S

OMPI
ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL

WIPO/ACE/18/26 REV.
ORIGINAL: INGLÉS
FECHA: 15 DE MAYO DE 2026

Comité Asesor sobre Observancia

Decimoctava sesión
Ginebra, 2 a 4 de junio de 2026

PARTICIPACIÓN DE LOS SERVICIOS INTERMEDIARIOS EN EL BLOQUEO DE SITIOS WEB: CÓMO LOS LEGISLADORES, LOS TRIBUNALES Y LAS INSTITUCIONES ESTÁN CONFIGURANDO EL PAPEL DE LOS INTERMEDIARIOS EN LA LUCHA CONTRA LA PIRATERÍA DE DERECHOS DE AUTOR EN LÍNEA

Contribución elaborada por el Sr. Okke Delfos Visser, vicepresidente principal y consejero general adjunto para asuntos internacionales de la Motion Picture Association, Bruselas (Bélgica) *

RESUMEN

Este trabajo analiza el papel fundamental que desempeñan los servicios intermediarios, que van más allá de los simples proveedores de servicios de Internet, en el bloqueo de sitios web de piratería ilegal en los regímenes de medidas cautelares sin culpa. Las mejores prácticas actuales,[1] la normativa de la Unión Europea (en particular, la Ley de Servicios Digitales), la jurisprudencia y las normas institucionales avalan la participación de una amplia variedad de intermediarios en el bloqueo de sitios web. Entre ellos se encuentran los registradores de nombres de dominio, las redes privadas virtuales (VPN), los motores de búsqueda y las redes de distribución de contenido. De hecho, las investigaciones indican que la participación de una amplia variedad de intermediarios en los procedimientos de bloqueo aumenta significativamente su eficacia y reduce la elusión. Además, se deberían aprovechar las soluciones automatizadas entre los titulares de derechos y los intermediarios pertinentes

* Las opiniones expresadas en este documento son las del autor y no reflejan necesariamente las de la Secretaría ni las de los Estados miembros de la OMPI.

[1] Véase la contribución de la Motion Picture Association a la 17.ª sesión del Comité Asesor sobre Observancia de la OMPI, celebrada del 4 al 6 de febrero de 2025, disponible en https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_17/wipo_ace_17_14_prov.pdf.

(incluidos los proveedores de servicios de Internet) para hacer frente a las numerosas tácticas de elusión desplegadas por los sitios infractores.

I. EFICACIA DEL BLOQUEO DE SITIOS WEB

1. La Motion Picture Association (MPA) actúa como portavoz y defensora a escala mundial de la industria internacional del cine, la televisión y la transmisión en línea.[2] Nuestros estudios miembros son Netflix Studios, LLC, Paramount Pictures Corporation, Prime Video y Amazon MGM Studios, Sony Pictures Entertainment Inc., Universal City Studios LLC, Walt Disney Studios Motion Pictures y Warner Bros. Discovery. La MPA desempeña un papel destacado en la lucha contra la difusión ilegal de contenido protegido por derechos de autor, que perjudica al próspero ecosistema digital. Uno de los principales objetivos de la MPA es reducir o mitigar la piratería mediante estrategias de aplicación de la ley eficaces, lo que incluye la colaboración con intermediarios que puedan prestar servicios en línea a los operadores de piratería.

2. El equipo de protección de contenido de la MPA trabaja a través de la Alianza para la Creatividad y el Entretenimiento (ACE), que es la organización líder mundial en la lucha contra la piratería en línea. La ACE se creó en 2017 por iniciativa de la MPA y ahora agrupa a más de 50 empresas de medios de comunicación y entretenimiento de todo el mundo. La ACE se centra en la aplicación de la ley y la colaboración con organismos gubernamentales y autoridades judiciales para localizar a los operadores y organizaciones piratas y cerrar los servicios ilegales. Juntas, la MPA y la ACE aplican un enfoque integral para combatir la piratería en línea, con un amplio abanico de actividades, tales como la recopilación de información y las investigaciones; la supervisión de la nueva legislación sobre bloqueo de sitios web en todo el mundo; la interposición de acciones de derecho a la información para obtener datos sobre los operadores de piratería de los proveedores de servicios intermediarios; y la solicitud del bloqueo y la eliminación de los sitios web fraudulentos o servicios infractores.

3. En la actualidad, más de 60 países cuentan con sistemas jurídicos que permiten procedimientos administrativos y/o judiciales para bloquear sitios web. La MPA tiene experiencia directa en más de 30 de estos países y ha desarrollado una gran experiencia en este ámbito. Un análisis interno sobre la eficacia de las órdenes de bloqueo de sitios web obtenidas entre 2024 y 2025 comparó el número de visitas a los sitios web antes y después de los bloqueos. Los resultados muestran que el bloqueo por parte de los proveedores de servicios de Internet tradicionales produce una reducción media de las visitas a los sitios web de piratería afectados del 89 %. En países como Italia, Francia, Brasil, Corea del Sur y la India, la reducción media de las visitas tras el bloqueo de sitios web superó el 90 % en 2024.[3]

[2] https://www.motionpictures.org/about/#mission.

[3] Los datos disponibles públicamente también muestran que la eficacia del bloqueo de sitios web oscila entre el 60 % y el 97 % en los distintos países. En relación con el Reino Unido, véase Danaher *et al.*, *The Effect of Piracy Website Blocking on Consumer Behavior*, MIS Quarterly, 631, junio de 2020, pp. 637 y 639 ("los bloqueos de noviembre de 2014 [de 53 sitios web] fueron eficaces para reducir las visitas a los sitios bloqueados. Las visitas a los sitios bloqueados se redujeron en un 88 % entre los tres meses anteriores a los bloqueos y los tres meses posteriores". Refiriéndose a los datos de las oleadas de bloqueos de 2012 y 2013, "las visitas a los sitios bloqueados se reducen entre un 80 % y un 95 % en los distintos grupos, lo que indica un bloqueo eficaz"), disponible en https://www.cmu.edu/entertainment-analytics/documents/effectiveness-of-anti-piracy-efforts/uk-blocking-misq.pdf. En relación con Australia y Corea del Sur, véase MPA, *"Measuring the Effect of Piracy Website Blocking in Australia on Consumer Behavior*", enero de 2020, disponible en https://www.mpa-apac.org/wp-content/uploads/2020/02/Australia-Site-Blocking-Summary-January-2020.pdf (en referencia a un bloqueo de diciembre de 2018, "la visita media a los sitios bloqueados disminuyó drásticamente para el grupo de tratamiento, y la visita a este grupo de sitios se redujo en un 61 % en total desde el periodo previo al periodo posterior"), y MPA, *Estudio de la MPA sobre el impacto del bloqueo de sitios en Corea del Sur*, 2016, p. 11, disponible en https://www.mpa-apac.org/wp-content/uploads/2018/05/MPAA_Impact_of_Site_Blocking_in_South_Korea_2016.pdf ("el impacto de nivel 1 fue claro: las visitas a los sitios bloqueados habían disminuido una media del 90 % tres meses después del bloqueo (97 % tras la oleada 1, 93 % tras la oleada 2 y 79 % tras la oleada 3)").

4. La eficacia del bloqueo de sitios web también se ha medido en términos del aumento del consumo legal en Brasil, la India, el Reino Unido y Australia. Varios estudios han demostrado que el bloqueo de sitios web impulsó el consumo legal en un 5,2 % en Brasil en 2021, y en un 8,1 % y un 3,1 % en la India en 2019 y 2020, respectivamente.[4] En el Reino Unido, un estudio de 2020 estimó que, debido al bloqueo de sitios web, el uso de sitios de suscripción legales aumentó de entre 7 y 12 puntos porcentuales.[5] Por último, en Australia, se produjo un aumento del 5 % en el tráfico hacia sitios web legales de visualización de contenido.[6]

5. Los titulares de derechos invierten enormes cantidades de capital en contenido, y sus ingresos y perspectivas de producción futura se ven gravemente perjudicados por la piratería. Para aumentar aún más la eficacia del bloqueo del acceso a contenido pirateado, es necesaria la intervención y la colaboración de los proveedores de servicios intermediarios en línea a lo largo de toda la cadena de distribución ilegal. Cada vez son más los legisladores, tribunales y organismos administrativos que reconocen esta necesidad.

II. LA DSA SIGUE LOS PASOS DE LA DIRECTIVA DE COMERCIO ELECTRÓNICO DE LA UNIÓN EUROPEA

6. La DSA (Reglamento n.º 2022/2065 de la Unión Europea)[7] es una de las normas más completas en materia de responsabilidad de los intermediarios en línea, directamente aplicable en los 27 Estados miembros de la Unión Europea. Inspirada en la Directiva de la Unión Europea sobre el comercio electrónico y reflejando la mayoría de sus artículos, la DSA ha heredado las mismas reglas de puerto seguro para los meros conductos, los proveedores de almacenamiento en caché y los proveedores de alojamiento, pero también ha aclarado aún más qué intermediarios deben incluirse en esas respectivas categorías.

7. A este respecto, el considerando 29[8] de la DSA resulta de gran utilidad para especificar qué tipo de intermediarios se ajustan a la definición de proveedores de “mero conducto”, entre los que se incluyen las VPN, los servicios del sistema de nombres de dominio (DNS), los resolutores y los registradores, mientras que entre los ejemplos citados de proveedores de

[4] Véase Danaher *et al.*, *The Impact of Online Piracy Website Blocking on Legal Media Consumption*, 12 de febrero de 2024, disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4723522.
[5] Véase Danaher *et al.*, *The Effect of Piracy Website Blocking on Consumer Behavior*, MIS Quarterly, 631, junio de 2020, citado más arriba.
[6] Véase *“Measuring the Effect of Piracy Website Blocking in Australia on Consumer Behavior,* citado en la nota al pie 3.
[7] El texto de la DSA está disponible en https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng.
[8] El considerando 29 de la DSA establece que “los servicios de intermediación abarcan una amplia gama de actividades económicas que se desarrollan en línea y que evolucionan continuamente para permitir una transmisión de la información rápida, segura y protegida, y para garantizar la comodidad de todos los participantes en el ecosistema en línea”. Por ejemplo, los servicios de intermediación de “mero conducto” incluyen categorías genéricas de servicios, tales como puntos de intercambio de Internet, puntos de acceso inalámbrico, redes privadas virtuales, servicios y resolutores de DNS, registros de dominios de nivel superior, registradores, autoridades de certificación que emiten certificados digitales, voz sobre IP y otros servicios de comunicación interpersonal, mientras que los ejemplos genéricos de servicios de intermediación de “almacenamiento en caché” incluyen la mera provisión de redes de distribución de contenido, proxis inversos o proxis de adaptación de contenido. Dichos servicios son cruciales para garantizar la transmisión fluida y eficiente de la información distribuida en Internet. Entre los ejemplos de “servicios de alojamiento” se incluyen categorías de servicios como la computación en la nube, el alojamiento web, los servicios de posicionamiento de pago o los servicios que permiten la difusión de información y contenido en línea, incluido el almacenamiento y el intercambio de archivos. Los servicios de intermediación pueden prestarse de forma aislada, como parte de otro tipo de servicio de intermediación, o simultáneamente con otros servicios de intermediación. El hecho de que un servicio específico constituya un servicio de “mero conducto”, de “almacenamiento en caché” o de “alojamiento” depende exclusivamente de sus funciones técnicas, que pueden evolucionar con el tiempo, y debe evaluarse caso por caso.

"almacenamiento en caché" se encuentran las redes de distribución de contenido (CDN) y los proxis inversos.[9]

8. Además, el considerando 25[10] subraya la importancia de garantizar que las medidas cautelares sin culpa se apliquen a los intermediarios que, aunque no sean responsables, tienen sin embargo la capacidad técnica para intervenir y poner fin o impedir una infracción, incluso desactivando el acceso a contenido ilegal específico.

9. Por último, el considerando 31[11] reconoce que, en función del sistema jurídico de cada Estado miembro, las autoridades judiciales o administrativas nacionales pueden ordenar a los prestadores de servicios de intermediación que tomen medidas contra los contenidos ilícitos o que faciliten información específica. Esto guarda coherencia con los artículos 4 a 6 de la DSA, que preservan la posibilidad de que las autoridades judiciales o administrativas exijan a los proveedores de servicios de intermediación que pongan fin a las infracciones o las impidan, entre otras cosas retirando los contenidos ilícitos o inhabilitando el acceso a los mismos. La DSA no crea por sí misma una nueva base jurídica sustantiva para las órdenes de bloqueo de sitios protegidos por derecho de autor. Antes bien, preserva y complementa los marcos jurídicos vigente, nacionales y de la UE, incluido el artículo 8.3, de la Directiva 2001/29/CE13.[12]

10. Cabe señalar que esta infraestructura jurídica no constituye una invención sin precedentes de la Unión Europea, ni se aplica únicamente en ella, como se destaca a continuación en relación con la jurisprudencia india. De hecho, se deriva del artículo 14, apartado 2, del Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre Derecho de Autor de 1996,[13] que aborda la protección de los derechos de autor y derechos conexos en el entorno digital, y que obliga a las Partes Contratantes a garantizar que sus legislaciones dispongan de procedimientos de ejecución que permitan actuar eficazmente contra cualquier acto de infracción de los derechos contemplados en el Tratado, incluyendo

[9] Los tribunales europeos ya están recurriendo a la DSA para ampliar el alcance de las medidas cautelares sin culpa a otros tipos de intermediarios con el fin de proteger las obras protegidas por derechos de autor, como el Tribunal Civil de París, que, en su sentencia de 28 de marzo de 2025 en el asunto Canal Plus contra Cloudflare Inc., declaró que "Los proveedores de sistemas de resolución de nombres de dominio y de redes de distribución de contenido, que están expresamente cubiertos por el mencionado Reglamento DSA, sin perjuicio de las exenciones de responsabilidad de las que puedan gozar por otros conceptos, desempeñan una función de transmisión".

[10] El considerando 25 de la DSA establece que "Las exenciones de responsabilidad establecidas en el presente Reglamento no deben afectar a la posibilidad de dictar medidas cautelares de diversa índole contra los proveedores de servicios de intermediación, incluso cuando cumplan las condiciones establecidas en el marco de dichas exenciones. Dichas medidas cautelares podrían consistir, en particular, en órdenes de los tribunales o de las administraciones, dictadas de conformidad con el Derecho de la Unión, que exijan la cesación o la prevención de cualquier infracción, incluida la retirada del contenido ilícito especificado en dichas órdenes, o la inhabilitación del acceso a los mismos".

[11] El considerando 31 de la DSA establece que "En función del sistema jurídico de cada Estado miembro y del ámbito del Derecho de que se trate, las administraciones judiciales o administrativas nacionales, incluidas las autoridades policiales, pueden ordenar a los prestadores de servicios de intermediación que actúen contra uno o varios contenidos ilícitos específicos o que faciliten determinada información específica. Las legislaciones nacionales en las que se basan dichas órdenes difieren considerablemente y las órdenes se dictan cada vez más en situaciones transfronterizas. A fin de garantizar que dichas órdenes puedan cumplirse de manera eficaz y eficiente, en particular en un contexto transfronterizo, de modo que las Administraciones públicas competentes puedan desempeñar sus tareas y los prestadores no se vean sometidos a cargas desproporcionadas, sin afectar indebidamente a los derechos e intereses legítimos de terceros, es necesario establecer determinadas condiciones que deben cumplir dichas órdenes y ciertos requisitos complementarios relativos a su tramitación. En consecuencia, el presente Reglamento debe armonizar únicamente determinadas condiciones mínimas específicas que deben cumplir dichas órdenes para que surja la obligación de los prestadores de servicios de intermediación de informar a las Administraciones competentes sobre el cumplimiento de dichas órdenes. Por lo tanto, el presente Reglamento no establece la base jurídica para la emisión de dichas órdenes, ni regula su ámbito territorial o su ejecución transfronteriza.

[12] El artículo 8, apartado 3, de la Directiva 2001/29/CE establece que "los Estados miembros velarán por que los titulares de derechos puedan solicitar medidas cautelares contra los intermediarios cuyos servicios sean utilizados por un tercero para infringir un derecho de autor o los derechos conexos".

[13] El texto del Tratado de la OMPI sobre Derecho de Autor (WCT) está disponible en https://www.wipo.int/wipolex/en/text/295166.

medidas correctivas rápidas para prevenir las infracciones y medidas correctivas que actúen como elemento disuasorio frente a nuevas infracciones.

III. PARTICIPACIÓN DE OTROS TIPOS DE INTERMEDIARIOS EN LA PRÁCTICA

11. En la era tecnológica actual, el contenido pirateado se consume principalmente en línea. Desde principios de la década de 2000, el aumento de la jurisprudencia favorable ha permitido a los titulares de derechos obtener medidas cautelares sin necesidad de demostrar culpa, que inicialmente eran estáticas y, posteriormente, dinámicas, ordenando a los proveedores de servicios de Internet que bloquearan el acceso a sitios y servicios piratas. En los casos en que se disponía de la información pertinente, la aplicación de la ley se dirigió directamente contra los operadores de piratería y los proveedores de alojamiento. Sin embargo, la experiencia práctica ha demostrado que los operadores a menudo se esconden tras identidades ficticias o robadas, y no acatan las cartas de cese y desistimiento. Por su parte, los servidores de alojamiento suelen ser imposibles de rastrear, protegidos por técnicas de anonimización o por el hecho de estar ubicados en países donde la aplicación de la ley resulta extremadamente difícil.

12. La colaboración con todos los intermediarios de la cadena de la piratería es esencial, ya que cada uno de ellos puede intervenir de manera eficaz, dentro de sus ámbitos de competencia, y con las medidas más adecuadas. Este enfoque mejora la eficacia y el alcance de las órdenes de bloqueo, al tiempo que reduce las formas de eludirlas. Entre los intermediarios clave, se incluyen los sistemas de búsqueda, los registradores de dominios, las redes de distribución de contenido, las VPN y los servicios DNS alternativos.

A. Suspensión de dominios y su eficacia

13. Los registradores de nombres de dominio (DNR) registran nombres de dominio a cambio de una tarifa en nombre de los registrantes, es decir, los propietarios de sitios web, de modo que la dirección IP alfanumérica utilizada para un dominio pueda ser fácilmente encontrada por las personas a través de los sistemas de búsqueda.

14. Recientemente, en cumplimiento de órdenes judiciales, los registradores de nombres de dominio (DNR) han suspendido dominios ilegales con efecto mundial, lo que ha impedido el acceso a numerosos sitios web desde cualquier parte del mundo. Desde 2023,[14] el Tribunal Superior de Delhi (India) ha venido dictando órdenes que obligan a los DNR, independientemente de su ubicación, a bloquear y suspender los nombres de dominio infractores. En 2025, las órdenes judiciales se ampliaron a las aplicaciones infractoras y otros servicios, protegiendo las retransmisiones en tiempo real.[15] En la orden dictada a favor de Star India, con fecha del 29 de mayo de 2025, el Tribunal Superior de Delhi declaró lo siguiente:

> “En la nueva era tecnológica, hoy en día resulta cada vez más fácil y cómodo para los infractores crear variantes alfanuméricas, espejo o de redireccionamiento de sitios web fraudulentos, y para cuando se pueda llevar a cabo la incorporación de terceros y la subsanación de las medidas cautelares, ciertas actividades infractoras sensibles al factor tiempo, como la transmisión en directo de eventos deportivos, ya han comenzado de forma ilegal y, para cuando la parte afectada, como el demandante, acude a este Tribunal, ya es demasiado tarde”, ordenando a los Registradores que “suspendan el registro de los nombres de dominio, las URL y las interfaces de usuario infractoras notificadas por el demandante en tiempo real”.

[14] Véase Universal City Studios LLC. y otros contra Dotmovies.baby y otros, CS(COMM) 514/2023.
[15] Véase Star India Private Limited contra IPTV Smarters, caso CS(COMM) 108/2025, 29 de mayo de 2025. Véase también Dazn Limited & Anr contra Buffsports. Me y otros, CS(COMM) 536/2025, 28 de mayo de 2025.

15. Como resultado, varios registradores de todo el mundo han cumplido estas órdenes judiciales suspendiendo dominios a escala mundial y proporcionando información sobre los operadores de piratería.[16] Sin embargo, algunos registradores siguen sin cumplir las órdenes judiciales, lo que subraya la necesidad de una mayor colaboración y concienciación sobre su papel fundamental.

16. Un análisis interno de 275 sitios web de piratería populares bloqueados en la India reveló que[17] durante los tres meses anteriores y posteriores a las órdenes, las visitas a los 138 dominios bloqueados y suspendidos disminuyeron un 11 % adicional en comparación con las visitas a los 137 restantes, bloqueados únicamente a nivel local por los proveedores de servicios de Internet. El impacto mundial fue aún mayor: los dominios que también fueron bloqueados en otros países y suspendidos por los registradores disminuyeron, de media, un 44 % más que aquellos que solo fueron bloqueados. En general, las visitas mundiales a sitios bloqueados y suspendidos disminuyeron un 99 % entre julio de 2024 y julio de 2025, ya que la suspensión de un dominio suele hacer que este no esté disponible para cualquier solución alternativa al bloqueo de sitios, como el uso de VPN y servicios DNS alternativos.[18]

B. Bloqueo de redes de distribución de contenido

17. A lo largo de la cadena de distribución de contenido pirateado, diversos servicios ilegales también se aprovechan de los servidores proxis inversos y los servicios de CDN.[19] Se han logrado algunos avances, entre ellos interfaces de programación de aplicaciones (API) específicas para que los titulares de derechos soliciten más información sobre los dominios que ocultan su dirección IP real tras servidores proxis inversos; un trato favorable para los denominados “denunciantes de confianza”; y medidas tecnológicas para bloquear el acceso a contenido ilegal a nivel de CDN.[20]

18. La aplicación rigurosa de los bloqueos de acceso a las CDN podría reducir sustancialmente las visitas a los sitios piratas; sin embargo, siguen existiendo importantes retos. El principal de ellos es la capacidad de los operadores de sitios piratas para registrar un número casi infinito de dominios en sus cuentas de CDN y gestionarlos fácilmente, de modo que, tan pronto como se bloquea el dominio actual, este es sustituido por un nuevo dominio, que entra en funcionamiento de inmediato.

[16] En la sentencia del caso Star India contra IPTV Smarters, el Tribunal ordenó a los demandados “que revelaran todos los datos, tales como el nombre y la dirección, junto con los datos de pago relativos a dichos sitios web y aplicaciones móviles fraudulentos”.
[17] “Dominio popular” se refiere a un sitio web con más de 50 000 visitas en todo el mundo durante el mes de la suspensión.
[18] Si bien cabe esperar que los dominios suspendidos y bloqueados dejen de estar disponibles por completo (disminución del 100 % de las visitas), la diferente magnitud de la disminución puede deberse a imprecisiones en la comunicación de las fechas efectivas de suspensión de los dominios, así como a visitas residuales procedentes de enlaces antiguos.
[19] Véanse los informes de la Lista de Vigilancia de la Unión Europea sobre Falsificación y Piratería de 2025 y 2022. Disponibles en https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2025)132&lang=en; y https://circabc.europa.eu/ui/group/d0803128-7d62-40ee-8349-c43ee92745aa/library/b36f701d-2850-4768-9b3e-e487140e11e5/details?download=true.
[20] En varias ocasiones, LaLiga española ha confirmado que ha llegado a acuerdos con Akamai Technologies y CDN77 para eliminar contenido que infringe los derechos de autor, incluso en tiempo real. Véase https://www.panoramaaudiovisual.com/2025/04/04/laliga-trabaja-cdn77-akamai-lucha-contra-pirateria/. Véase también la sentencia del Tribunal Civil de París de 28 de marzo de 2025, citada anteriormente. Asimismo, Cloudflare declaró que es posible llegar a acuerdos voluntarios con los titulares de derechos para aplicar bloqueos geográficos a sitios web a través de sus CDN y sus servicios de seguridad, tal y como hizo en el Reino Unido. Véase la noticia del blog de Cloudflare en https://blog.cloudflare.com/h1-2025-transparency-report/.

C. Eliminación oportuna de resultados en los sistemas de búsqueda

19. La exclusión de los resultados de búsqueda consiste en eliminar páginas web o enlaces concretos de los resultados de los sistemas de búsqueda, de modo que dejen de aparecer en el índice de búsqueda para determinadas consultas. Australia fue el primer país en incluir, de forma obligatoria, en su Ley de Derechos de Autor las medidas cautelares relativas a los "proveedores de motores de búsqueda en línea" y a la exclusión de los listados, lo que dio lugar a acuerdos voluntarios con los principales motores de búsqueda, que ahora aplican esta práctica en diversos países. Otro ejemplo es la sentencia del Tribunal Supremo francés en el caso Allostreaming,[21] en la que el Tribunal exigió a los proveedores de motores de búsqueda que eliminaran de sus índices los sitios web que infringieran la ley de forma sistemática, en virtud de la transposición francesa del artículo 8, apartado 3, de la Directiva sobre la sociedad de la información.

20. Cuando se combina con el bloqueo de sitios web, la eliminación de los resultados de búsqueda tiene un impacto significativo en la reducción del número total de visitas a sitios web fraudulentos. Las investigaciones internas muestran que la eliminación oportuna de los resultados de búsqueda, llevada a cabo poco después del bloqueo local por parte de los proveedores de servicios de Internet, provoca una disminución media del tráfico un 25 % mayor que en los casos en los que no se ha llevado a cabo dicha eliminación oportuna.

21. Si los nombres de los sitios piratas (marcas piratas) y los últimos dominios activos siguen apareciendo en los primeros puestos de los resultados de los sistemas de búsqueda, a los usuarios de Internet siempre les resultará relativamente fácil encontrarlos, independientemente de cualquier bloqueo previo. Por esta razón, la colaboración y las medidas oportunas y diligentes por parte de los sistemas de búsqueda siguen siendo esenciales.

D. VPN y bloqueo de DNS alternativos para evitar tácticas de elusión

22. Las VPN y los servicios de DNS alternativos son intermediarios que pueden permitir el acceso a dominios bloqueados por los proveedores de servicios de Internet locales. Si bien pueden utilizarse legítimamente por motivos de privacidad, se emplean cada vez más como herramientas de elusión. Recientemente, la legislación y la jurisprudencia francesas e italianas han incluido este tipo de intermediarios en el ámbito de aplicación de sus regímenes de bloqueo de sitios web.

23. En Italia, la versión actual de la ley contra la piratería[22] incluye ambos tipos de intermediarios entre aquellos que pueden ser objeto de órdenes impuestas por la Administración nacional de telecomunicaciones (AGCOM).[23] En Francia, entre 2024 y 2025, el Tribunal Civil de París dictó varias órdenes de bloqueo de sitios web contra servicios de VPN y

[21] Véase el Tribunal Supremo francés, 6 de julio de 2017, ECLI:FR:CCASS:2017:C100909. Se exigió a Google, Microsoft Bing y Yahoo! que eliminaran de sus índices los sitios que infringían de forma sistemática, de conformidad con la transposición francesa del art. 8, apartado 3, de la Directiva 2001/29/CE, que permite a los titulares de derechos solicitar medidas proporcionadas contra cualquier persona que pueda contribuir a subsanar las infracciones. Según la jurisprudencia del caso *Allostreaming*, se puede exigir a los proveedores de servicios de Internet y a los motores de búsqueda que asuman íntegramente los costes de las medidas, siempre que la orden deje al intermediario libertad para determinar las medidas concretas necesarias para obtener el resultado deseado y no exija un "sacrificio insoportable".

[22] Ley n.º 93/2023.

[23] Por ejemplo, Google parece haber dado pasos positivos en la colaboración en el bloqueo en tiempo real a nivel de DNS alternativo; véase la declaración pública de la AGCOM sobre la colaboración con Google, disponible en https://www.agcom.it/comunicazione/comunicati-stampa/comunicato-stampa-39, mientras que la colaboración con las VPN parece menos evidente, dado que estas se muestran muy reacias a cumplir.

DNS alternativos de renombre.[24] El Tribunal determinó que estos intermediarios pueden contribuir a subsanar las infracciones con sus actividades de transmisión de datos, también de conformidad con las disposiciones de la DSA que los califican como servicios intermediarios. En consonancia con la jurisprudencia del Tribunal de Justicia de la Unión Europea,[25] las medidas se consideraron proporcionadas, ya que tenían una duración limitada y dejaban a los intermediarios libertad para seleccionar los medios técnicos más adecuados, sin imponer una obligación general de supervisión.

IV. ÓRDENES JUDICIALES FLEXIBLES PARA HACER FRENTE A LAS ESTRUCTURAS DE PIRATERÍA EN CONSTANTE EVOLUCIÓN

24. Una novedad reciente en el Reino Unido ilustra cómo los tribunales están adaptando los marcos de las órdenes judiciales para hacer frente a la naturaleza cambiante de la piratería en línea. Partiendo de la dilatada jurisprudencia británica en materia de bloqueo de sitios web en virtud del artículo 97A de la Ley de Derechos de Autor, Diseños y Patentes, que incluye las órdenes tradicionales de bloqueo de sitios web y las posteriores órdenes contra marcas piratas, el Tribunal Superior de Justicia ha dictado ahora una orden “ómnibus” de bloqueo de sitios web de mayor alcance.[26]

25. Esta orden permite a los titulares de derechos solicitar el bloqueo de servicios de piratería audiovisual que infrinjan la ley de forma sistemática y que cumplan criterios definidos, sin tener que presentar una nueva solicitud judicial para cada nuevo dominio o nombre de sitio disponible en el futuro. Esto es especialmente importante cuando los operadores de piratería utilizan nombres genéricos, descriptivos o que cambian con frecuencia para evitar quedar sujetos a órdenes basadas en marcas o específicas de dominios.

26. El Tribunal aceptó que esta forma más amplia de subsanación era necesaria y proporcionada a la luz de la magnitud y la naturaleza cambiante del problema de las infracciones en línea, la carga operativa que suponen las solicitudes repetidas y el uso responsable demostrado de las medidas de bloqueo de sitios web por parte de los titulares de derechos a lo largo de muchos años. La orden tiene una duración de seis meses y puede prorrogarse en función de una obligación de información posterior, que exige a los titulares de derechos presentar al tribunal información sobre su aplicación y eficacia, preservando así la supervisión judicial y la rendición de cuentas. Este tipo de orden no requiere ampliar la responsabilidad de los intermediarios, sino garantizar que los mecanismos de medidas cautelares sin culpa existentes sigan siendo eficaces en la práctica en entornos digitales en rápida evolución.

[24] En lo que respecta a las VPN, véanse las sentencias dictadas en los siguientes asuntos del Tribunal Civil de París: n.º 24/14722, de 15 de mayo de 2025, y n.º 25/05198, de 18 de julio de 2025, ambos entre Canal+ y Express Technologies, Expressco Services, Cyberghost, Proton, NordVPN y Surfshark. Los servicios de DNS alternativos fueron objeto de las siguientes sentencias del Tribunal Civil de París: n.º 23/14722 y n.º 23/14726, de 16 de mayo de 2024; n.º 23/14731, de 30 de mayo de 2024; n.º 24/06759, de 12 de septiembre de 2024; n.º 24/11187 y 24/11188, de 24 de octubre de 2024, Canal + contra Google, Cloudflare y Cisco, n.º 24/12413, 24/12414, de 5 de diciembre de 2024, Canal + contra Vercara LLC y Quad9, y n.º 24/12415, de 5 de diciembre de 2024, Canal + contra Google, Cloudflare y Vercara. Estos casos se interpusieron basándose en la amplia definición contenida en el artículo 333-10 del Código del Deporte francés, de “cualquier persona que pueda contribuir a subsanar” la violación de los derechos de explotación audiovisual, lo que permite incluir los servicios de VPN y DNS alternativos en esta categoría. El Tribunal ordenó a los proveedores de DNS alternativos que aplicaran, en el marco de sus respectivos servicios de resolución de nombres de dominio, “todas las medidas de bloqueo adecuadas para impedir el acceso desde el territorio francés, por cualquier medio eficaz, y en particular mediante el bloqueo de los nombres de dominio o subdominios, a los sitios web señalados”.

[25] Véase la sentencia del Tribunal de Justicia de la Unión Europea C-314/12, de 24 de marzo de 2014, UPC Telekabel Wien GmbH contra Constantin Film Verleih GmbH.

[26] Véase la sentencia del Tribunal Superior de Justicia, [2026] EWHC 1087 (Ch), de 7 de mayo de 2026, Columbia Pictures Industries, Inc. y otros contra British Telecommunications Plc y otros.

27. Esta novedad es especialmente relevante a la luz de los recientes cambios en el comportamiento técnico y operativo de los operadores de piratería. Aunque no se tiene constancia de que los sistemas de "IA agentiva" totalmente autónomos se utilicen aún de forma generalizada en el ecosistema de la piratería, varios avances tecnológicos ya están reduciendo sustancialmente las barreras para el cambio de dominio a gran escala y los esquemas evasivos, de modo que los operadores piratas pueden ahora desplegar rápidamente sitios de transmisión en línea clonados utilizando bases de código de libre acceso y sistemas automatizados de registro de dominios de bajo coste, a menudo combinados con API de registro masivo y estrategias de migración basadas en redireccionamientos. Como resultado, los servicios infractores operan cada vez más a través de redes rotativas de dominios, incluyendo nombres genéricos o no relacionados con marcas, diseñados específicamente para eludir las medidas tradicionales de bloqueo específicas de dominios o basadas en marcas. En algunos casos, los operadores mantienen múltiples dominios intercambiables con una infraestructura, bibliotecas de contenido y funcionalidad sustancialmente idénticas, lo que permite a los usuarios ser redirigidos sin problemas a dominios sustitutivos.

V. AUTOMATIZACIÓN

28. Otro fenómeno que está cobrando impulso es la adopción de plataformas automatizadas, no solo para coordinar mejor las solicitudes de los titulares de derechos, sino también para dar cabida a los más diversos servicios intermediarios en sus actividades de bloqueo. Estas pueden funcionar de acuerdo con las mejores prácticas, respetando las garantías procesales, los principios de transparencia y proporcionalidad, y las salvaguardias procesales, lo que permite a los titulares de derechos comunicarse directamente con los intermediarios, con o sin la supervisión de una autoridad independiente.

29. Este enfoque automatizado facilitaría la colaboración entre las partes y la haría más eficiente, permitiendo un bloqueo y desbloqueo rápidos, lo que también resulta adecuado para conciliar la necesidad de proteger en tiempo real el contenido transmitido ilegalmente. Por lo tanto, debería alentarse la adopción de dichos sistemas, sustituyendo la comunicación por correo electrónico con archivos adjuntos, que suele requerir tiempos de tramitación más largos y entraña una mayor complejidad.

30. Algunas autoridades administrativas nacionales[27] ya se han dotado de plataformas automatizadas o semiautomatizadas que se mejoran constantemente y permiten un bloqueo y desbloqueo rápidos, así como una comunicación fluida entre los titulares de derechos, los intermediarios y las autoridades de supervisión. Los tribunales parecen alentar los medios automatizados de actualización y notificación entre los titulares de derechos y los intermediarios.[28] Sin embargo, entidades privadas como la MPA también se están dotando de instrumentos similares, que facilitan la detección de infracciones, la obtención de pruebas y la comunicación con los intermediarios.

[27] Algunos ejemplos conocidos son la AGCOM en Italia, la Organización Helénica de Derechos de Autor (EDPPI) en Grecia, la Inspección General de Actividades Culturales (IGAC) en Portugal y la Administración Nacional de Telecomunicaciones (ANATEL) en Brasil.
[28] Véase la sentencia del Tribunal Federal Civil y Comercial de Argentina (Sala XI), de 7 de abril de 2025, n.º 4426/2025, Warner Bros. Entertainment Inc. y otros contra Pelisplushd.bz y otros.

V. CONCLUSIÓN

31. Los datos empíricos muestran que una mayor colaboración de diversos intermediarios en la prevención del acceso a sitios y servicios ilegales conduce a un bloqueo más eficaz y a una mayor protección de la propiedad intelectual.

32. Con el fin de aumentar la eficiencia y mejorar la armonización con los sistemas de los intermediarios, debería utilizarse en mayor medida la automatización y las herramientas tecnológicas para combatir la piratería, lo que permitiría reducir costes y cargas a largo plazo. Este enfoque ayudará a combatir la piratería y sus futuras evoluciones, protegiendo tanto a los titulares de los derechos como, en última instancia, a los propios usuarios, que se exponen a riesgos para su seguridad al usar sitios web piratas, como el robo de identidad o la infección por programas maliciosos.

[Fin de la contribución]