E

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

WIPO/ACE/18/26 REV.
ORIGINAL: ENGLISH
DATE: MAY 15, 2026

Advisory Committee on Enforcement

Eighteenth Session
Geneva, June 2 to 4, 2026

INVOLVEMENT OF INTERMEDIARY SERVICES IN SITE BLOCKING: HOW LAWMAKERS, COURTS, AND INSTITUTIONS ARE SHAPING THE ROLE OF INTERMEDIARIES IN ADDRESSING ONLINE COPYRIGHT PIRACY

Contribution prepared by Mr. Okke Delfos Visser, Senior Vice President, Associate General Counsel, International, Motion Picture Association, Brussels, Belgium[*]

ABSTRACT

This contribution explores the critical role played by intermediary services, beyond simply Internet service providers (ISPs), to block illegal piracy sites in no-fault injunction regimes. Current best practices,[1] regulations (particularly the Digital Services Act (DSA) of the European Union (EU)), case law, and institutional rules all support the involvement of a broad range of intermediaries in site blocking. Examples include domain name registrars, virtual private networks (VPNs), search engines and content delivery networks. In fact, research indicates that involving a broad range of intermediaries in blocking procedures significantly enhances the effectiveness of the measures and reduces circumvention. Also, automated solutions between rights holders and relevant intermediaries, including ISPs, should be leveraged to address the myriad circumvention tactics deployed by infringing sites.

[*] The views expressed in this document are those of the author and not necessarily those of the Secretariat or of the Member States of WIPO.

[1] See the Motion Picture Association contribution to the Seventeenth Session of the Advisory Committee on Enforcement at WIPO, February 4–6, 2025, available at https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_17/wipo_ace_17_14_prov.pdf.

I. EFFECTIVENESS OF SITE BLOCKING

1. The Motion Picture Association (MPA) serves as the global voice of and advocate for the international film, television and streaming industry.[2] Our member studios are Netflix Studios, LLC, Paramount Pictures Corporation, Prime Video & Amazon MGM Studios, Sony Pictures Entertainment Inc., Universal City Studios LLC, Walt Disney Studios Motion Pictures, and Warner Bros. Discovery. MPA plays a leading role in tackling the illegal dissemination of copyright-protected content, which harms the thriving digital ecosystem. One of the main goals of MPA is to reduce or mitigate piracy through effective enforcement strategies, including by collaborating with intermediaries that may provide online services to piracy operators.

2. The MPA content protection team works through the Alliance for Creativity and Entertainment (ACE), which is the world's leading online anti-piracy organization. ACE was created in 2017 at the initiative of MPA and now brings together over 50 media and entertainment companies worldwide. ACE focuses on enforcement and collaboration with government agencies and judicial authorities to identify piracy operators and organizations and shut down illegal services. Together, MPA and ACE apply a 360-degree approach to tackle online piracy, with a broad spectrum of activities, such as intelligence gathering and investigations; monitoring new site blocking legislation worldwide; pursuing right of information (ROI) actions to obtain data on piracy operators from intermediary service providers; and requesting the blocking and delisting of infringing websites or services.

3. Currently, more than 60 countries have legal systems that allow for administrative and/or judicial site blocking procedures. MPA has direct experience in over 30 of these countries and has developed significant expertise in this area. Internal data-driven analysis on the effectiveness of site blocking orders obtained between 2024 and 2025 compared the number of website visits before and after the blocks. Results show that blocking by traditional ISPs yields an average reduction in visits to targeted piracy websites of 89 per cent. In countries such as Italy, France, Brazil, South Korea and India, the average reduction in visits after site blocking surpassed 90 per cent in 2024.[3]

4. The effectiveness of site blocking has also been measured in terms of the increase in legal consumption in Brazil, India, the United Kingdom and Australia. Several studies have shown that site blocking boosted legal consumption by 5.2 per cent in Brazil in 2021 and by 8.1 and 3.1 per cent in India in 2019 and 2020 respectively.[4] In the United Kingdom, a 2020 study assessed that due to site blocking the use of legal subscription sites increased of between 7

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

[3] Publicly available data also shows that the effectiveness of site blocking ranges between 60 per cent and 97 per cent across different countries. In relation to the United Kingdom, see Danaher et al., *The Effect of Piracy Website Blocking on Consumer Behavior*, MIS Quarterly, 631, June 2020, pp. 637 and 639 ("the November 2014 blocks [of 53 sites] were effective at reducing visits to blocked sites. Visits to blocked sites dropped by 88% from the three months before the blocks to the 3 months after." Referring to data from blocking waves in 2012 and 2013, "visits to blocked sites drop by 80 to 95% across the various groups, indicating an effective block"), available at https://www.cmu.edu/entertainment-analytics/documents/effectiveness-of-anti-piracy-efforts/uk-blocking-misq.pdf. In relations to Australia and South Korea, see MPA, *Measuring the Effect of Piracy Website Blocking in Australia on Consumer Behavior*, January 2020, available at https://www.mpa-apac.org/wp-content/uploads/2020/02/Australia-Site-Blocking-Summary-January-2020.pdf (referring to a December 2018 block, "average visitation to blocked sites declined sharply for the treatment group, with visitation to this group of sites was [sic] down 61% overall from the pre-period to the post-period"), and MPA, *MPA Study on Site Blocking Impact in South Korea*, 2016, p. 11, available at https://www.mpa-apac.org/wp-content/uploads/2018/05/MPAA_Impact_of_Site_Blocking_in_South_Korea_2016.pdf ("the Level 1 impact was clear: visits to blocked sites had declined on average 90% as of three months after a block (97% after Wave 1, 93% after Wave 2 and 79% after Wave 3)".)

[4] See Danaher et al., *The Impact of Online Piracy Website Blocking on Legal Media Consumption*, February 12, 2024, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4723522.

and 12 percentage points.[5] Lastly, in Australia there was an increase of 5 per cent in traffic to legal content-viewing sites.[6]

5. Rights holders invest enormous amounts of capital into content, and their revenues and future production prospects are severely damaged by piracy. To further increase the effectiveness of blocking access to pirated content, the intervention and collaboration of online intermediary service providers throughout the illegal distribution chain is necessary. This need is being recognized by an increasing number of legislators, courts and administrative bodies.

II. THE DSA IN THE FOOTSTEPS OF THE EU E-COMMERCE DIRECTIVE

6. The DSA (EU Regulation No. 2022/2065)[7] is one of the most comprehensive pieces of legislation on responsibility of online intermediaries, directly applicable in all 27 EU member States. Building upon the EU Directive on electronic commerce and mirroring most of its articles, the DSA has inherited the same safe harbor rules for mere conduits, caching and hosting providers, but has also further clarified which intermediaries should fall into those respective categories.

7. In this regard, Recital 29[8] of the DSA is extremely helpful in specifying what kind of intermediaries fit the definition of “mere conduit” providers, including VPNs, domain name system (DNS) services, resolvers and registrars, while cited examples of “caching” providers include content delivery networks (CDNs) and reverse proxies.[9]

8. In addition, Recital 25[10] underscores the significance of ensuring that no-fault injunctions cover intermediaries that, while not liable, nevertheless have the technical capability to intervene and terminate or prevent an infringement, including by disabling access to specific illegal content.

---

[5] See Danaher et al., *The Effect of Piracy Website Blocking on Consumer Behavior*, MIS Quarterly, 631, June 2020, cited above.
[6] See *Measuring the Effect of Piracy Website Blocking in Australia on Consumer Behavior* cited in footnote 3.
[7] The text of the DSA is available at https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng.
[8] DSA Recital 29 provides that "Intermediary services span a wide range of economic activities which take place online and that develop continually to provide for transmission of information that is swift, safe and secure, and to ensure convenience of all participants of the online ecosystem. For example, ‘mere conduit’ intermediary services include generic categories of services, such as internet exchange points, wireless access points, virtual private networks, DNS services and resolvers, top-level domain name registries, registrars, certificate authorities that issue digital certificates, voice over IP and other interpersonal communication services, while generic examples of ‘caching’ intermediary services include the sole provision of content delivery networks, reverse proxies or content adaptation proxies. Such services are crucial to ensure the smooth and efficient transmission of information delivered on the internet. Examples of ‘hosting services’ include categories of services such as cloud computing, web hosting, paid referencing services or services enabling sharing information and content online, including file storage and sharing. Intermediary services may be provided in isolation, as a part of another type of intermediary service, or simultaneously with other intermediary services. Whether a specific service constitutes a ‘mere conduit,’ ‘caching’ or ‘hosting’ service depends solely on its technical functionalities, which might evolve in time, and should be assessed on a case-by-case basis."
[9] European courts are already referring to the DSA to extend the scope of the no-fault injunctions to other kinds of intermediaries to protect copyrighted works, such as the Paris Civil Court, that, in its judgement of 28 March 2025 in the case Canal Plus vs Cloudflare Inc., stated that "Providers of domain name resolution systems and content delivery network, which are expressly covered by the aforementioned DSA Regulation, notwithstanding any exemptions from liability they may otherwise enjoy, perform a transmission function."
[10] DSA Recital 25 states that "The exemptions from liability established in this Regulation should not affect the possibility of injunctions of different kinds against providers of intermediary services, even where they meet the conditions set out as part of those exemptions. Such injunctions could, in particular, consist of orders by courts or administrative authorities, issued in compliance with Union law, requiring the termination or prevention of any infringement, including the removal of illegal content specified in such orders, or the disabling of access to it."

9. Lastly, Recital 31[11] of the DSA acknowledges that, depending on the legal system of each Member State, national judicial or administrative authorities may order providers of intermediary services to act against illegal content or to provide specific information. This is consistent with Articles 4 to 6 of the DSA, which preserve the possibility for judicial or administrative authorities to require intermediary service providers to terminate or prevent infringements, including by removing illegal content or disabling access to it. The DSA does not itself create a new substantive legal basis for copyright site blocking orders. Rather, it preserves and complements existing EU and national legal frameworks, including Article 8(3) of the Directive 2001/29/EC,[12] while setting certain procedural requirements for orders addressed to intermediary service providers.

10. It should be noted that this legal infrastructure does not constitute an unprecedented invention by the EU, nor is it applied only there, as highlighted below in relation to Indian jurisprudence. In fact, it stems from Article 14(2) of the World Intellectual Property Organization (WIPO) Copyright Treaty of 1996[13] addressing the protection of copyrights and related rights in the digital environment, which obligates contracting Parties to ensure that enforcement procedures are available under their law to permit effective action against any act of rights infringement covered by the Treaty, including expeditious remedies to prevent infringements and remedies to act as a deterrent to further infringements.

III. INVOLVEMENT OF OTHER KINDS OF INTERMEDIARIES IN PRACTICE

11. In the current technological age, pirated content is mostly consumed online. Since the early 2000s, an increase in favorable case law has allowed rights holders to obtain no-fault injunctions that were initially static and later dynamic, ordering ISPs to block access to pirate sites and services. In cases where the relevant information was available, enforcement directly targeted piracy operators and hosting providers. However, hands-on experience has shown that operators often hide behind fictitious or stolen identities and do not comply with cease-and-desist letters. Meanwhile, hosting servers are often untraceable, shielded by anonymization techniques or by the virtue of being located in countries where legal enforcement is extremely difficult.

12. Collaboration with all intermediaries in the piracy chain is essential, as each can intervene effectively within their areas of competence and with the most appropriate measures. This approach enhances the efficiency and reach of blocking orders, while reducing circumvention. Key intermediaries include search engines, domain registrars, content delivery networks, VPNs and alternative DNS services.

---

[11] DSA Recital 31 provides that "Depending on the legal system of each Member State and the field of law at issue, national judicial or administrative authorities, including law enforcement authorities, may order providers of intermediary services to act against one or more specific items of illegal content or to provide certain specific information. The national laws on the basis of which such orders are issued differ considerably and the orders are increasingly addressed in cross-border situations. In order to ensure that those orders can be complied with in an effective and efficient manner, in particular in a cross-border context, so that the public authorities concerned can carry out their tasks and the providers are not subject to any disproportionate burdens, without unduly affecting the rights and legitimate interests of any third parties, it is necessary to set certain conditions that those orders should meet and certain complementary requirements relating to the processing of those orders. Consequently, this Regulation should harmonize only certain specific minimum conditions that such orders should fulfil in order to give rise to the obligation of providers of intermediary services to inform the relevant authorities about the effect given to those orders. Therefore, this Regulation does not provide the legal basis for the issuing of such orders, nor does it regulate their territorial scope or cross-border enforcement."

[12] Article 8(3) of Directive 2001/29/EC states that “Member States shall ensure that rights holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right”.

[13] The text of the WIPO Copyright Treaty (WCT) is available at https://www.wipo.int/wipolex/en/text/295166.

A. Domain suspension and its effectiveness

13. Domain name registrars (DNR) register domain names for a fee on behalf of registrants, i.e. website owners, so that the alphanumeric IP address used for a domain can be easily found by humans through search engines.

14. Recently, pursuant to court injunctions, DNRs suspended illegal domains with global effect, making numerous targets unreachable from all over the world. Since 2023,[14] the High Court of Delhi in India has been issuing orders compelling DNRs, wherever located, to lock and suspend infringing domain names. In 2025, the injunctions were extended to infringing apps and other services, protecting real-time broadcasts.[15] In the order granted in favor of Star India, dated May 29, 2025, the Delhi High Court stated the following:

> "In the new age of technology, today it has become increasingly easy and convenient for infringers to create alpha-numeric/mirror/redirect variants of infringing websites, and by the time impleadment and extension of relief(s) can take place, certain time-sensitive infringing activities like live streaming of sporting events have already commenced illegally and by the time the effected party like the plaintiff approaches this Court, it is too late", ordering registrars to "suspend the domain name registration of infringing domains/URLs/UIs notified by the plaintiff on real time basis."

15. As a result, several registrars around the world have complied with these Court orders by globally suspending domains and providing information on piracy operators.[16] However, some registrars remain non-compliant with the Court orders, underscoring the need for stronger collaboration and greater awareness of their critical role.

16. An internal analysis of 275 popular piracy websites blocked in India revealed that[17] during the three months before and after the orders, visits to the 138 domains blocked and suspended declined by an additional 11 per cent compared to visits to the remaining 137 only blocked locally by ISPs. The global impact was even stronger: domains that were blocked also in other countries and suspended by registrars decreased on average by 44 per cent more than those that were only blocked. Overall, worldwide visits to blocked and suspended sites declined by 99 per cent from July 2024 to July 2025, since domain suspension typically makes the domain unavailable to any site blocking workarounds, such as use of VPNs and alternative DNS services.[18]

B. Content delivery network blocking

17. Along the distribution chain of pirated content, various illegal services also take advantage of reverse proxy server and CDN services.[19] Some progress has been made, including dedicated application programming interfaces (APIs) for rights holders to request more information about domains hiding their real IP address behind reverse proxy servers; favorable

[14] See Universal City Studios LLC. & Ors. vs. Dotmovies.baby & Ors., CS(COMM) 514/2023.
[15] See Star India Private Limited vs. IPTV Smarters Case CS(COMM) 108/2025, 29 May 2025. See also Dazn Limited & Anr vs. Buffsports. Me & Ors., CS(COMM) 536/2025, 28 May 2025.
[16] In the judgement of Star India vs. IPTV Smarters the Court ordered the defendants "to disclose complete details such as name and address, along with payment details qua the said rogue websites and rogue mobile applications".
[17] "Popular domain" refers to a website with more than 50,000 visits worldwide in the suspension month.
[18] While suspended and blocked domains may be expected to become completely unavailable (decrease of100 per cent visits), the different measured decline may be due to inaccuracy in communication of the effective domain suspension dates as well as residual visits from old links.
[19] See the 2025 and 2022 EU Counterfeit and Piracy Watch List reports. Available at https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2025)132&lang=en; and https://circabc.europa.eu/ui/group/d0803128-7d62-40ee-8349-c43ee92745aa/library/b36f701d-2850-4768-9b3e-e487140e11e5/details?download=true.

treatment for so-called “trusted flaggers”; and technological measures to block access to illegal content at the CDN level.[20]

18. Rigorous enforcement of CDN access blocks could substantially reduce visits to pirate sites, however, significant challenges remain. Chief among these is the ability of pirate site operators to register a near-infinite number of domains on their CDN accounts and easily manage them so that as soon as the current domain is blocked, it is replaced by a new domain that is immediately operational.

C. Timely delisting from search engines

19. Delisting means removing specific web pages or links from search engine results so that they are no longer visible in the search index for queries. Australia first included “online search engine provider” and delisting injunctions in its Copyright Act as a mandate, which led to voluntary arrangements with leading search engines who now engage in this practice in various countries. Another example is the French Supreme Court decision in the Allostreaming case,[21] in which the Court required search engine providers to delist structurally infringing websites under the French implementation of Article 8(3) of the InfoSoc Directive.

20. When combined with site blocking, delisting has a significant impact in reducing the total number of visits to rogue websites. Internal research shows that timely delisting, carried out shortly after the local blocking by ISPs, leads to an average of 25 per cent greater decline in traffic than in cases where timely delisting has not been carried out..

21. If the names of pirate sites (pirate brands) and the latest active domains continue to remain at the top of search engine results, it will always be relatively easy for Internet users to find them, regardless of any previous blocks. For this reason, timely and diligent collaboration and action taken by search engines remain essential.

D. VPN and alternative DNS blocking to avoid circumvention tactics

22. VPN and alternative DNS services are intermediaries that can permit access to domains blocked by local ISPs. While they can be used legitimately for privacy reasons, they are increasingly employed as circumventing tools. Recently, French and Italian legislation and case law included these types of intermediaries within the scope of their site blocking regimes.

23. In Italy, the current version of the anti-piracy law[22] includes both types of intermediaries among those that can be subject to orders imposed by the national telecommunications authority (AGCOM).[23] In France, between 2024 and 2025, the Paris Civil Court issued several

---

[20] On several occasions, the Spanish LaLiga has confirmed that it has reached agreements with Akamai Technologies and CDN77 to remove content that infringes copyright, even in real time. See https://www.panoramaaudiovisual.com/2025/04/04/laliga-trabaja-cdn77-akamai-lucha-contra-pirateria/. See also the judgement of the Paris Civil Court of March 28, 2025, cited above. Also Cloudflare declared voluntary agreements with rightholders are possible to geoblock websites through its CDN and security services, as it did in the United Kingdom. See Cloudflare blog news here https://blog.cloudflare.com/h1-2025-transparency-report/.

[21] See French Supreme Court, July 6, 2017, ECLI:FR:CCASS:2017:C100909. Google, Microsoft Bing and Yahoo! were required to delist structurally infringing sites pursuant to the French implementation of Art. 8(3) of the Directive2001/29/EC, allowing rights holders to request proportionate measures against any person likely to contribute remedying the infringements. According to the *Allostreaming* case law, ISPs and search providers can be required to fully bear the costs of the measures as long as the order leaves the intermediary free to determine the actual measures needed to obtain the targeted result and does not require an “unbearable sacrifice.”

[22] Law No. 93/2023.

[23] For example, Google appears to have made positive strides in collaborating in real-time blocking at the alternative DNS level, see AGCOM's public statement on collaboration with Google available at https://www.agcom.it/comunicazione/comunicati-stampa/comunicato-stampa-39, while collaboration with VPNs seems to be less obvious, given that VPNs seems very reluctant to comply.

site blocking orders towards renowned VPN and alternative DNS services.[24] The Court determined that these intermediaries can contribute to remedying the infringements with their activities of transmitting data, also according to the DSA provisions that qualify them as intermediary services. Consistent with the case law of the Court of Justice of the European Union,[25] the measures were considered proportionate as they were time-limited and left intermediaries free to select the most suitable technical means, without imposing a general monitoring obligation.

IV. FLEXIBLE COURT ORDERS TO ADDRESS EVOLVING PIRACY STRUCTURES

24. A recent development in the United Kingdom illustrates how courts are adapting injunction frameworks to address the changing nature of online piracy. Building on the long-standing British site blocking case law under section 97A of the Copyright, Designs and Patents Act, including traditional site blocking orders and subsequent pirate brand orders, the High Court of Justice has now granted a broader "omnibus" site blocking order.[26]

25. This order enables rights holders to seek blocking of structurally infringing audiovisual piracy services that meet defined criteria, without having to bring a fresh court application for each new domain or site name available in the future. This is particularly important where piracy operators use generic, descriptive, or frequently changing names to avoid being captured by brand-based or domain-specific orders.

26. The Court accepted that this broader form of relief was necessary and proportionate in light of the scale and evolving nature of the problem of online infringements, the operational burden of repeated applications, and the demonstrated responsible use of site blocking remedies by rights holders over many years. The order has a duration of 6 months and can be extended also depending on an ex-post reporting obligation, requiring rights holders to submit to the Court information on implementation and effectiveness, thereby preserving judicial oversight and accountability. This type of order does not require expanding intermediary liability but rather ensuring that existing no-fault injunction mechanisms remain practically effective in rapidly evolving online environments.

27. This development is particularly relevant in light of recent changes in the technical and operational behavior of piracy operators. While fully autonomous "agentic AI" systems are not yet known to be widely used in the piracy ecosystem, several technological developments are already materially lowering the barriers to large-scale domain hopping and evasive schemes, so that pirate operators can now rapidly deploy cloned streaming sites using openly available codebases and low-cost automated domain registration systems, often combined with bulk registration APIs and redirect-based migration strategies. As a result, infringing services increasingly operate through rotating networks of domains, including generic or non-brand-

[24] Regarding VPNs, see the judgements in the following Paris Civil Court cases: No. 24/14722 of 15 May 2025, and No. 25/05198 of 18 July 2025, both involving Canal + vs. Express Technologies, Expressco Services, Cyberghost, Proton, Nordvpn, and Surfshark. Alternative DNS services were involved in the following judgements of the Paris Civil Court: No. 23/14722 and No. 23/14726 of May 16, 2024, No. 23/14731 of May 30, 2024, No. 24/06759 of September 12, 2024, No. 24/11187 and 24/11188 of October 24, 2024, Canal + vs. Google, Cloudflare and Cisco, No. 24/12413, 24/12414 of December 5, 2024, Canal + vs. Vercara LLC and Quad9, and No. 24/12415 of December 5, 2024, Canal + vs. Google, Cloudflare and Vercara. These cases were filed based on the broad definition contained in Article 333-10 of the French Sports Code, of "any person likely to contribute to remedying" the violation of audiovisual exploitation rights, allowing to include VPN and alternative DNS services into this category. The Court ordered the alternative DNS providers to implement, within the framework of their respective domain name resolution services, "all appropriate blocking measures to prevent access from French territories, by any effective means, and in particular by blocking the domain names or sub-domains, to the identified websites".

[25] See the Court of Justice of the European Union judgement C-314/12, March 24, 2014, UPC Telekabel Wien GmbH vs. Constantin Film Verleih GmbH.

[26] See the High Court of Justice, [2026] EWHC 1087 (Ch), May 7, 2026, Columbia Pictures Industries, Inc. & Ors. vs. British Telecommunications Plc & Ors.

related names specifically designed to evade traditional domain-specific or brand-based blocking measures. In some cases, operators maintain multiple interchangeable domains with substantially identical infrastructure, content libraries and functionality, allowing users to be seamlessly redirected to replacement domains.

V. Automation

28. Another phenomenon that is gaining momentum is the adoption of automated platforms, not only to better coordinate the requests of rights holders, but also to accommodate the most varied intermediary services in their blocking activities. These can operate in accordance with best practices, adhering to due process, principles of transparency and proportionality, and procedural safeguards, putting rights holders in direct communication with intermediaries, with or without the supervision of a third-party authority.

29. This automated approach would make collaboration between parties smoother and more cost effective, allowing for rapid blocking and unblocking, which is also suitable for reconciling the need to protect illegally transmitted content in real-time. The adoption of such systems should therefore be encouraged, replacing email communication with attachments which usually require longer processing times and involve greater complexity.

30. Some national administrative authorities[27] have already equipped themselves with automated or semi-automated platforms that are constantly being improved and allow for rapid blocking and unblocking and smooth communication between rights holders, intermediaries, and supervising authorities. Courts seem to encourage automated updating and notification means between rights holders and intermediaries.[28] However, private entities such as MPA are also equipping themselves with similar instruments, which facilitate detection of infringements, evidence acquisition and communication with intermediaries.

VI. CONCLUSION

31. Empirical data shows that greater collaboration in preventing access to illegal sites and services by various intermediaries leads to more effective blocking and greater protection for intellectual property.

32. Automation and technological tools should be further used to combat piracy, with a view to increasing efficiency and enhancing harmonization with the systems of intermediaries, to enable reduced costs and burdens in the long term. This approach will help to combat piracy and its future developments, protecting both rights holders and ultimately users themselves, who are exposed to the risk of malware and identity theft on pirate websites.

[End of contribution]

[27] Known examples are AGCOM for Italy, the Hellenic Copyright Organization (EDPPI) for Greece, the General Inspection of Cultural Activities (IGAC) for Portugal, and the National Telecommunication Authority (ANATEL) for Brazil.

[28] See judgement of the Federal Civil and Commercial Court of Argentina (11th chamber), April 7, 2025, No. 4426/2025, Warner Bros. Entertainment Inc. & Ors. vs. Pelisplushd.bz & Ors.