F

OMPI
ORGANISATION MONDIALE
DE LA PROPRIÉTÉ
INTELLECTUELLE

WIPO/ACE/18/26
ORIGINAL : ANGLAIS
DATE : 15 MAI 2026

Comité consultatif sur l'application des droits

Dix-huitième session
Genève, 2 – 4 juin 2026

ROLE DES SERVICES INTERMEDIAIRES DANS LE BLOCAGE DE SITES : COMMENT LES LEGISLATEURS, LES TRIBUNAUX ET LES INSTITUTIONS FAÇONNENT LE ROLE DES INTERMEDIAIRES DANS LA LUTTE CONTRE LES ATTEINTES EN LIGNE AU DROIT D'AUTEUR

Contribution établie par M. Okke Delfos Visser, premier vice-président et conseiller juridique adjoint, Questions internationales, Motion Picture Association Bruxelles (Belgique)[*]

RESUME

La présente contribution examine le rôle critique joué par les services intermédiaires, au-delà du simple rôle de fournisseurs d'accès Internet, pour bloquer les sites pirates illégaux dans les systèmes permettant l'émission d'injonctions sans qu'une faute ait été commise. Les meilleures pratiques en vigueur[1], les règlements (en particulier la loi sur les services numériques de l'Union européenne), la jurisprudence et les règles institutionnelles vont toutes dans le sens de la participation d'un large éventail d'intermédiaires pour le blocage de sites. On peut citer, à titre d'exemple, les services d'enregistrement des noms de domaine, les réseaux privés virtuels (VPN), les moteurs de recherche et les réseaux de diffusion de contenu. En effet, des études montrent que le fait d'associer un large éventail d'intermédiaires aux procédures de blocage renforce sensiblement l'efficacité des mesures et réduit les tentatives de contournement. Il convient également de tirer parti des solutions automatisées mises en place entre les titulaires de droits et les intermédiaires concernés, notamment les fournisseurs d'accès Internet, afin de contrer la multitude de techniques de contournement utilisées par les sites contrefaisants.

[*] Les opinions exprimées dans le présent document sont celles de l'auteur et pas nécessairement celles du Secrétariat ou des États membres de l'OMPI.

[1] Voir la contribution de la Motion Picture Association à la dix-septième session du Comité consultatif sur l'application des droits à l'OMPI, 4-6 février 2025, disponible à l'adresse https://www.wipo.int/edocs/mdocs/enforcement/fr/wipo_ace_17/wipo_ace_17_14.pdf.

I. L'EFFICACITE DU BLOCAGE DE SITES

1. La Motion Picture Association MPA est le porte-parole et le défenseur de l'industrie internationale du cinéma, de la télévision et de la diffusion en continu[2]. Nos studios membres sont Netflix Studios, LLC, Paramount Pictures Corporation, Prime Video & Amazon MGM Studios, Sony Pictures Entertainment Inc., Universal City Studios LLC, Walt Disney Studios Motion Pictures et Warner Bros. Discovery. La MPA joue un rôle de premier plan dans la lutte contre la diffusion illégale de contenus protégés par le droit d'auteur, qui nuit au bon fonctionnement de l'écosystème numérique. L'un des principaux objectifs de la MPA est de réduire ou d'atténuer le piratage grâce à des stratégies d'application efficaces, notamment en collaborant avec les intermédiaires susceptibles de fournir aux auteurs d'actes de piratage des services en ligne.

2. L'équipe de la MPA chargée de la protection des contenus travaille en collaboration avec l'Alliance for Creativity and Entertainment (ACE), la principale organisation mondiale de lutte contre le piratage en ligne. L'Alliance for Creativity and Entertainment (ACE) a été créée en 2017 à l'initiative de la MPA et rassemble aujourd'hui plus de 50 entreprises de médias et de divertissement à travers le monde. Elle se concentre sur l'application des droits et la collaboration avec les organismes publics et les autorités judiciaires afin d'identifier les opérateurs et les organisations à l'origine des actes de piratage et de mettre un terme aux services illégaux. Ensemble, la MPA et l'Alliance for Creativity and Entertainment appliquent une approche à 360 degrés pour lutter contre le piratage en ligne, avec un large éventail d'activités telles que la collecte de renseignements et les enquêtes, le suivi des nouvelles législations relatives au blocage de sites à l'échelle mondiale, des actions fondées sur le droit d'accès à l'information pour obtenir des données sur les opérateurs à l'origine d'actes de piratage auprès des fournisseurs de services intermédiaires, et la demande de blocage et de retrait de la liste des sites Web ou des services contrefaisants.

3. Actuellement, plus de 60 pays disposent de systèmes juridiques autorisant des procédures administratives ou judiciaires de blocage de sites. La MPA a une expérience directe dans plus de 30 de ces pays et a accumulé de vastes compétences dans ce domaine. Une analyse interne fondée sur des données, concernant l'efficacité des injonctions de blocage de sites obtenues entre 2024 et 2025, a permis de comparer le nombre de visites de sites Web avant et après les blocages. Les résultats montrent que le blocage mis en place par les fournisseurs traditionnels d'accès à l'Internet entraîne en moyenne une réduction de 89% du nombre de visites sur les sites pirates ciblés. Dans des pays comme l'Italie, la France, le Brésil, la Corée du Sud et l'Inde, la réduction moyenne du nombre de visites après le blocage d'un site a dépassé les 90% en 2024[3].

4. L'efficacité du blocage de sites a également été mesurée du point de vue de l'augmentation de la consommation légale au Brésil, en Inde, au Royaume-Uni et en Australie.

---

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

[3] Les données accessibles au public montrent également que l'efficacité du blocage de sites varie entre 60% et 97% selon le pays. Pour le Royaume-Uni, voir Brett Danaher et al., *The Effect of Piracy Website Blocking on Consumer Behavior*, MIS Quarterly 631, juin 2020, pages 637 et 639 ("Nous constatons que les blocages de novembre 2014 [de 53 sites] ont permis de réduire les visites sur les sites bloqués. Le nombre de visites sur les sites bloqués a chuté de 88% entre les trois mois précédant les blocages et les trois mois suivants". En se référant aux données relatives aux vagues de blocage de 2012 et 2013, "Le nombre de visites sur les sites bloqués diminue de 80 à 95% dans les différents groupes, ce qui indique que le blocage est efficace.") En ce qui concerne l'Australie et la Corée du Sud, voir MPA, *Measuring the Effect of Piracy Website Blocking in Australia on Consumer Behavior*, janvier 2020, disponible à l'adresse https://www.mpa-apac.org/wp-content/uploads/2020/02/Australia-Site-Blocking-Summary-January-2020.pdf (s'agissant d'un blocage en décembre 2018, "le nombre moyen de visites sur les sites bloqués a fortement diminué pour le groupe expérimental, le nombre de visites sur ce groupe de sites ayant baissé de 61% au total entre la période précédant les blocages et les trois mois suivants"), et MPA, *MPA Study on Site Blocking Impact in South Korea*, 2016, p. 11, disponible à l'adresse https://www.mpa-apac.org/wp-content/uploads/2018/05/MPAA_Impact_of_Site_Blocking_in_South_Korea_2016.pdf ("l'impact de niveau 1 était évident : les visites sur les sites bloqués avaient diminué en moyenne de 90% trois mois après le blocage (97% après la première vague, 93% après la deuxième vague et 79% après la troisième vague)".).

Plusieurs études ont montré que le blocage de sites a entraîné une hausse de la consommation de contenus légaux de 5,2% au Brésil en 2021 et de 8,1% et 3,1% en Inde en 2019 et 2020 respectivement[4]. Au Royaume-Uni, une étude réalisée en 2016 a révélé que le blocage de sites avait entraîné une augmentation de 6% du nombre de visites sur des sites payants légaux de diffusion en continu et de 10% du nombre de vidéos visionnées sur des sites légaux de diffusion en continu financés par la publicité, tandis qu'une étude ultérieure menée en 2020 a estimé que l'utilisation des sites légaux par abonnement avait augmenté de 7 à 12 points de pourcentage en raison du blocage de sites[5]. Enfin, l'Australie a enregistré une augmentation de 5% du trafic vers les plateformes légales de visionnage de contenus[6].

5. Les titulaires de droits investissent des sommes colossales dans les contenus, et le piratage porte gravement atteinte à leurs revenus ainsi qu'à leurs perspectives de production futures. Pour renforcer encore l'efficacité du blocage de l'accès aux contenus piratés, l'intervention et la collaboration des prestataires de services intermédiaires en ligne à tous les niveaux de la chaîne de distribution illégale sont indispensables. Cette nécessité est reconnue par un nombre croissant de législateurs, de tribunaux et d'organismes administratifs.

II. LE REGLEMENT SUR LES SERVICES NUMERIQUES (DSA) EMBOITE LE PAS A LA DIRECTIVE DE L'UNION EUROPEENNE SUR LE COMMERCE ELECTRONIQUE

6. Le règlement sur les services numériques (DSA) (règlement UE n° 2022/2065)[7] est l'un des textes législatifs les plus complets sur la responsabilité des intermédiaires en ligne, directement applicable dans les 27 États membres de l'UE. S'inspirant de la directive de l'Union européenne sur le commerce électronique et reprenant la plupart de ses articles, le règlement sur les services numériques a repris les mêmes principes de "sphère de sécurité" pour les fournisseurs de services de simple transport, de services de mise en cache et de services d'hébergement, mais a également précisé quels intermédiaires devaient être classés dans ces différentes catégories.

7. À cet égard, le considérant 29[8] du règlement sur les services numériques est extrêmement utile pour préciser quels types d'intermédiaires correspondent à la définition de

---

[4] Voir Danaher et al., *The Impact of Online Piracy Website Blocking on Legal Media Consumption*, 12 février 2024, disponible à l'adresse https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4723522.

[5] Voir Danaher et al., *Website Blocking Revisited : The Effect of the UK November 2014 Blocks on Consumer Behavio*r, 18 avril 2016, disponible à l'adresse https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2766795, et Danaher et al., *The Effect of Piracy Website Blocking on Consumer Behavior*, MIS Quarterly, juin 2020.

[6] Voir *Measuring the Effect of Piracy Website Blocking in Australia on Consumer Behavior* cité dans la note de bas de page 3.

[7] Le texte du règlement sur les services numériques est disponible à l'adresse https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022R2065.

[8] Le considérant 29 du règlement sur les services numériques prévoit que "Les services intermédiaires couvrent un large éventail d'activités économiques qui ont lieu en ligne et évoluent en permanence pour permettre une transmission d'informations rapide, sûre et sécurisée, ainsi que pour garantir le confort de tous les participants à l'écosystème en ligne. À titre d'exemple, les services intermédiaires de 'simple transport' comprennent des catégories génériques de services telles que les points d'échange Internet, les points d'accès sans fil, les réseaux privés virtuels, les services de DNS et de résolution de noms de domaine, les registres de noms de domaine de premier niveau, les bureaux d'enregistrement de noms de domaine, les autorités de certification qui délivrent des certificats numériques, la voix sur IP et d'autres services de communication interpersonnelle, tandis que les exemples génériques de services intermédiaires de 'mise en cache' comprennent la seule fourniture de réseaux d'acheminement de contenus, de serveurs mandataires inverses ou de serveurs mandataires d'adaptation de contenus. De tels services sont essentiels pour garantir la transmission fluide et efficace des informations fournies sur l'Internet. Parmi les exemples de 'services d'hébergement' figurent des catégories de services telles que l'informatique en nuage, l'hébergement de sites Internet, les services de référencement payant ou les services permettant le partage d'informations et de contenus en ligne, y compris le stockage et le partage de fichiers. Les services intermédiaires peuvent être fournis isolément, dans le cadre d'un autre type de service intermédiaire, ou simultanément avec d'autres services intermédiaires. La question de savoir si un service spécifique constitue un service de 'simple transport', de 'mise en cache' ou d''hébergement' dépend uniquement de ses fonctionnalités techniques, lesquelles sont susceptibles d'évoluer dans le temps, et devrait être appréciée au cas par cas".

fournisseurs de “services de simple transport”, y compris les réseaux privés virtuels (VPN), les services de DNS (systèmes de noms de domaine), les services de résolution et les bureaux d’enregistrement, tandis que les exemples cités de fournisseurs de “services de mise en cache” comprennent les réseaux d’acheminement de contenus et les serveurs mandataires inverses[9].

8. En outre, le considérant 25[10] souligne qu’il est important de veiller à ce que les injonctions sans faute s’appliquent aux intermédiaires qui, bien qu’ils ne soient pas responsables, disposent néanmoins des moyens techniques d’intervenir pour mettre fin ou prévenir les infractions, notamment en rendant impossible l’accès à certains contenus.

9. Enfin, le considérant 31[11] prévoit que les États membres peuvent choisir une procédure judiciaire ou administrative pour obtenir de telles ordonnances, une possibilité expressément envisagée par les articles 4 à 6. La base juridique de ces types d’injonctions réside dans l’ancien article 8, paragraphe 3, de la directive 2001/29/CE du Parlement européen et du Conseil, qui faisait expressément référence à ce type de mesures à l’encontre des intermédiaires pour la protection des droits d’auteur.

10. Il convient de noter que ce cadre juridique ne constitue pas une innovation sans précédent de l’UE et qu’il n’est pas non plus appliqué uniquement sur le territoire de l’UE, comme le montre ci-dessous la jurisprudence indienne. En fait, il découle de l’article 14.2 du Traité de l’Organisation Mondiale de la Propriété Intellectuelle (OMPI) sur le droit d’auteur de 1996[12], qui porte sur la protection du droit d’auteur et des droits connexes dans l’environnement numérique, et qui stipule que “[l]es parties contractantes feront en sorte que leur législation comporte des procédures destinées à faire respecter les droits prévus par le présent traité, de manière à permettre une action efficace contre tout acte qui porterait atteinte à ces droits, y compris des mesures propres à prévenir rapidement toute atteinte et des mesures propres à éviter toute atteinte ultérieure”.

---

9 Les tribunaux européens s’appuient déjà sur le règlement sur les services numériques pour étendre le champ d’application des injonctions sans faute à d’autres types d’intermédiaires afin de protéger les œuvres protégées par le droit d’auteur. C’est le cas notamment du Tribunal judiciaire de Paris qui, dans son jugement du 28 mars 2025 rendu dans l’affaire *Canal Plus* c. *Cloudflare Inc.*, a déclaré que “Les fournisseurs de systèmes de résolution de noms de domaine et de réseaux d’acheminement de contenus, qui sont expressément visés par le règlement sur les services numériques susmentionné, exercent une fonction de transmission, nonobstant toute exemption de responsabilité dont ils pourraient autrement bénéficier”.

10 Le considérant 25 du règlement sur les services numériques stipule que “Les exemptions de responsabilité établies dans le présent règlement ne devraient pas affecter la possibilité de procéder à des injonctions de différents types à l’encontre des fournisseurs de services intermédiaires, alors même qu’ils remplissent les conditions fixées dans le cadre de ces exemptions. Ces injonctions peuvent notamment revêtir la forme d’injonctions de juridictions ou d’autorités administratives, émises conformément au droit de l’Union, exigeant qu’il soit mis fin à toute infraction ou que l’on prévienne toute infraction, y compris en retirant les contenus illicites spécifiés dans ces injonctions, ou en rendant impossible l’accès à ces contenus”.

11 Le considérant 31 du règlement sur les services numériques stipule que “En fonction du système juridique de chaque État membre et du domaine juridique en cause, les autorités judiciaires ou administratives nationales, y compris les autorités répressives, peuvent enjoindre aux fournisseurs de services intermédiaires de prendre des mesures à l’encontre d’un ou de plusieurs éléments de contenus illicites spécifiques ou de fournir certaines informations spécifiques. Les législations nationales sur la base desquelles ces injonctions sont émises diffèrent considérablement et, de plus en plus souvent, les injonctions sont émises dans des contextes transfrontières. Afin de garantir le respect efficace et efficient de ces injonctions, en particulier dans un contexte transfrontière, de sorte que les autorités publiques concernées puissent accomplir leurs missions et que les fournisseurs ne soient pas soumis à des charges disproportionnées, sans porter indûment atteinte aux droits et intérêts légitimes de tiers, il est nécessaire de fixer certaines conditions auxquelles ces injonctions devraient répondre et certaines exigences complémentaires relatives au traitement de ces injonctions. En conséquence, le présent règlement devrait n’harmoniser que certaines conditions minimales spécifiques devant être respectées par ces injonctions pour donner naissance à l’obligation, pour les fournisseurs de services intermédiaires, d’informer les autorités concernées de la suite donnée à ces injonctions. Par conséquent, le présent règlement n’offre pas une base juridique pour l’émission de ces injonctions ni ne réglemente leur champ d’application territorial ou leur exécution transfrontière”.

12 Le texte du Traité de l’OMPI sur le droit d’auteur est disponible à l’adresse https://www.wipo.int/wipolex/fr/text/295166.

III. ROLE D'AUTRES TYPES D'INTERMEDIAIRES DANS LA PRATIQUE

11. À l'ère technologique actuelle, les contenus piratés sont principalement consommés en ligne. Depuis le début des années 2000, l'évolution favorable de la jurisprudence a permis aux titulaires de droits d'obtenir des injonctions sans qu'aucune faute ne soit commise, injonctions d'abord statiques puis dynamiques, ordonnant aux fournisseurs d'accès Internet de bloquer l'accès aux sites et services pirates. Lorsque les informations nécessaires étaient disponibles, les mesures d'application des droits visaient directement les opérateurs de sites de piratage et les hébergeurs. Toutefois, l'expérience pratique a montré que les opérateurs se cachent souvent derrière des identités fictives ou volées et ne respectent pas les lettres de mise en demeure. Par ailleurs, les serveurs d'hébergement sont souvent introuvables, protégés par des techniques d'anonymisation ou du fait qu'ils sont situés dans des pays où il est extrêmement difficile de faire respecter la loi.

12. La collaboration avec tous les acteurs de la chaîne du piratage est essentielle, car chacun peut intervenir efficacement dans son domaine de compétence et en prenant les mesures les plus appropriées. Cette approche renforce l'efficacité et la portée des ordonnances de blocage, tout en réduisant les possibilités de contournement. Les principaux intermédiaires sont les moteurs de recherche, les bureaux d'enregistrement de domaines, les réseaux d'acheminement de contenus, les réseaux privés virtuels et les services DNS alternatifs.

A. La suspension de domaine et son efficacité

13. Les bureaux d'enregistrement de noms de domaine enregistrent les noms de domaine moyennant une taxe pour le compte des titulaires, c'est-à-dire les propriétaires de sites Web, afin que l'adresse IP alphanumérique associée à un domaine puisse être facilement trouvée par les utilisateurs via les moteurs de recherche.

14. Récemment, suite à des injonctions judiciaires, les bureaux d'enregistrement de noms de domaine ont suspendu des domaines illégaux avec un effet mondial, rendant ainsi de nombreux sites inaccessibles partout dans le monde. Depuis 2023[13], la Haute Cour de Delhi, en Inde, a émis des ordonnances obligeant les bureaux d'enregistrement de noms de domaine, où qu'ils se trouvent, à bloquer et à suspendre des noms de domaine contrefaisants. En 2025, les injonctions ont été étendues aux applications et autres services en infraction, protégeant ainsi les diffusions en temps réel[14]. Dans l'ordonnance rendue en faveur de Star India, datée du 29 mai 2025, la Haute Cour de Delhi a déclaré ce qui suit :

> "À l'ère des nouvelles technologies, il est aujourd'hui de plus en plus facile et pratique pour les auteurs d'atteintes de créer des variantes alphanumériques, des sites miroirs ou de rediriger l'utilisateur vers des sites Web contrefaisants. Ainsi, avant même que la mise en cause de tiers et l'extension des mesures de protection puissent avoir lieu, certaines activités contrefaisantes sensibles au facteur temps, telles que la diffusion en direct d'événements sportifs, ont déjà commencé illégalement; et lorsque la partie lésée, comme le demandeur, saisit la Cour, il est déjà trop tard". La Haute Cour a donc ordonné aux bureaux d'enregistrement de "suspendre en temps réel l'enregistrement des noms de domaine, URL et interfaces utilisateur contrefaisants signalés par le demandeur".

15. En conséquence, plusieurs bureaux d'enregistrement à travers le monde se sont conformés à ces décisions de justice en suspendant les domaines à l'échelle mondiale et en

---

13 Voir *Universal City Studios LLC. & Ors.* c. *Dotmovies.baby & Ors.*, CS(COMM) 514/2023.

14 Voir *Star India Private Limited* c. *IPTV Smarters* Case CS(COMM) 108/2025, 29 mai 2025. Voir également *Dazn Limited & Anr* c. *Buffsports. Me & Ors.*, CS(COMM) 536/2025, 28 mai 2025.

fournissant des informations sur les opérateurs de piratage[15]. Néanmoins, certains bureaux d'enregistrement ne respectent toujours pas les ordonnances de la Cour, ce qui souligne la nécessité d'une collaboration plus étroite et d'une meilleure sensibilisation à leur rôle essentiel.

16. Une analyse interne de 275 sites Web de piratage populaires bloqués en Inde a révélé que[16], au cours des trois mois précédant et suivant les ordonnances, le nombre de visites des 138 domaines bloqués et suspendus avait diminué de 11% supplémentaires par rapport au nombre de visites des 137 autres sites bloqués localement par les fournisseurs d'accès à Internet. L'impact mondial a été encore plus fort : les domaines bloqués dans d'autres pays et suspendus par les bureaux d'enregistrement ont diminué en moyenne de 44% de plus que ceux qui n'étaient que bloqués. Dans l'ensemble, les visites mondiales de sites bloqués et suspendus ont diminué de 99% entre juillet 2024 et juillet 2025, car la suspension d'un domaine le rend généralement indisponible pour toute solution de contournement du blocage de sites, telle que l'utilisation de VPN et de services DNS alternatifs[17].

B. Blocage du réseau d'acheminement de contenus

17. Tout au long de la chaîne d'acheminement des contenus piratés, divers services illégaux tirent également profit des serveurs mandataires inverses et des services de réseaux d'acheminement de contenus. Certains progrès ont été réalisés, notamment des interfaces de programmation d'applications (API) permettant aux titulaires de droits de demander davantage d'informations sur les domaines cachant leur véritable adresse IP derrière des serveurs mandataires inverses, un traitement favorable pour les "signaleurs de confiance" et des mesures technologiques visant à bloquer l'accès aux contenus illégaux au niveau du réseau d'acheminement de contenus[18].

18. Une application rigoureuse des mesures de blocages d'accès par les réseaux d'acheminement de contenus pourrait réduire sensiblement le nombre de visites sur les sites pirates, mais des défis de taille subsistent. Au premier plan figure la capacité des exploitants de sites pirates à enregistrer un nombre quasi illimité de noms de domaine sur leurs comptes CDN et à les gérer facilement, de sorte que dès qu'un nom de domaine est bloqué, il est remplacé par un nouveau nom de domaine immédiatement opérationnel.

C. Déréférencement rapide de résultats fournis par un moteur de recherche

19. Le déréférencement consiste à supprimer certaines pages Web ou certains liens des résultats des moteurs de recherche, de sorte qu'ils ne soient plus visibles dans l'index de recherche. L'Australie a été la première à inscrire dans sa loi sur le droit d'auteur l'obligation pour les "fournisseurs de moteurs de recherche en ligne" de se conformer à des injonctions de

---

15 Dans le jugement de *Star India* c. *IPTV Smarters*, la Cour a ordonné aux défendeurs "de communiquer toutes les informations nécessaires, telles que leur nom et leur adresse, ainsi que les détails relatifs aux paiements effectués au titre desdits sites Web et applications mobiles frauduleux".

16 Le terme "domaine populaire" désigne un site Web ayant reçu plus de 50 000 visites dans le monde entier au cours du mois de suspension.

17 Si l'on peut s'attendre à ce que les domaines suspendus et bloqués deviennent totalement inaccessibles (baisse de 100% du trafic), la variation constatée dans la baisse observée peut s'expliquer par un manque de précision dans la communication des dates effectives de suspension des domaines, ainsi que par la présence de visites résiduelles provenant d'anciens liens.

18 À plusieurs reprises, LaLiga espagnole a confirmé avoir conclu des accords avec Akamai Technologies et CDN77 pour supprimer les contenus portant atteinte au droit d'auteur, même en temps réel. Voir https://www.panoramaaudiovisual.com/2025/04/04/laliga-trabaja-cdn77-akamai-lucha-contra-pirateria/. Voir également le jugement du Tribunal judiciaire de Paris du 28 mars 2025, mentionné plus haut. Cloudflare a également déclaré qu'il était possible de conclure des accords volontaires avec les titulaires de droits afin de mettre en place un géoblocage des sites Web via son réseau d'acheminement de contenus et ses services de sécurité, comme cela a été le cas au Royaume-Uni. Voir les actualités du blog de Cloudflare à l'adresse https://blog.cloudflare.com/h1-2025-transparency-report/.

déréférencement, ce qui a donné lieu à des accords volontaires avec les principaux moteurs de recherche, qui appliquent désormais cette pratique dans divers pays. Un autre exemple est l'arrêt rendu par la Cour de cassation française dans l'affaire Allostreaming[19], dans lequel la Cour a imposé aux fournisseurs de moteurs de recherche de déréférencer les sites Web structurellement illicites, en application de la transposition par la France de l'article 8.3) de la directive sur la société de l'information.

20. Combinée au blocage de sites, le déréférencement a un impact significatif sur la réduction du nombre total de visites sur les sites Web frauduleux. Des études internes montrent qu'un déréférencement rapide, effectué peu après le blocage local par les fournisseurs d'accès Internet, entraîne une baisse du trafic supérieure de 25% en moyenne à celle observée dans les cas où ce déréférencement n'a pas été effectué en temps opportun.

21. Si les noms des sites pirates (marques pirates) et les derniers domaines actifs continuent de figurer en tête des résultats des moteurs de recherche, les internautes pourront toujours les trouver assez facilement, malgré les blocages antérieurs. C'est pourquoi il est essentiel que les moteurs de recherche collaborent et agissent en temps utile et avec diligence.

D. Blocage de réseaux privés virtuels (VPN) et de services DNS alternatifs pour empêcher toute tentative de contournement

22. Les réseaux privés virtuels (VPN) et les services DNS alternatifs sont des intermédiaires qui peuvent permettre l'accès à des domaines bloqués par les fournisseurs d'accès Internet locaux. S'ils peuvent être utilisés légitimement pour des raisons de protection de la vie privée, ils sont de plus en plus utilisés comme outils de contournement. Récemment, la législation et la jurisprudence françaises et italiennes ont inclus ces types d'intermédiaires dans le champ d'application de leurs dispositifs de blocage de sites.

23. En Italie, la version actuelle de la loi antipiratage[20] inclut les deux types d'intermédiaires parmi ceux pouvant faire l'objet de mesures imposées par l'autorité nationale des télécommunication (AGCOM)[21]. En France, entre 2024 et 2025, le Tribunal judiciaire de Paris a émis plusieurs ordonnances de blocage de sites à l'encontre de réseaux privés virtuels et de services DNS alternatifs[22]. Le Tribunal a déterminé que ces intermédiaires peuvent contribuer

---

19 Voir Cour de cassation française, 6 juillet 2017, ECLI:FR:CCASS:2017:C100909. Google, Microsoft Bing et Yahoo! ont été contraints de déréférencer les sites structurellement illicites, conformément à la mise en œuvre par la France de l'article 8.3) de la directive 2001/29/CE, qui permet aux titulaires de droits de demander des mesures proportionnées à l'encontre des intermédiaires dont les services sont utilisés pour porter atteinte à leurs droits. Selon la jurisprudence *Allostreaming*, les fournisseurs d'accès à Internet et les fournisseurs de moteurs de recherche peuvent être tenus de supporter l'intégralité des coûts des mesures, à condition que l'ordonnance laisse l'intermédiaire libre de déterminer les mesures réelles nécessaires pour obtenir le résultat visé et n'exige pas un "sacrifice insupportable".

20 Loi n° 93/2023.

21 Par exemple, Google semble avoir fait des avancées positives en collaborant au blocage en temps réel de services DNS alternatifs. Voir la déclaration publique de l'AGCOM sur la collaboration avec Google disponible sur https://www.agcom.it/comunicazione/comunicati-stampa/comunicato-stampa-39, alors que la collaboration avec les réseaux privés virtuels semble moins évidente, ceux-ci semblant très réticents à se conformer aux exigences.

22 En ce qui concerne les VPN, voir les jugements rendus dans les affaires suivantes par le Tribunal judiciaire de Paris : jugements nos 24/14722 du 15 mai 2025 et 25/05198 du 18 juillet 2025, concernant tous deux *Canal +* c*. Express Technologies, Expressco Services, Cyberghost, Proton, Nordvpn et Surfshark*. Des services DNS alternatifs ont été mis en cause dans les jugements suivants rendus par le Tribunal judiciaire de Paris : jugements nos 23/14722 et 23/14726 du 16 mai 2024, jugements nos 23/14731 du 30 mai 2024, 24/06759 du 12 septembre 2024, 24/11187 et 24/11188 du 24 octobre 2024, *Canal +* c*. Google, Cloudflare et Cisco*, jugements nos 24/12413, 24/12414 du 5 décembre 2024, *Canal +* c*. Vercara LLC et Quad9*, et 24/12415 du 5 décembre 2024, *Canal +* c. *Vercara LLC et Quad9. Google, Cloudflare et Cisco*, 24/12413, 24/12414 du 5 décembre 2024, *Canal +* c*. Vercara LLC et Quad9*, et 24/12415 du 5 décembre 2024, *Canal +* c. *Google, Cloudflare et Vercara*. Ces actions ont été intentées en vertu de la définition générale figurant à l'article 333-10 du Code du sport français, qui vise "toute personne susceptible de contribuer à remédier" à des atteintes aux droits d'exploitation audiovisuelle, autorisant ainsi l'inclusion des services VPN et des services DNS alternatifs. La Cour a ordonné aux fournisseurs de services DNS

[Suite de la note page suivante]

à remédier aux atteintes grâce à leurs activités de transmission de données, conformément aux dispositions du règlement sur les services numériques qui les qualifient de services intermédiaires. Conformément à la jurisprudence de la Cour de justice de l'Union européenne[23], les mesures ont été jugées proportionnées car elles étaient limitées dans le temps et laissaient aux intermédiaires la liberté de choisir les moyens techniques les plus appropriés, sans imposer d'obligation générale de surveillance.

IV. DES ORDONNANCES JUDICIAIRES FLEXIBLES POUR FAIRE FACE A L'EVOLUTION DES STRUCTURES DE PIRATAGE

24. Une évolution récente au Royaume-Uni illustre la manière dont les tribunaux adaptent les dispositifs d'injonction pour faire face à la nature changeante du piratage en ligne. S'appuyant sur la jurisprudence britannique de longue date en matière de blocage de sites en vertu de l'article 97A de la loi sur le droit d'auteur, les dessins et modèles et les brevets, y compris les ordonnances traditionnelles de blocage de sites et les ordonnances ultérieures relatives aux marques pirates, la Haute Cour de justice vient d'accorder une ordonnance "globale" de blocage de sites d'une portée plus large[24].

25. Cette ordonnance permet aux titulaires de droits de demander le blocage des services de piratage audiovisuel structurellement illicites qui répondent à des critères précis, sans avoir à introduire une nouvelle requête auprès du tribunal pour chaque nouveau nom de domaine ou site qui pourrait apparaître à l'avenir. Cela revêt une importance particulière lorsque les pirates utilisent des noms génériques, descriptifs ou changeant fréquemment afin d'échapper aux ordonnances ciblant des marques ou des domaines précis.

26. La Cour a reconnu que cette forme plus large de réparation était nécessaire et proportionnée compte tenu de l'ampleur et de la nature évolutive du problème des infractions en ligne, de la charge opérationnelle que représentent les demandes répétées et de l'utilisation responsable des mesures de blocage de sites par les titulaires de droits, démontrée depuis de nombreuses années. L'ordonnance a une durée de six mois et peut être prolongée, notamment en fonction d'une obligation de rapport a posteriori, qui impose aux titulaires de droits de communiquer à la Cour des informations sur la mise en œuvre et l'efficacité de la mesure, garantissant ainsi le contrôle et la responsabilité judiciaires. Ce type d'ordonnance ne nécessite pas d'étendre la responsabilité des intermédiaires, mais vise plutôt à garantir que les mécanismes d'injonction sans qu'une faute soit requise restent efficaces dans la pratique, dans des environnements en ligne en constante évolution.

27. Cette évolution est particulièrement pertinente à la lumière des changements récents dans le comportement technique et opérationnel des opérateurs pirates. Si les systèmes d'"IA agentique" entièrement autonomes ne semblent pas encore être largement utilisés dans l'écosystème du piratage, plusieurs avancées technologiques réduisent déjà considérablement les obstacles au changement de domaine à grande échelle et aux techniques de contournement, de sorte que les opérateurs pirates peuvent désormais déployer rapidement des sites de diffusion en continu clonés en utilisant des bases de code librement accessibles et des systèmes automatisés d'enregistrement de domaines à faible coût, souvent associés à des API d'enregistrement en masse et à des stratégies de migration basées sur la redirection. En conséquence, les services illicites opèrent de plus en plus souvent à travers des réseaux de

---

alternatifs de mettre en œuvre, dans le cadre de leurs services respectifs de résolution de noms de domaine, "toutes les mesures de blocage appropriées pour empêcher l'accès depuis les territoires français, par tout moyen efficace, et notamment en bloquant les noms de domaine ou sous-domaines, aux sites Web identifiés".

[23] Voir l'arrêt de la Cour de justice de l'Union européenne C-314/12, 24 mars 2014, *UPC Telekabel Wien GmbH* c*. Constantin Film Verleih GmbH*.

[24] Voir Haute Cour de justice, [2026] EWHC 1087 (Ch), 7 mai 2026, *Columbia Pictures Industries, Inc. & Ors.* c*. British Telecommunications Plc & Ors*.

domaines changeant régulièrement, comprenant des noms génériques ou sans rapport avec des marques, spécialement conçus pour contourner les mesures de blocage traditionnelles ciblant des domaines ou des marques précis. Dans certains cas, les opérateurs gèrent plusieurs domaines interchangeables avec une infrastructure, des bibliothèques de contenus et des fonctionnalités sensiblement identiques, ce qui permet aux utilisateurs d'être redirigés de manière transparente vers des domaines de remplacement.

V. AUTOMATISATION

28. Un autre phénomène qui prend de l'ampleur est l'adoption de plateformes automatisées, non seulement pour mieux coordonner les demandes des titulaires de droits, mais aussi pour permettre aux services intermédiaires les plus divers de mener à bien leurs activités de blocage. Ces mécanismes peuvent fonctionner conformément aux meilleures pratiques, dans le respect des procédures, des principes de transparence et de proportionnalité, ainsi que des garanties procédurales, en permettant aux titulaires de droits de communiquer directement avec les intermédiaires, avec ou sans la supervision d'une autorité tierce.

29. Cette approche automatisée faciliterait la collaboration entre les parties et la rendrait plus rentable, puisqu'elle permettrait de bloquer et de débloquer rapidement l'accès, tout en répondant à la nécessité de protéger les contenus diffusés illégalement en temps réel. Il convient donc d'encourager l'adoption de tels systèmes, qui remplacent les communications par courrier électronique accompagnées de pièces jointes, lesquelles nécessitent généralement des délais de traitement plus longs et sont plus complexes à gérer.

30. Certaines autorités administratives nationales[25] se sont déjà dotées de plateformes automatisées ou semi-automatisées, qui font l'objet d'améliorations constantes et permettent un blocage et un déblocage rapides, ainsi qu'une communication fluide entre les titulaires de droits, les intermédiaires et les autorités de contrôle. Les tribunaux semblent favoriser les moyens automatisés de mise à jour et de notification entre les titulaires de droits et les intermédiaires[26]. Cependant, des entités privées telles que la MPA se dotent également d'outils similaires, qui facilitent la détection des infractions, la collecte de preuves et la communication avec les intermédiaires.

VI. CONCLUSION

31. Les données empiriques montrent qu'une collaboration accrue entre les différents intermédiaires pour empêcher l'accès aux sites et services illicites permet un blocage plus efficace et une meilleure protection de la propriété intellectuelle.

32. Il convient de recourir davantage à l'automatisation et aux outils technologiques pour lutter contre le piratage, dans le but d'accroître l'efficacité et de renforcer l'harmonisation avec les systèmes des intermédiaires, afin de réduire les coûts et les charges sur le long terme. Elle contribuera à lutter contre le piratage et ses formes futures, protégeant ainsi tant les titulaires de droits que, en fin de compte, les utilisateurs eux-mêmes, qui sont exposés au risque de logiciels malveillants et d'usurpation d'identité sur les sites pirates.

[Fin de la contribution]

---

[25] Des exemples connus sont l'AGCOM pour l'Italie, l'Organisation hellénique du droit d'auteur (EDPPI) pour la Grèce, l'Inspection générale des activités culturelles (IGAC) pour le Portugal et l'Autorité nationale des télécommunications (ANATEL) pour le Brésil.

[26] Voir le jugement de la Cour fédérale civile et commerciale de l'Argentine (11e chambre), 7 avril 2025, n° 4426/2025, *Warner Bros. Entertainment Inc. & Ors.* c. *Pelisplushd.bz & Ors*.