cualquiera de las siguientes situaciones:

Restricciones de visibilidad de contenidos, incluyendo eliminación, bloqueo o relegación.

Suspensión o terminación del servicio, total o parcial.

Afectación del uso de medios de pago.

Suspensión o terminación de la cuenta de usuario.

19. ¿Qué es una “declaración de motivos”?

Se trata de las razones que justifican que el PSSI afecte una cuenta, por ejemplo, procediendo a la retirada de un contenido.

Contenido mínimo de la declaración de motivos:

Motivación

Motivos en los que se ha basado la decisión, especificando su origen (p. ej., notificación enviada a través del sistema de denuncias o procedente de investigaciones propias).

Fundamentación

En caso de contenido ilícito, especificar su base jurídica y, en caso de que se trata de una incompatibilidad con los T&C, referencia al fundamento contractual.

Medios automatizados

Transparencia sobre los medios automatizados utilizados para adoptar la decisión.

Consecuencias de la decisión

Información detallada sobre si las medidas que se van a adoptar (p. ej., restricción de visibilidad, suspensión de pagos monetarios, retirada de información) y su duración y ámbito territorial.

Vías de recurso

Información sobre las vías de recurso disponibles para impugnar la decisión.

Solo hay **dos excepciones** en las que no es obligatorio facilitar una declaración de motivos a los usuarios afectados: (i) si el afectado no es localizable (p. ej., no se conocen los datos de contacto electrónicos del usuario); o (ii) se trata de **contenidos comerciales engañosos de gran volumen** (contenidos comerciales difundidos a través de la manipulación intencionada del servicio, por ejemplo, a través del de *bots* o cuentas falsas).

20. ¿Cómo deben actuar los PSSI si sospechan que se está cometiendo un delito?

En determinados supuestos, el PSSI puede sospechar que se ha cometido o que está a punto de cometerse un delito que implique una amenaza para la vida o la seguridad de las personas, ya sea a raíz de investigaciones propias o denuncias de terceros. En este caso, el prestador debe comunicarlo sin dilación a las autoridades policiales o judiciales competentes.

21. Mecanismos obligatorios para apelar las decisiones tomadas por el PSSI

Las plataformas y los VLOP/VLOSE deben permitir que los usuarios puedan apelar sus decisiones [Q22] en un plazo de seis meses desde que se adoptaron. Con este fin, deben facilitar tanto mecanismos internos de apelación, como información relacionada con la resolución extrajudicial de conflictos.

Sistema interno de gestión de reclamaciones

- Los destinatarios del servicio puedan **apelar las decisiones del PSSI** en materia de afectación de cuentas de forma electrónica y gratuita
- Disponible durante **al menos 6 meses** desde que se informó de la decisión
- **No cabe la decisión por IA**, debe participar personal cualificado: *¡Human in the loop!*
- La decisión debe comunicarse sin dilación indebida, de forma motivada e informando de la posibilidad de acudir a la resolución extrajudicial

Resolución extrajudicial de litigios por órganos certificados

- A elección del destinatario del servicio, de entre los órganos de resolución extrajudicial de litigios certificados por el CSD.
- Las decisiones no son vinculantes
- Debe informarse de esta posibilidad en la web.
- Pago del coste por la plataforma si el órgano de resolución extrajudicial le da la razón al usuario.
- No afecta a la posibilidad de acudir a la vía judicial.

22. ¿Qué decisiones deben ser apelables?

Las decisiones para las que deben facilitarse mecanismos de apelación son las siguientes:

1. Decisiones de retirar, bloquear o afectar la visibilidad de un contenido; o de no hacerlo.
2. Decisiones de suspender o cesar la prestación del servicio, en todo o en parte; o de no hacerlo.
3. Decisiones de suspender o suprimir una cuenta de usuarios; o de no hacerlo.
4. Decisiones de suspender, cesar o restringir la capacidad de monetizar el contenido alojado por el usuario; o de no hacerlo.

23. El canal preferente de los “alertadores fiables” (*trusted flaggers)*

Las plataformas y los VLOP/VLOSE deben adoptar las medidas técnicas y organizativas necesarias para tratar de forma prioritaria las notificaciones enviadas por “alertadores fiables”.

Los alertadores fiables

La condición de alertador fiable la otorgará, previa solicitud, el Coordinador de Servicios Digitales del Estado miembro en el que resida el solicitante, y siempre que se cumplan las siguientes condiciones:

- Deberá poseer conocimientos y competencias específicas para detectar, identificar y notificar contenidos ilícitos.
- No puede depender de ningún PSSI.
- Debe realizar sus actividades con el fin de enviar notificaciones de manera diligente, precisa y objetiva.

24. Nuevas obligaciones de los PSSI para combatir activamente el abuso de sus servicios y sistemas

Los PSSI deberán proteger a los usuarios de "**usos indebidos**" de su plataforma mediante una doble obligación: (i) suspender las cuentas de los usuarios que **publican contenido manifiestamente ilícito de forma frecuente**; y (ii) suspender los mecanismos de notificación y acción y de reclamaciones internas a los usuarios que los utilicen para solicitar la **retirada de contenidos de forma manifiestamente infundada o presentar reclamaciones manifiestamente infundadas**.

¿Cómo debe implementarse en la práctica?

Advertencia previa

Es obligatorio enviar una advertencia previa al usuario afectado **antes** de afectar su cuenta, informando sobre los motivos de la suspensión y las vías de recurso contra la decisión adoptada.

También tendrán que advertir en los términos y condiciones de la política adoptada respecto de estos usos indebidos, de forma clara y detallada, e incluir ejemplos de los hechos y circunstancias que las plataformas tienen en cuenta para adoptar medidas de protección contra usos indebidos y para fijar la duración de dichas medidas.

Adicionalmente, los PSSI podrán establecer en sus términos y condiciones medidas más rigurosas para el caso de contenidos manifiestamente ilícitos relacionados con delitos graves (p. ej., pornografía infantil).

Análisis

Las plataformas deberán analizar cada caso de forma individualizada, actuando de forma diligente, objetiva y no arbitraria, teniendo en cuenta todos los hechos y circunstancias del caso. Antes de tomar medidas de protección, deberán atender a: (i) las cifras absolutas de usos indebidos; (ii) la proporción respecto del contenido total publicado; (iii) la gravedad y consecuencias de dichos usos indebidos; y (iv) si es factible, la intención del usuario afectado.

Decisión de afectación

En aquellos casos en los que la plataforma decida afectar una determinada cuenta (p. ej., suspensión), deberá explicar los motivos al afectado.

El período de suspensión deberá ser razonable (no existe ninguna guía interpretativa).

25. Requisitos aplicables al diseño de la interfaz en línea

Las plataformas y los VLOP/VLOSE no pueden diseñar, organizar ni gestionar sus interfaces en línea de forma que puedan resultar en el engaño o la manipulación de los destinatarios del servicio de forma que distorsionen o afecten su capacidad de tomar decisiones libres e informadas (patrones oscuros).

La Comisión Europea se ha centrado especialmente en las prácticas dirigidas a priorizar las opciones del usuario cuando toma una decisión, insistir al usuario para que cambie una decisión ya tomada, o dificultar la baja del servicio de modo que sea más difícil que la suscripción.

Códigos de conducta

La Comisión fomentará la elaboración de códigos de conducta voluntarios que deben apoyar y complementar las obligaciones de transparencia relativas a la publicidad para los prestadores de plataformas en línea. Estos códigos establecerán unos mecanismos flexibles y eficaces para facilitar y potenciar el cumplimiento de dichas obligaciones, en particular en lo que se refiere a las modalidades de transmisión de la información pertinente sobre el anunciante y a información significativa sobre la monetización de los datos.

La Comisión fomentará la elaboración de los códigos de conducta a más tardar el 18 de febrero de 2025 y su aplicación a más tardar el 18 de agosto de 2025. Cuando sea conveniente, la Comisión puede invitar a la Agencia de los Derechos Fundamentales o al Supervisor Europeo de Protección de Datos a expresar sus opiniones sobre el código de conducta correspondiente.

26. ¿Cuáles son las obligaciones de transparencia en materia de publicidad?

Cuando una plataforma, VLOP/VLOSE publique anuncios en su interfaz, deberá cumplir con las siguientes obligaciones:

- Identificar el anuncio como “publicidad”.
- Identificar quién es el anunciante y, en caso de que el anuncio no haya sido pagado por éste, indicar quién lo pagó.
- Facilitar información significativa a la que pueda accederse desde el anuncio, sobre cuáles son los principales parámetros utilizados para determinar a quién se le muestra el anuncio y, en su caso, acerca de cómo puede cambiar esos parámetros.
- No presentar anuncios basados en la elaboración de perfiles [Q27] utilizando categorías especiales de datos personales.
- No presentar anuncios basados en la elaboración de perfiles mediante la utilización de datos personales del usuario cuando sean conscientes, con una seguridad razonable, de que el destinatario del servicio es un menor.

Además, deben facilitar ciertos mecanismos para los destinarios del servicio que vaya a difundir publicidad:

- Proporcionar una funcionalidad que permita al usuario declarar que un determinado contenido es o contiene comunicaciones comerciales.
- Asegurar que cuando un usuario declare que un contenido es comercial, éste se identifique claramente como tal a otros usuarios en tiempo real.

27. ¿Qué quiere decir el concepto “elaboración de perfiles”?

Se refiere a toda forma de tratamiento automatizado de datos personales consistente en utilizar dichos datos para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

28. Nuevas obligaciones de transparencia sobre los sistemas de recomendación

Los PSSI que utilicen sistemas de recomendación deben describirlos en sus términos y condiciones de uso, de forma clara y sencilla, incluyendo: (i) cuáles son los criterios más significativos a la hora de determinar la información sugerida al usuario; y (ii) cuál es la importancia relativa de dichos parámetros.

En el caso de sistemas que permitan varias opciones para ofrecer la información, debe facilitarse al usuario una funcionalidad que le permita seleccionar y modificar en cualquier momento su opción preferida.

La obligación ya existía en cumplimiento del Reglamento P2B2C y de la Ley General para la Defensa de los Consumidores y Usuarios.

29. ¿Qué medidas adicionales deberán adoptarse para la protección de menores?

Los PSSI accesibles a menores deberán:

1. Establecer medidas adecuadas y proporcionadas para garantizar la privacidad, seguridad y protección de los menores.
2. No presentar anuncios basados en la elaboración de perfiles **[Q27]** cuando sean razonablemente conscientes de que el destinatario del servicio es un menor.

Estas medidas no implican que los PSSI estén obligados a tratar datos personales adicionales con el fin de evaluar si el destinatario del servicio es un menor o no.

30. ¿En qué consisten las obligaciones de trazabilidad de los comerciantes?

Los mercados en línea **[Q4]** deberán garantizar que los comerciantes **[Q31]** puedan ser objeto de trazabilidad por parte de los usuarios a los que se ofertan sus servicios, para lo que deberán implementar los siguientes procesos:

1 Obtención de información para el alta de comerciantes

- Nombre, dirección, teléfono y correo electrónico.
- Copia del documento de identificación o identificación electrónica (eIDAS).
- Datos de la cuenta de pago.
- Información del Registro Mercantil (si aplica) incluyendo nombre y número de registro.
- Auto certificación de que el comerciante cumplirá con la normativa aplicable en la Unión Europea.

2 Verificación de la información recibida

Antes de permitir el acceso a los servicios, el *marketplace* deberá hacer todo lo posible para verificar que la información suministrada es fiable y completa. No se exige que dicha comprobación sea excesivamente costosa. Se sugiere:

- Utilizar bases de datos o interfaces en línea oficiales (p. ej., registros mercantiles nacionales, sistemas de intercambio de información sobre IVA).
- Solicitar documentos justificativos fiables (p. ej., estados bancarios, certificados de cuentas de pago, certificados empresariales y certificados del registro mercantil).
- Recurrir a otras fuentes fiables.

3 Aprobación / Rechazo

En caso de que la plataforma tenga razones para creer que hay información inexacta, incompleta o desactualizada, se solicitará al comerciante que la subsane. Si no lo hace, no se deberá permitir el acceso al servicio hasta que el comerciante atienda la solicitud en su totalidad.

4 Apelación

- Habilitar mecanismos de apelación para comerciantes rechazados.
- Incluir acceso a gestión de reclamaciones y mecanismos de resolución extrajudicial de disputas.

5 Controles aleatorios

Destinados a la comprobación *ex post* en bases de datos abiertas de si los productos o servicios ofertados han sido identificados como ilícitos.

6 Publicidad

Parte de la información obtenida de los oferentes debe ponerse a disposición de los usuarios consumidores en el interfaz de la web, de manera clara, fácilmente accesible y comprensible, incluyendo:

- Datos de contacto del comerciante.
- Datos del registro (en caso de que esté inscrito).
- Auto certificado de cumplimiento de la normativa UE.

7 Conservación y confidencialidad

La información debe conservarse de manera segura por un período de seis meses desde que finalizó la relación contractual y, transcurrido ese plazo, destruirse. Deberá además asegurarse la confidencialidad de la información recabada, salvo orden judicial o administrativa.

En relación con el alta de nuevos vendedores/oferentes a partir del 17 de febrero de 2024, se deberá obtener esta información antes de permitirles el acceso. En el caso de oferentes que ya estaban utilizando el servicio en esta fecha, se deberá obtener esta información antes del **17 de febrero de 2025** y, en caso de no obtenerla, suspender su acceso al servicio hasta que se regularice la situación.

31. ¿Qué es un comerciante a efectos del Reglamento?

Un comerciante es toda persona física o jurídica, ya sea privada o pública, que actúe, incluso a través de otra persona que actúe en su nombre o en su representación, con fines relacionados con su actividad comercial, negocio, oficio o profesión.

32. Exigencias de diseño del interfaz de los mercados en línea

El objetivo perseguido por la DSA es que los mercados en línea permitan a los comerciantes cumplir con sus obligaciones en materia precontractual de conformidad y seguridad de productos. ¿Cómo? Implementado una interfaz que permita que los comerciantes faciliten, como mínimo, la siguiente información:

- Nombre, la dirección, el número de teléfono y la dirección de correo electrónico del operador económico.
- Identificación clara e inequívoca de los productos promocionados.
- Cualquier signo que identifique al comerciante (p. ej., marca, logo).
- En su caso, información relativa al etiquetado y marcado de conformidad con las normas de seguridad y conformidad de los productos.

33. ¿En qué consiste la obligación de informar a los consumidores sobre la existencia de productos o servicios ilícitos?

Los mercados en línea **[Q4]** que detecten que en su plataforma se están ofreciendo productos o servicios ilícitos deberán informar a los usuarios que los han adquirido. En concreto, se deberá informar:

De que el producto o servicio es ilícito	De la identidad del comerciante	De cualquier vía de recurso pertinente

Cuando no se disponga de los datos de contacto de todos los consumidores afectados, dicha información se pondrá a disposición del pública de forma fácilmente accesible en la interfaz en línea.

34. ¿En qué consiste el análisis de riesgos exigible a las VLOP y los VLOSE?

Las VLOP y VLOSE deberán llevar a cabo evaluaciones de riesgos sobre cualquier riesgo sistémico **[Q35]** asociado al diseño, funcionamiento o uso de sus servicios (incluyendo el uso de sistemas algorítmicos), así como posibles usos indebidos por parte de los destinatarios de estos servicios.

La evaluación tendrá en cuenta la gravedad del impacto potencial y la probabilidad de dichos riesgos (p. ej., evaluar si el potencial impacto negativo puede afectar a un gran número de personas, su posible irreversibilidad o la dificultad de subsanarlo y restablecer la situación existente antes del impacto potencial). En concreto, debe atenderse especialmente a los siguientes factores:

- El diseño de sistemas de recomendación y de cualquier otro sistema algorítmico.
- Los sistemas de moderación de contenidos.
- Los T&C generales aplicables y su ejecución.
- Los sistemas de selección y presentación de anuncios.
- Las prácticas del prestador relacionadas con los datos.
- La manipulación intencionada del servicio (p. ej., creación de cuentas falsas, uso de *bots* o explotación automatizada del mismo).
- La amplificación y difusión potencialmente rápida y amplia de contenido ilícito y de información incompatible con los T&C.

35. ¿Qué se considera riesgo sistémico?

Se consideran riesgos sistémicos los siguientes:

Difusión de contenido ilícito (p. ej., difusión de materiales de abuso sexual de menores) y realización de actividades ilícitas (p. ej., venta de productos prohibidos).

Cualquier efecto negativo real o previsible: (a) en los derechos fundamentales (p. ej., uso indebido del servicio para el envío de notificaciones abusivas); (b) sobre el discurso cívico, los procesos electorales y la seguridad pública; o (c) relacionado con la violencia de género, la protección de la salud pública y los menores y las consecuencias negativas graves para el bienestar físico y mental de la persona (p. ej., diseño web que estimula adicciones).

36. ¿Cada cuánto tiempo debe realizarse el análisis de riesgos sistémicos?

Al menos una vez al año y antes de desplegar funcionalidades que puedan tener un impacto crítico en los riesgos detectados. Se deberán conservar durante los tres años posteriores a su realización.

37. Pautas de actuación para las plataformas ante los riesgos sistémicos detectados

Deberán aplicar medidas de reducción de riesgos **razonables, proporcionadas** (a la luz de la capacidad económica del PSSI y de la necesidad de evitar restricciones innecesarias) y **efectivas**, respetando los derechos fundamentales, prestando especial atención al impacto en la libertad de expresión.

Por ejemplo, dichas medidas pueden implicar la adaptación del diseño y funcionamiento de los servicios, T&C o procesos de moderación de contenidos, la corrección de los criterios utilizados en sus recomendaciones, el refuerzo de sus sistemas de internos de supervisión, la realización de pruebas y adaptación de sistemas algorítmicos y publicitarios o el ajuste de la cooperación con alertadores fiables.

También se tendrá en cuenta:

1. la rapidez y calidad del tratamiento de las notificaciones.

A este respecto, por ejemplo, el Código de conducta para la lucha contra la incitación ilegal al odio en internet de 2016 establece un punto de referencia para tratar notificaciones válidas para la eliminación de la incitación ilegal al odio en menos de 24 horas. Otros tipos de contenidos ilícitos pueden requerir plazos más largos o más cortos para el tratamiento de las notificaciones, que dependerán de los hechos, las circunstancias y los tipos de contenidos ilícitos de que se trate.

2. el interés superior de los menores, en especial cuando sus servicios se dirijan principalmente a menores o sean utilizados predominantemente por ellos.

38. ¿Cómo deben llevarse a cabo las auditorías internas?

Los VLOP y VLOSE deberán someterse a auditorías independientes **[Q39]** para evaluar el cumplimiento de sus obligaciones y cualquier compromiso complementario adquirido de conformidad con códigos de conducta y protocolos de crisis.

Para ello, es responsabilidad de los VLOP y VLOSE:

1. Facilitar la cooperación y asistencia necesaria a los auditores (p. ej., dándoles acceso a los datos y locales pertinentes, respondiendo a sus preguntas).

2. Tener en cuenta las recomendaciones operativas con el objetivo de adoptar las medidas para aplicarlas y plazo de **un mes** para adoptar un informe de aplicación que recoja estas medidas.

39. ¿Qué se considera una auditoría independiente de cara a la evaluación de riesgos sistémicos?

El Reglamento exige que se trate de organizaciones que cumplan los siguientes requisitos:

- Sean independientes de la plataforma (p. ej., no hayan prestado servicios distintos a los de auditoría en un periodo de un año, no realicen la autoría a cambio de honorarios).
- Posean conocimientos en materia de gestión de riesgos y tengan capacidades técnicas para auditar algoritmos.
- Sean objetivos y rigurosos con la ética profesional.

Además, el informe de auditoría que debe estar fundamentado, ofreciendo un relato coherente de las actividades realizadas y las conclusiones alcanzadas. Los informes de auditoría deben presentar una opinión clara sobre el cumplimiento de la DSA por parte del servicio auditado.

En su caso, el informe debe incluir una descripción de los elementos concretos que no pudieron auditarse, y una explicación de por qué fue así. También incluirá recomendaciones y medidas de mejora que debe adoptar el prestador para cumplir con las obligaciones de la DSA. Se trata de incentivar la máxima colaboración por parte de los auditados.

El 20 de octubre de 2023 la Comisión adoptó un acto delegado con las normas aplicables a las auditorías independientes para evaluar el cumplimiento de la DSA por parte de las VLOP y VLOSE. El acto delegado establece los pasos que los servicios designados deben aplicar para verificar las capacidades y la independencia de su auditor. También establece los principios fundamentales que los auditores deben aplicar al realizar las auditorías que exige la DSA.

Los auditores deben utilizar plantillas para elaborar las auditorías independientes, y los VLOP y VLOSE también deberán utilizarlas para elaborar sus informes de aplicación. ¿Por qué? Para garantizar la comparabilidad entre los informes de los distintos servicios.

Las auditorías representan una importante herramienta de rendición de cuentas y forman parte de los diversos requisitos de transparencia de la DSA. Los 19 servicios designados en abril de 2023 deberán someterse a una primera auditoría a más tardar 16 meses después de su designación, es decir, a finales de agosto de 2024. Tendrán que transmitir el informe de auditoría a la Comisión y a la autoridad competente de su Estado miembro de establecimiento los informes de auditoría, y también deberán publicar estos informes a más tardar en un plazo de tres meses a partir del momento en que finalicen el informe de ejecución de la auditoría.

Pulsa aquí para más información.

40. Requisitos de transparencia adicionales para los VLOP/VLOSE

Las VLOP y VLOSE que presenten anuncios publicitarios en sus interfaces tienen la obligación de recopilar un repositorio de publicidad, publicarlo en una sección de su interfaz y hacer posible que, mediante una herramienta de búsqueda, se pueda realizar consultas usando distintos criterios. El repositorio deberá incluir información exacta y completa sobre las siguientes materias:

- Contenido del anuncio (incluyendo nombre del producto, servicio o marca y el objeto del anuncio).
- Nombre del anunciante (y en su caso, de la persona que ha pagado el anuncio).
- Período de difusión.
- Grupo de destinatarios (en su caso) junto con parámetros de inclusión y exclusión (criterios de personalización y de difusión).
- Comunicaciones comerciales de los vendedores en *marketplaces*.
- Número total de destinatarios del servicio alcanzados por cada Estado miembro (impresiones).
- No deberá contener ningún dato personal de los usuarios del anuncio.

Sistemas de recomendación

Las VLOP y VLOSE deben garantizar sistemáticamente que los destinatarios de su servicio disfruten de opciones alternativas que no se basen en la elaboración de perfiles **[Q27]** para los parámetros principales de sus sistemas de recomendación. Estas opciones deben ser directamente accesibles desde la interfaz en línea en la que se presentan las recomendaciones.

Centro Europeo para la Transparencia Algorítmica

El 18 de abril de 2023, la Comisión puso en marcha el Centro Europeo para la Transparencia Algorítmica (ECAT), un centro científico pionero en su género con sede en Sevilla que prestará apoyo a la Comisión y a las autoridades nacionales en la supervisión del cumplimiento de la DSA.

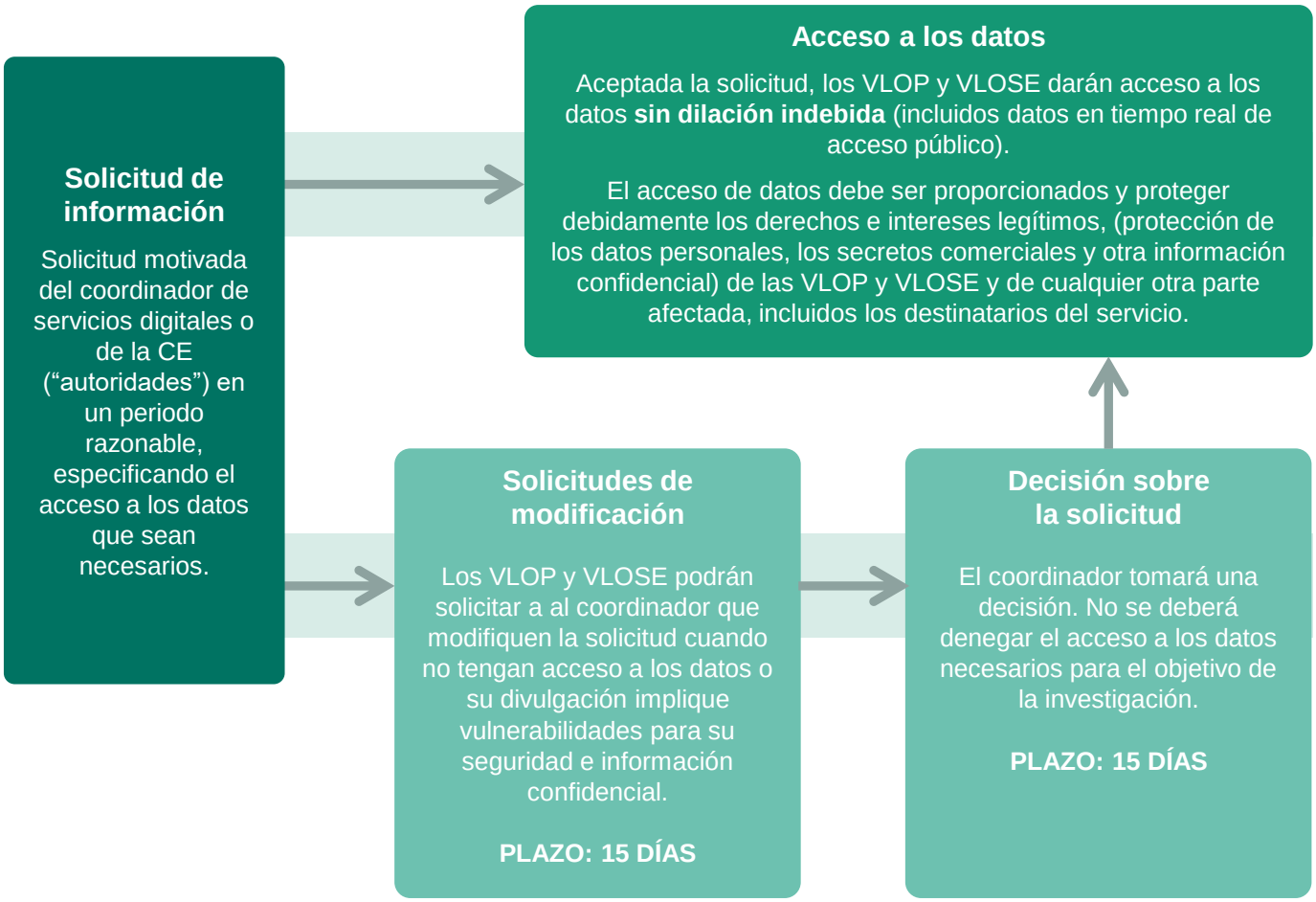
Entre otras cosas, el ECAT:

- realizará pruebas técnicas de los sistemas algorítmicos para comprender su funcionamiento
- analizará informes de transparencia, evaluaciones de riesgos y auditorías independientes
- apoyará investigaciones e inspecciones
- identificará los riesgos emergentes asociados al uso de VLOP/VLOSE
- actuará como centro de conocimientos para la investigación realizada gracias al acceso a los datos facilitados por la DSA.

En este marco, el ECAT también ha firmado un acuerdo de cooperación con el centro francés Pôle d'expertise de la Régulation Numérique (PEReN), uno de los primeros equipos de ciencia de datos del mundo que trabaja en los temas cubiertos por la DSA. También ha designado la lista de miembros del grupo especial sobre el Código de conducta de la UE en materia de diseño adaptado a la edad, que inició sus trabajos el 13 de junio de 2023.

41. ¿Qué datos deben compartir los VLOP/VLOSE con las autoridades públicas?

Para vigilar y evaluar debidamente el cumplimiento por parte de las VLOP y VLOSE de sus obligaciones, el coordinador de servicios digitales del establecimiento **[Q46]** o la Comisión pueden requerir acceso o informes relativos a datos específicos, incluidos los datos relacionados con algoritmos.



Uso de los datos recopilados

Seguimiento y evaluación del cumplimiento del Reglamento por parte de la plataforma, teniendo en cuenta sus derechos e intereses.

Objeto de la solicitud

- **A las autoridades:** explicación del diseño y funcionamiento de sistemas algorítmicos y de recomendación.
- **A investigadores autorizados [Q42]:** datos necesarios para realizar estudios para la detección de riesgos sistémicos y la evaluación de las medidas para mitigarlos (p. ej., datos sobre procesos de moderación de contenidos o sistemas internos de gestión de reclamaciones, número de visualizaciones de contenidos por parte de los usuarios).

Consulta pública sobre el acto delegado relativo al acceso de datos

Con el propósito de mejorar el seguimiento de las actuaciones de las plataformas para hacer frente a los contenidos ilícitos, así como a otros riesgos sociales como la difusión de desinformación y los riesgos que puedan afectar a la salud mental de los usuarios, se permite a los investigadores autorizados acceder a ciertos datos de las VLOP y VLOSE hasta ahora no divulgados.

La consulta del acto delegado tuvo lugar del **25 de abril al 31 de mayo de 2023.**

Se recibieron **133 contribuciones**, que recogían información sobre las necesidades de acceso a los datos de los investigadores

También se abordaron **cuestiones operativas del acceso a datos**, como los requisitos técnicos y de procedimiento de las aplicaciones de acceso a datos.

Los encuestados subrayaron la necesidad de un procedimiento de solicitud normalizado y de más orientaciones sobre los criterios que deben cumplir los investigadores para ser autorizados. También destacaron la importancia de contar con un mecanismo que armonice las necesidades de acceso a los datos de los investigadores y exigían más claridad sobre las obligaciones de los VLOP/VLOSE.

Sobre la base de las contribuciones recibidas, la Comisión está preparando actualmente un acto delegado en el que se detallan las condiciones técnicas y los requisitos de procedimiento para un proceso eficaz, práctico y claro de acceso a los datos que ofrezca también salvaguardias adecuadas contra los abusos. Está previsto que el acto delegado se adopte en la primavera de 2024.

Pulsa aquí para más información sobre el estado de trámite del acto delegado.

El 18 de enero de 2024, la Comisión envió solicitudes motivadas de información a las 17 VLOP/VLOSE designadas el 25 de abril de 2023 para que proporcionen información sobre las medidas que han adoptado para cumplir con sus obligaciones. Las plataformas deberán facilitar dicha información antes del 8 de febrero de 2024 y, en virtud de la evaluación de las respuestas, la Comisión determinará si se debe dar acceso a los datos a los investigadores autorizados. Para más información, pulsa aquí.

42. Requisitos para ser considerado “investigador autorizado”

Son investigadores que cumplan las siguientes condiciones:

1. que estén afiliados a un organismo de investigación;

2. que sean independientes desde el punto de vista de los intereses comerciales;

3. que revelen en la solicitud cómo se financia la investigación;

4. que estén en condiciones de satisfacer los requisitos específicos en materia de seguridad y confidencialidad de los datos correspondientes a cada solicitud y de proteger los datos personales, y que describan en su solicitud las medidas técnicas y organizativas apropiadas que hayan adoptado a tal fin;

5. que demuestren en la solicitud que su acceso a los datos y los plazos solicitados son necesarios y proporcionados para los fines de su investigación, y que los resultados esperados de dicha investigación contribuirán a esos fines;

6. que las actividades de investigación previstas se lleven a cabo para realizar estudios que contribuyan a la detección de riesgos sistémicos y a la evaluación de la idoneidad, eficiencia y medidas de reducción de riesgos de los VLOP y VLOSE.

7. que se hayan comprometido a hacer públicos los resultados de su investigación de forma gratuita, en un plazo razonable tras la finalización de la investigación.

43. ¿Qué relevancia otorga el Reglamento a la elaboración de códigos de conducta por parte de las VLOP/VLOSE?

La Comisión y la Junta deben fomentar la elaboración de códigos de conducta voluntarios, así como la aplicación de las disposiciones de esos códigos. Estos códigos serán revisados y adaptados periódicamente por la Comisión y la Junta.

Aunque la aplicación de los códigos de conducta debe ser medible y estar sujeta a supervisión pública, no debe afectar al carácter voluntario de dichos códigos y a la libertad de los interesados para decidir si desean participar.

44. Obligaciones de cooperación de las VLOP/VLOSE en circunstancias de crisis

En tiempos de crisis la Comisión podrá exigir a las VLOP y VLOSE, previa recomendación de la Junta Europea de Servicios Digitales, que inicien urgentemente una respuesta a la crisis.

En concreto, las medidas que se consideran exigibles incluyen las siguientes:

A Evaluar si el funcionamiento y uso de sus servicios contribuye o puede contribuir a una amenaza grave.

B Determinar y aplicar medidas específicas, eficaces y proporcionadas para prevenir y limitar cualquier contribución a la amenaza grave (p. ej., adaptación de los procesos de moderación de contenidos, adaptación de las condiciones generales, los sistemas algorítmicos pertinentes y los sistemas publicitarios, o la adaptación del diseño de sus interfaces en línea).

C Informar a la Comisión de las evaluaciones realizadas y del impacto de las medidas adoptadas.

¿Cuándo tenemos una “crisis”?

Son circunstancias extraordinarias que pueden dar lugar a una amenaza grave para la seguridad pública o la salud pública en la Unión o en partes significativas de esta. Las crisis puedes derivarse, por ejemplo, de conflictos armados o actos de terrorismo, incluidos los conflictos o actos de terrorismo emergentes, las catástrofes naturales como terremotos y huracanes, así como las pandemias y otras amenazas transfronterizas graves para la salud pública.

¿Qué requisitos deben cumplir las medidas que la Comisión exija a los VLOP y VLOSE en situaciones de crisis?

Las medidas deben cumplir con los requisitos establecidos por el Reglamento y ser ajustadas a Derecho. En concreto, la Comisión debe velar por el cumplimiento de los siguientes requisitos:

1. Las medidas son estrictamente necesarias, justificadas y proporcionadas a la gravedad de la amenaza, la urgencia y las implicaciones en los derechos fundamentales.
2. Debe establecerse un plazo razonable para la adopción.
3. En principio, las acciones deben limitarse a un periodo máximo de tres meses, ya que tienen carácter excepcional.
4. En caso de que evolucione la crisis, se podrá revocar la decisión o ampliar el periodo de aplicación.

La Comisión puede iniciar la elaboración de **protocolos de crisis voluntarios** para coordinar una respuesta rápida, colectiva y transfronteriza en el entorno en línea. Este puede ser el caso, por ejemplo, cuando las plataformas en línea se utilizan de forma indebida para propagar rápidamente contenidos ilícitos o desinformación, o bien cuando surja la necesidad de difundir rápidamente información fiable.

Ante el papel que desempeñan las VLOP/VLOSE en la difusión de información, se debe fomentar su colaboración y aplicación de protocolos de crisis específicos y limitados en el tiempo y referidos a circunstancias extraordinarias. Estos protocolos no deben suponer una obligación de monitorización ni búsqueda activa de hechos o circunstancias que indiquen contenidos ilícitos

MÓDULO D

Organismos competentes y régimen sancionador

45. Órganos competentes para supervisar y hacer cumplir el Reglamento

Coordinador de servicios digitales

Nivel estatal

Competencias exclusivas sobre los PSSI que tienen su establecimiento principal en su territorio o su representante legal designado.

Supervisión

Investigación

- Solicitud de información sobre posibles infracciones
- Inspección de las instalaciones del PSSI
- Pedir explicaciones al personal

Ejecución

- Aceptar los compromisos y declararlos vinculantes
- Emitir órdenes de cesación a través de las autoridades judiciales
- Multas y multas coercitivas
- Adopción de medidas cautelares
- Muy graves: (1) Plan de acción; (2) Limitación de acceso temporal

Certificación de alertadores de confianza

Certificación de órganos extrajudiciales de resolución de litigios

Comisión europea

Nivel UE

Competencias exclusivas sobre las VLOP/VLSE en materia de riesgos sistémicos y no exclusivas en materia de cumplimiento de las VLOP/VLOSE.

- Investigación en materia de cumplimiento
- Incoación de procedimientos
- Solicitudes de información
- Realizar entrevistas y tomar declaraciones
- Realizar inspecciones
- Adoptar medidas cautelares
- Negociar y adoptar compromisos
- Acciones de seguimiento
- Decisiones en materia de incumplimiento
- Multas y multas coercitivas
- Restricción de acceso

Junta Europea de Servicios Digitales

Nivel UE

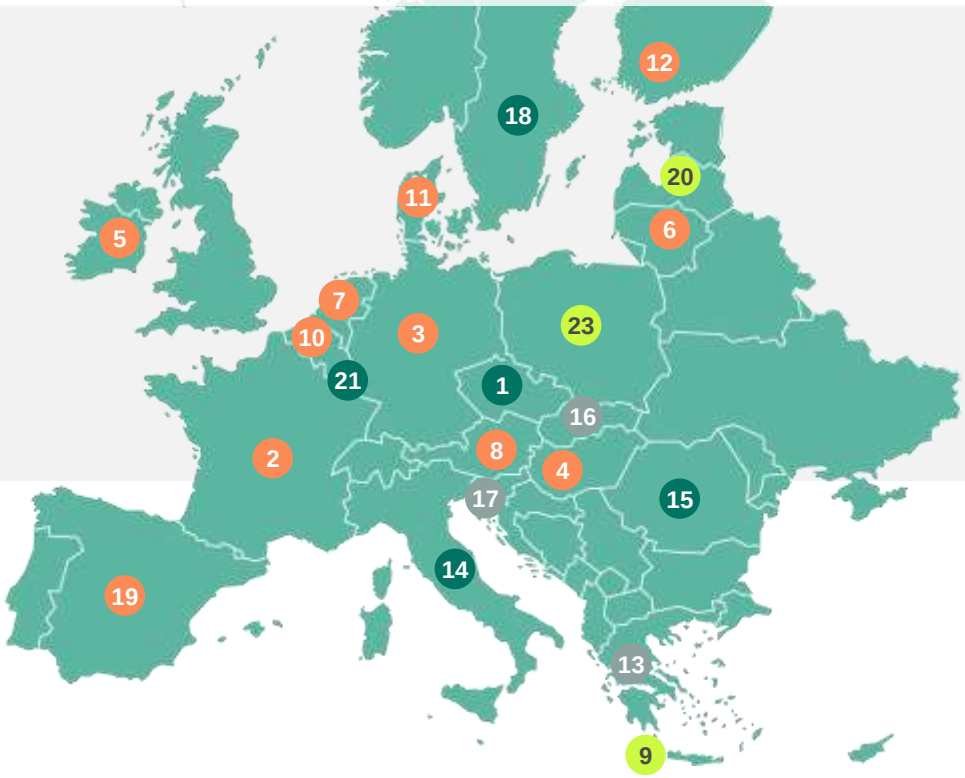
Formada por todos los CSD y presidida por la CE.

- Apoyo en la coordinación de investigaciones conjuntas
- Apoyo en el análisis de informes y resultados de las auditorías independientes aplicables a las VLOP/VLOSE
- Dictámenes, recomendaciones y asesoramiento
- Asesoramiento a la CE en la incoación de procedimientos frente a las VLOP/VLOSE
- Apoyo, promoción y elaboración de normas europeas, directrices, informes, modelos y códigos de conducta

Avance en la designación de Coordinadores de Servicios Digitales (CSD)

Estado

- Implementado
- Borrador
- Información pendiente
- Asunción



1 República Checa
Oficina Checa de Telecomunicaciones (CTU)

2 Francia
Autoridad de Regulación de la Comunicación Audiovisual y Digital (ARCOM)

3 Alemania
Agencia Federal de Redes (Bundesnetzagentur)

4 Hungría
Autoridad Nacional de Medios de Comunicación e Infocomunicaciones (NMHH)

5 Irlanda
Ireland's Media Comission (Comisiún na Meán)

6 Lituania
Autoridad Reguladora de las Comunicaciones de la República de Lituania (RRT)

7 Países Bajos
Autoridad de Consumidores y Mercados (ACM)

8 Austria
Autoridad de Comunicaciones de **Austria** (KommAustria). Apoyado por la Autoridad Reguladora Austriaca de Radiodifusión y Telecomunicacione (RTR)

9 Chipre
Autoridad de Radiotelevisión (CRTA)

10 Bélgica
Regulador flamenco de medios de comunicación (Vlaamse Regulator voor de Media).

11 Dinamarca
Autoridad Danesa de Competencia y Consumo (Konkurrence- og Forbrugerstyrelsen)

12 Finlancia
Agencia Finlandesa de Transportes y Comunicaciones (Traficom)

13 Grecia
Comisión Helénica de Telecomunicaciones y Correos (EETT)

14 Italia
Autoridad de Garantías de las Comunicaciones de Italia (AGCOM)

15 Rumanía
Autoridad Nacional para Gestión y Regulación de las Comunicaciones (ANCOM)

16 Eslovaquia
Consejo Eslovaco de Servicios Mediáticos (CMS)

17 Eslovenia
Agencia de Redes y Servicios de Comunicación (AKOS)

18 Suecia
Autoridad Sueca de Correos y Telecomunicaciones (PTS)

19 España
Comisión Nacional de los Mercados y la Competencia (CNMC)

20 Letonia
Centro de Protección de los Derechos de los Consumidores (PTAC)

21 Luxemburgo
Autoridad de la competencia

22 Malta
Autoridad de Comunicaciones de Malta (MCA)

23 Polonia
Oficina de Comunicaciones Electrónicas (UKE)

46. Y en caso de incumplimiento…

Los incumplimientos de las obligaciones establecidas en el Reglamento deben sancionarse de manera efectiva, proporcionada y disuasoria, teniendo en cuenta:

- Naturaleza, gravedad, recurrencia y duración del incumplimiento
- Interés público perseguido
- Número de destinatarios del servicio afectado
- Alcance y la clase de actividades realizadas
- Carácter intencionado o negligente de la infracción
- Capacidad económica del infractor

Los Estados miembros podrán aplicar:

- Multas de hasta el **6% de la facturación anual mundial** en caso de incumplimiento.
- Multas coercitivas periódicas de hasta el **5% del volumen de negocios medio diario mundial o de los ingresos anual**es del PSSI por cada día de retraso en el cumplimiento de las sanciones.
- Sanciones por proporcionar información incorrecta, incompleta o engañosa, por no responder o por no rectificar información incorrecta, incompleta o engañosa y por no someterse a una inspección hasta con importes máximos de hasta **el 1 % de los ingresos anuales, o del volumen de negocios anual** en todo el mundo del PSSI.

Para las VLOP y VLOSE, la Comisión podrá imponer dichas sanciones cuando constate que dicho prestador, de forma intencionada o por negligencia: a) infringe las disposiciones pertinentes del Reglamento; b) incumple una decisión por la que se ordenen medidas cautelares; o c) incumple un compromiso que se haya declarado vinculante por medio de una decisión adoptada por la Comisión.

Como medidas de último recurso, si la infracción persiste y causa un perjuicio grave a los usuarios y conlleva delitos penales que supongan una amenaza para la vida o la seguridad de las personas, la Comisión puede solicitar al CSD del Estado miembro en cuestión que pida a los tribunales nacionales una **restricción temporal de acceso de los destinatarios al servicio**, siguiendo un procedimiento específico.

Para más información sobre estos procedimientos, pulsa aquí.

GARRIGUES

Síguenos

La presente publicación contiene información de carácter general, sin que constituya opinión profesional ni asesoramiento jurídico. © J&A Garrigues, S.L.P., 2024. Quedan reservados todos los derechos. Se prohíbe la explotación, reproducción, distribución, comunicación pública y transformación, total y parcial, de esta obra, sin autorización escrita de J&A Garrigues, S.L.P.

J&A Garrigues, S.L.P. Reg. Merc. Madrid: Tomo 17.456, Folio 186, Sección 8ª, Hoja M-190538.
NIF: B81709081. Hermosilla, 3 – 28001 Madrid, España. + 34 91 514 52 00. info@garrigues.com

garrigues.com