Arcom
Le régulateur de la communication audiovisuelle et numérique

Les enjeux et les différents instruments de lutte contre le piratage dans les secteurs culturels et sportifs

Etude rédigée avec la collaboration de Carole Hentzgen, rapporteure

Décembre 2025

Sommaire

Sommaire 3

Synthèse 5

Introduction 9

I. L'évolution de la lutte contre le piratage : de la sensibilisation des internautes aux blocages dynamiques des sites illicites 13

1.1 Les premiers mécanismes historiques de la lutte contre les usages illicites en ligne ont eu une efficacité avérée mais sur un périmètre limité de pratiques de piratage 13

1.2 Face à un impératif d'adaptation, la France s'inscrit depuis la loi du 25 octobre 2021 dans un modèle de lutte anti-piratage renouvelé qui renforce les procédures judiciaires et administratives pour mieux cibler les services illicites 17

1.3 À la suite de la réforme de 2021, la consommation de sites illicites a diminué même si celle-ci continue à se maintenir à des niveaux significatifs 23

II. Si l'action du régulateur aux côtés de l'autorité judiciaire s'est révélée efficace, elle nécessite encore des adaptations face aux évolutions rapides des pratiques illicites en ligne 28

2.1 Le modèle français dual de lutte contre le piratage en ligne n'est pas une spécificité en Europe, même si les approches diffèrent d'un pays à l'autre en ce qui concerne le rôle attribué à l'autorité administrative nationale 28

2.2 Dans un environnement numérique en constante évolution, les titulaires de droit sont appelés à s'adapter aux stratégies adoptées par les services illicites pour les contrer 33

2.3 Au-delà des limites structurelles des dispositifs actuels, le cadre législatif et règlementaire pourrait, à droit constant, peser sur l'efficacité des actions anti-piratage 37

2.4 Sur le plan financier, par ailleurs, le coût de la lutte contre le piratage appelle à un nécessaire rééquilibrage afin de garantir la soutenabilité des dispositifs 40

III. L'action du régulateur aux côtés des ayants droit : vers un modèle renouvelé de régulation pour accompagner les titulaires de droits et pour encourager l'autorégulation ainsi que l'implication des services intermédiaires, sous réserve du respect des contraintes constitutionnelles 44

3.1 Une révision du paradigme de contrôle permettrait d'envisager un modèle renouvelé de régulation 44

3.2 Un modèle de régulation plus fédérateur permettrait de concilier la protection de la création et des évènements sportifs avec l' innovation. 51

3.3 De façon complémentaire à la régulation nationale, le droit pénal et le droit européen pourraient être davantage mobilisés. 56

Conclusion **63**

Annexes **65**

1. Lettre de mission 65
2. Textes juridiques en vigueur 67
3. Propositions de loi et amendements 78
4. Usages du RSN dans le cadre de la lutte contre le piratage 83
5. Comparaison des principaux indicateurs relatifs aux usages illicites 87
6. Indicateurs détaillés et données complémentaires – lutte contre le piratage 89
7. Compléments techniques 96

Synthèse

L'étude réalisée par l'Arcom à la demande de la présidente de la commission des affaires culturelles et de l'éducation de l'Assemblée nationale dresse le bilan de la lutte contre le piratage en France. Si les dispositifs mis en place depuis 2009, et particulièrement renforcés par la réforme de 2021, ont permis des avancées significatives dans la protection des contenus culturels et sportifs, la persistance de pratiques illicites à des niveaux élevés et leur constante évolution appellent à poursuivre l'adaptation du cadre d'action des pouvoirs publics.

Le système français de lutte contre le piratage repose sur une combinaison d'actions judiciaires et d'interventions administratives qui a démontré son efficacité. La procédure de réponse graduée, malgré son coût, reste un outil pédagogique unique permettant de sensibiliser directement les internautes : avec une baisse de 80 % du recours au pair à pair depuis 2009 et 75 % des abonnés avertis qui ne réitèrent pas leurs pratiques illicites, son impact sur les comportements est indéniable.

Les dispositifs d'injonction dynamique introduits en 2021, tant pour les sites miroirs culturels que pour les retransmissions sportives, ont également porté leurs fruits. L'audience des services illicites se situe aujourd'hui à son niveau le plus bas jamais mesuré, avec une diminution de 35 % entre 2021 et 2025. Les accès à plus de 13 000 noms de domaine ont été bloqués depuis 2022, témoignant de l'intensité de l'action menée.

Mais depuis quinze ans, les transformations rapides du numérique ont alimenté un développement protéiforme des pratiques illicites en ligne. Au titre des atteintes aux droits d'auteur et aux droits voisins dans la diffusion des œuvres culturelles et la retransmission des manifestations sportives, les internautes ont tiré profit des nouveaux usages, en particulier de l'essor du streaming et du téléchargement direct, pour adapter leurs stratégies d'accès illicites aux œuvres. Ainsi, malgré le déploiement notable d'une offre légale abordable et de qualité, et en dépit de la mise en place de divers instruments de lutte contre le piratage reposant sur la complémentarité des actions judiciaires et administratives, la consommation illicite de contenus dématérialisés se maintient encore aujourd'hui à des niveaux préoccupants.

Dans ce contexte, les outils pensés par le législateur, s'ils ont fait leur preuve, se révèlent aujourd'hui insuffisants pour garantir l'effectivité de la lutte contre le piratage face aux évolutions cycliques des modes de consommation illicite qui se sont continuellement adaptés aux réponses de la puissance publique. En particulier, les effets de la procédure de réponse graduée, ciblant le téléchargement en pair à pair, se retrouvent plus limités dans un environnement où cette pratique est en forte diminution. De même, l'apparition presque instantanée de nombreux sites miroirs, lesquels sont permis grâce à l'actualisation des noms de domaine ou des chemins d'accès, facilite grandement le contournement des mesures de blocages.

Au total, la consommation illicite des contenus culturels et sportifs représente une masse financière non négligeable. Elle constitue un manque à gagner conséquent pour les ayants droit, évalué à 1,5 milliard d'euros, soit 12 % du marché audiovisuel légal, sans compter le coût des mesures de blocage supporté par les fournisseurs d'accès à internet et par les titulaires de droits sportifs. À ces pertes s'ajoute un coût pour les finances publiques, comprenant notamment les dépenses engagées par l'Arcom dans le cadre de la mise en œuvre des actions de lutte contre le piratage, de l'ordre de 2,2 millions d'euros, ainsi qu'un montant estimé à plus de

400 millions d'euros correspondant à des cotisations sociales et des recettes fiscales, notamment de TVA, non perçues.

S'il résulte de ces constats qu'un certain nombre d'évolutions est indispensable pour permettre aux pouvoirs publics de mieux répondre aux atteintes aux droits des créateurs de contenus culturels et sportifs en ligne, de telles améliorations ne pourront se faire sans adaptations du cadre juridique en vigueur. Les propositions formulées dans ce rapport s'articulent ainsi autour de trois axes principaux.

Premier axe : réviser le paradigme de contrôle pour renouveler et simplifier la régulation

Les procédures de blocage des services illicites doivent être simplifiées. Plusieurs recommandations en ce sens sont présentées sous forme d'amendements à la proposition de loi visant à conforter la filière cinématographique en France ainsi qu'à la proposition de loi relative à l'organisation, à la gestion et au financement du sport professionnel.

L'urgence est à l'automatisation partielle des dispositifs de blocage, particulièrement pour les retransmissions sportives en direct. Le dispositif prévu par la proposition de loi relative à l'organisation, à la gestion et au financement du sport professionnel répond à cette nécessité en instaurant un système automatisé de blocage en temps réel, placé sous le contrôle de l'Arcom.

Cette évolution, inspirée notamment des modèles britannique et italien, permettra de traiter des volumes considérablement accrus de demandes de blocage dans des délais compatibles avec la durée des retransmissions. Elle implique néanmoins une transformation du rôle de l'Arcom : d'une vérification systématique de chaque service illicite signalé, l'Arcom passerait à un contrôle des systèmes de détection mis en place par les titulaires de droits et à une surveillance de la qualité des saisines.

En complément, l'attribution à l'Arcom d'un pouvoir coercitif en cas de non-application des demandes de blocage par les intermédiaires techniques renforcerait la crédibilité de l'Autorité dans l'espace numérique.

Enfin, l'Arcom doit favoriser, en les simplifiant, les interventions des intermédiaires en tenant à jour une liste des services illicites sportifs visés par une procédure de blocage et en la partageant avec des tiers. Dans la même logique, le dispositif d'inscription d'un service illicite sur la liste des services contrefaisants doit être revu pour en renforcer l'effectivité.

Deuxième axe : favoriser un modèle de régulation plus fédérateur pour concilier la protection de la création et des programmes sportifs avec l'innovation technologique

Si les fournisseurs d'accès à internet sont aujourd'hui pleinement intégrés au dispositif de lutte contre le piratage, notamment grâce à l'accord signé en 2023 entre les FAI et les titulaires de droits sportifs dans le cadre de la protection des retransmissions sportives, d'autres catégories d'intermédiaires doivent être davantage mobilisées.

Les DNS alternatifs et les fournisseurs de VPN, dont l'usage détourné à des fins illicites concerne 66 % des consommateurs illicites, constituent des partenaires prioritaires. Au-delà de ces acteurs, l'ensemble de l'écosystème numérique doit être associé à la lutte contre le piratage : hébergeurs, réseaux de diffusion de contenus (CDN), magasins

d'applications, places de marché, exploitants de moteurs de recherche en tant que régies publicitaires, prestataires de services de paiement en ligne. Cette stratégie, fondée sur la coopération volontaire plutôt que sur la contrainte systématique, présente plusieurs avantages : elle allège la charge des tribunaux, réduit les délais d'intervention, responsabilise les acteurs et favorise l'émergence de solutions techniques innovantes. Elle s'inscrit pleinement dans l'esprit de la recommandation de la Commission européenne du 4 mai 2023 sur la lutte contre le piratage en ligne des manifestations sportives.

L'accès à des services illicites peut être un argument commercial utilisé par des intermédiaires techniques : plusieurs fournisseurs de VPN ont conclu des partenariats commerciaux avec des influenceurs français et construisent leur message promotionnel sur la possibilité offerte de contourner les mesures de blocage nationales. Une modification de l'article 4 de la loi visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux mérite donc être envisagé pour interdire ce type de communication.

Par ailleurs, l'Arcom doit pouvoir développer des outils et procédures technologiques pour mener à bien ses missions. Dans le cadre de sa misson d'évaluation des mesures techniques d'identification (MTI) utilisées par les fournisseurs de services de partage de contenus pour assurer la protection des contenus en ligne, un accès aux outils de reconnaissance de contenus mis en place par les services numériques pour contrôler leur efficacité doit lui être autorisée , tout comme la possibilité d'utiliser des outils de collecte et de traitement automatisés de données. Le développement de ces techniques par l'Autorité pourrait s'avérer particulièrement utile pour assurer la protection du droit d'auteur dans le cadte du développement du recours à l'intelligence artificielle.

Troisième axe : mobiliser davantage le droit pénal et le droit européen

L'action pénale demeure indispensable pour cibler directement les services illicites et permettre leur fermeture durable. La création d'infractions pénales spécifiques aux atteintes aux droits sportifs, prévue par la proposition de loi relative à l'organisation, à la gestion et au financement du sport professionnel, constituerait une avancée importante. Elle permettrait aux titulaires de droits d'exploitation audiovisuelle de bénéficier de moyens d'action au plan pénal au-delà des seuls droits de retransmission audiovisuelle, et faciliterait l'obtention d'éléments de preuve pour identifier les auteurs des atteintes à ces droits. Cette évolution s'inscrirait dans la lignée de la recommandation de la Commission européenne de 2023 invitant les États membres à faciliter les investigations et à adopter des mesures concrètes contre les acteurs impliqués dans la diffusion non autorisée de contenus à grande échelle.

Le nouveau délit d'administration illicite de plateforme, introduit à l'article 323-3-2 du code pénal, complète utilement cet arsenal en ciblant les services qui facilitent sciemment les activités illicites tout en cherchant à se soustraire à leurs obligations légales.

Le droit européen offre également une complémentarité intéressante avec le dispositif national de lutte contre le piratage sans toutefois proposer un cadre commun de régulation. Le Règlement sur les services numériques (RSN) fournit des opportunités complémentaires qui doivent être pleinement exploitées, comme le statut de signaleur de confiance ou les dispositions de l'article 9 du RSN relatives aux injonctions adressées aux intermédiaires numériques.

***

La recherche d'une plus grande efficacité dans la lutte contre le piratage en ligne ne peut se faire à l'aune de réformes seulement paramétriques. Il convient en effet de privilégier une intervention publique à la fois plus réactive et flexible, ce qui implique de revoir intrinséquement les prérogatives du régulateur. Dans cette optique, un nouveau modèle peut être envisagé, au travers notamment de procédures administratives simplifiées, de l'implication forte d'acteurs volontaires (ayants droit, fournisseurs d'accès, hébergeurs, etc.) et du renforcement des pouvoirs de l'Arcom. Un tel cadre constituerait une avancée systémique possible, même si une attention particulière devrait aussi être portée sur les modalités d'exécution de ce dispositif pour que celui-ci s'inscrive en pleine conformité avec les normes constitutionnelles et européennes.

Introduction

Par lettre du 2 juin 2025, la présidente de la commission des affaires culturelles et de l'éducation de l'Assemblée nationale a confié au président de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) la réalisation d'une étude portant sur les enjeux et les différents instruments de lutte contre le piratage dans le secteur culturel et le sport professionnel.

En 2025, un internaute sur quatre déclare consommer illégalement des contenus culturels et sportifs[1] en ligne. La consommation illicite de contenus dématérialisés a nettement diminué depuis 2021, du fait des efforts conjugués des différentes autorités (Arcom, autorité judiciaire) et des titulaires de droits. Ces derniers, en parallèle des actions judiciaires qu'ils mènent depuis de nombreuses années, ont développé une offre légale riche et diversifiée, gratuite ou payante, couvrant tous les secteurs culturels, avec pas moins de 512 offres légales actuellement référencées par l'Arcom[2]. Le récent succès de Ligue 1+, développé par la Ligue de Football Professionnel et permettant d'accéder à la quasi-totalité des matchs de la Ligue 1, en atteste : avec plus d'un million d'abonnés un mois seulement après son lancement, Ligue 1+ montre qu'une offre légale de qualité, économiquement abordable et répondant aux attentes des spectateurs, participe activement à endiguer le piratage.

Il n'en demeure pas moins que les pratiques illicites se maintiennent à des niveaux élevés en dépit de ces différentes actions. Le persistance d'un niveau préoccupant de pratiques illicites s'explique principalement par les transformations rapides du paysage audiovisuel et des usages numériques, lesquelles favorisent la diversification des procédés de piratage et peuvent limiter l'efficacité des mesures de restriction (cf. annexes). Ainsi, plusieurs modes de consommation illicite coexistent aujourd'hui : visionnage en *streaming*[3], téléchargement direct, téléchargement en pair à pair[4] (P2P), *live streaming*[5], recours à l'IPTV illicite (directement sur des sites et applications ou par des boitiers dédiés), visionnage de flux illicites au moyen des réseaux sociaux, et services infonuagiques (*cloud)*[6]. L'apparition continuelle de nouveaux usages, essentiellement liés à la diversification des modes de consommation numérique, permet à l'offre illégale de suivre une évolution « cyclique » en recourant régulièrement à de nouveaux procédés pour mieux contourner les systèmes de blocages existants.

De la même façon, les stratégies de contournement des mesures de blocage des services illicites en ligne se sont multipliées et sont parfois, pour les profils les plus technophiles, de plus en plus élaborées sur le plan technologique. Celles-ci s'appuient, pour la plupart, sur des technologies neutres par essence mais dont l'utilisation est détournée à des fins illicites. Il s'agit essentiellement des VPN (*Virtual Private Network*, ou Réseau Privé Virtuel en français), qui offrent la possibilité à leurs utilisateurs de naviguer sur internet de façon relativement anonyme en prétendant se trouver dans le pays de leur choix et ainsi, par exemple, d'accéder à un site internet bloqué en France, et des services de DNS alternatifs (*Domain Name System*, ou système de noms de domaine), qui sont

[1] Les films et séries sont les contenus les plus directement concernés par la consommation illicite, consommées de manière illicite par respectivement 14 % et 8 % des internautes (source : Arcom, baromètre de la consommation 2025).
[2] https://www.arcom.fr/sites-plateformes/recherche?title_search=&body_value=
[3] Le *streaming* désigne une technique de diffusion et de lecture en ligne et en continu de données multimédias, qui évite le téléchargement préalable des données.
[4] Le pair à pair est un système d'échange de contenus qui repose sur des partages directs de fichiers entre ordinateurs sans passer par un serveur central.
[5] Le *live streaming* désigne un procédé de diffusion permettant aux internautes de consommer directement du contenu diffusé en temps réel (le plus souvent depuis un canal payant).
[6] Plateformes de services informatiques simplifiant, *via* Internet, le stockage et le traitement de données.

chargés d'établir la correspondance entre un nom de domaine et une adresse IP et qui constituent, par ce biais, une technique de contournement permettant d'accéder à des noms de domaine bloqués par les fournisseurs d'accès à internet (FAI) nationaux (cf. annexes). Ces outils, utilisés par les consommateurs en tant que moyens d'accès aux contenus illicites, pourraient être de plus en plus largement utilisés. Le détournement d'usage des services de VPN et de DNS à des fins de consommation illicite constitue en effet une pratique très plébiscitée chez les jeunes internautes : près de la moitié des consommateurs illicites âgés de 15-24 ans y ont recours.

Au-delà des techniques de contournement, certains modes plus récents de consommation, tels que la télévision par internet (IPTV[7]), ont prospéré grâce au développement du très haut débit (cf. annexes). Si ces technologies sont légales, les études menées par l'Arcom montrent qu'elles peuvent être utilisées à des fins de diffusion et de consommation illicites, tout particulièrement pour les contenus sportifs. Le recours aux services d'IPTV illicites est une forme de piratage qui s'est largement développé au cours des trois dernières années (11 % des internautes français indiquent y avoir recours et deux tiers des utilisateurs d'IPTV illicite précisent avoir commencé il y a moins de trois ans). Généralement payantes, ces offres « tout-en-un » proposent pour une somme modique un accès à des milliers de chaines TV et à des dizaines de milliers de contenus à la demande (films, séries, contenus exclusifs proposés par les services de vidéo à la demande sur abonnement tels que Netflix, Prime Video, Disney+ ou des chaines payantes telles que Canal+ ou beIN SPORTS, etc.), rediffusés sans autorisation. L'infrastructure de ces services, qui repose sur un écosystème complexe en faisant intervenir différentes activités et de nombreux acteurs (serveurs de *streaming*, réseaux dédiés de diffusion de contenus, fournisseurs d'abonnement, serveurs d'authentification, développeurs d'applications, producteurs de boitiers et de clés électroniques), impose aux pouvoirs publics de revoir les modalités classiques de blocage des contenus illicites.

Dans ce contexte mouvant où les procédés de piratage parviennent à s'adapter aux réponses institutionnelles et à se renouveler, les secteurs du sport et de la culture subissent des préjudices particulièrement conséquents liés aux pratiques illégales en ligne. En 2023, le manque à gagner total (sport et culture) est évalué à 1,5 milliards d'euros, soit 12 % du marché audiovisuel légal. Le manque à gagner relatif aux contenus audiovisuels (hors sport) est évalué à 1,2 milliards d'euros, représentant 12 % de la valeur de l'offre légale de ce segment de marché en 2023[8]. Pour le secteur du sport, il est estimé à 290 millions d'euros, soit 15 % de ce segment de marché. Les clubs professionnels sont les plus directement impactés (130 millions d'euros) compte tenu de leur dépendance aux droits de diffusion (en moyenne plus d'un tiers de leurs revenus). Le sport amateur est également touché par l'intermédiaire de la taxe Buffet (5 % sur les droits de retransmissions) non perçue, pour laquelle le manque à gagner est évalué à 15 millions d'euros. De surcroît, les contenus contrefaisants dématérialisés génèrent également un manque à gagner significatif pour les ressources de l'État[9]. S'agissant des recettes sociales et fiscales, les pratiques de piratage ont engendré un préjudice estimé à 230 millions d'euros en matière de TVA, sans compter les 190 millions d'euros de cotisations sociales et d'impôts divers - principalement l'impôt sur les sociétés et celui sur le revenu - qui n'ont pu être recouvrés.

[7] *Internet Protocol Television*.
[8] Arcom (2024), « étude d'impact socioéconomique sur l'industrie audiovisuelle et les finances publiques de la consommation illicite en ligne », Essentiel 18, novembre 2024, https://www.arcom.fr/se-documenter/etudes-et-donnees/etudes-bilans-et-rapports-de-larcom/bilan-2024-de-larcom-sur-la-lutte-contre-le-piratage
[9] L'estimation du manque à gagner pour les finances publiques comprend les taxes qui auraient été collectées, ainsi que les cotisations sociales et impôts qui auraient été perçus au titre des emplois supplémentaires créés en cas de report de la consommation vers l'offre légale.

Aux effets financiers sur les industries culturelle et l'écosystème sportif et sur les finances publiques s'ajoute le coût de la lutte contre le piratage, tant pour les titulaires de droits que pour les institutions publiques. En particulier, la pérennité de la procédure de réponse graduée, dont le coût reste élevé pour l'Arcom, même au regard de son efficacité notoire sur les usages illicites en pair à pair (diminution de 80 % entre 2009 et 2025), peut susciter des questions légitimes dans un contexte budgétaire contraint. Si cette procédure, qui repose sur des avertissements envoyés au titulaire de la connexion internet utilisée à des fins illicites, est aujourd'hui le seul vecteur de communication au public et qu'elle atteint son objectif pédagogique avec efficacité, les coûts de fonctionnement induits sont importants, surtout concernant l'indemnisation des FAI pour les demandes d'identification des abonnés[10] et le fonctionnement du système d'information de l'Autorité.

Par ailleurs, à droit constant, le cadre législatif et règlementaire pourrait peser à terme sur l'efficacité des futures actions anti-piratage. À cet égard, l'appréciation qu'aura le Conseil d'Etat quant à la conformité de la procédure de réponse graduée aux exigences résultant de la jurisprudence de la Cour de justice de l'Union européenne (CJUE)[11] pourrait nécessiter des adaptations substantielles. Pour les compétitions sportives, depuis la loi n° 2021-1382 du 25 octobre 2021, les articles L. 333-10 et suivants du code du sport instaurent un mécanisme original de lutte contre les retransmissions illicites de manifestations et de compétitions sportives, celui de « l'injonction dynamique » (cf. annexes). Ce dispositif est efficace mais un dispositif d'automatisation des mesures « en temps réel » pourrait être envisagé pour l'améliorer. Une telle nouvelle mesure, portée par la proposition de loi sénatoriale relative à l'organisation, à la gestion et au financement du sport professionnel[12] qui sera examinée plus en détail dans la suite de ce rapport, ne s'inscrit toutefois pas dans un cadre juridique vierge mais s'insère dans un ensemble normatif visant à assurer un juste équilibre entre un objectif et une liberté constitutionnellement garantis : d'une part, l'objectif de sauvegarde de l'ordre public, d'autre part la liberté de communication en ligne, à laquelle il est portée atteinte lorsqu'est bloqué l'accès à des services de communication en ligne.

Des adaptations sont également en cours dans la protection des contenus culturels, pour faciliter le recours au dispositif de lutte contre les sites miroirs et son optimisation. D'autres évolutions apparaissent souhaitables comme une meilleure coordination de l'action pénale à l'encontre des services illicites ou l'extension à d'autres intermédiaires des mesures d'injonction dynamique (par le recours aux accords volontaires) ou enfin le renforcement de la sensibilisation du grand public.

Devant la diversification des usages illicites et les enjeux socioéconomiques et juridiques qu'ils soulèvent, il convient de privilégier une intervention publique à la fois réactive et flexible afin de garantir la protection effective des droits sur les contenus culturels et sportifs, tout en veillant au respect des droits et libertés fondamentaux. Jusqu'à présent, la complémentarité entre les actions judiciaires et la régulation administrative a permis d'obtenir de bons résultats dans la lutte contre le piratage en ramenant en 2024

[10] En application des dispositions de l'article L. 34-1 du code des postes et des communications électroniques, les modalités de compensation des surcoûts identifiables et spécifiques des prestations assurées par les FAI à la demande de l'Arcom sont déterminées par le décret n°2017-313 du 9 mars 2017 (codifié dans le code de la propriété intellectuelle à l'article R. 331-9). Les tarifs applicables à ces prestations sont fixés par arrêté du 23 mars 2017.

[11] Affaire préjudicielle C-470/21 La Quadrature du Net e.a. (dite « Hadopi »). Arrêt de la CJUE : https://curia.europa.eu/juris/document/document.jsf?text=&docid=285361&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=5729484

[12] Proposition de loi déposée au Sénat par le sénateur Laurent Lafon le 18 mars 2025 et adoptée par le Sénat le 10 juin 2025 - https://www.senat.fr/travaux-parlementaires/textes-legislatifs/la-loi-en-clair/proposition-de-loi-relative-a-lorganisation-a-la-gestion-et-au-financement-du-sport-professionnel.html

l'audience des services illicites de *streaming*, de téléchargement direct et de pair à pair, principalement utilisé dans le piratage audiovisuel, à des niveaux les plus bas jamais mesurés, après des baisses significatives enregistrées en 2022 et 2023. Cependant, le maintien d'un taux déclaratif de consommation illicite à un niveau encore élevé en 2025, du fait du développement de protocoles illicites et de modes de contournement des mesures de lutte contre le piratage, appelle à faire évoluer davantage les mesures prises par les pouvoirs publics pour renforcer leur agilité et leur efficacité face à la résilience de cet écosystème illicite.

Dans cette optique, la première partie du rapport rappelle le fonctionnement des outils classiques dédiés à la protection des contenus culturels et sportifs en ligne. La deuxième partie prend appui sur des exemples européens et décrit les enjeux liés à l'adaptation des actions combinées du régulateur et de l'autorité judiciaire dans un environnement numérique en constante évolution. Enfin, la dernière partie vise à identifier les contours d'un modèle élargi de régulation en vue, de simplifier et de moderniser le modèle actuel mis en œuvre par l'Arcom, d'encourager l'autorégulation et l'implication volontaires des services intermédiaires, et, enfin, de mobiliser davantage le droit européen et le droit pénal.

I. L'évolution de la lutte contre le piratage : de la sensibilisation des internautes aux blocages dynamiques des sites illicites

En quinze ans, les politiques publiques ont progressivement intégré la lutte contre le piratage en ligne comme une priorité face au déploiement du numérique, aboutissant à la mise en place de plusieurs dispositifs dont l'efficacité s'est révélée satisfaisante.

1.1 Les premiers mécanismes historiques de la lutte contre les usages illicites en ligne ont eu une efficacité avérée mais sur un périmètre limité de pratiques de piratage

1. **Historiquement, le système français de lutte contre le piratage en ligne se présente comme un système mixte combinant l'effet des décisions judiciaires civiles (initialement conçues pour lutter contre les services proposant des contenus culturels contrefaisants), lesquelles peuvent ordonner le blocage ou le déréférencement d'un service diffusant illégalement un contenu protégé (outre les actions pénales), et l'action de l'autorité administrative, qui intervient en complément.**

Les titulaires de droits ont la possibilité d'initier des actions pénales afin de faire sanctionner les personnes physiques ou morales responsables de la gestion des sites illicites sur le fondement du délit de contrefaçon, actions qui se heurtent en pratique à des difficultés d'identification des administrateurs des serveurs incriminés, d'une part, et à une coopération internationale parfois insuffisante, d'autre part. Depuis 2009[13], ces acteurs du secteur culturel peuvent également demander devant le juge civil le blocage de l'accès à ces contenus illicites en se fondant sur l'article L. 336-2 du code de la propriété intellectuelle (CPI). Cet article consacre les actions en cessation, à l'origine des injonctions de blocage, lesquelles constituent une des composantes majeures des mesures de protection actuelles. Il s'agit d'une voie de droit permettant d'empêcher rapidement l'accès à un service illicite (y compris si celui-ci est hébergé et administré à l'étranger), tout particulièrement dans le cas où ce service n'a pas pu ou ne pourra pas être fermé par d'autres moyens, notamment au pénal compte tenu des obstacles rappelés ci-dessus. Ces actions en cessation permettent au tribunal judiciaire, lorsqu'une atteinte à un droit d'auteur ou à un droit voisin est causée par un service de communication au public en ligne, d'ordonner, y compris en référé, toute mesure nécessaire pour prévenir ou faire cesser cette violation, à l'encontre de toute personne susceptible d'y contribuer. À cette fin, le juge s'appuie sur plusieurs critères pour déterminer la nature de l'atteinte au droit, tels que le nombre de visites mensuelles, le type d'œuvres disponibles sur le service, la proportion d'œuvres protégées, ainsi que les modalités d'accès au service.

Dans ces conditions, les demandes visant à empêcher l'accès aux services illicites peuvent prendre deux formes distinctes : les dispositions de l'article L. 336-2 du CPI peuvent en effet être mobilisées pour obtenir des injonctions non seulement à l'encontre des FAI et des moteurs de recherche, mais également à l'encontre de toutes les personnes susceptibles de contribuer à remédier à la violation commise, afin que ceux-ci mettent en place des mesures de blocage des services proposant aux internautes des contenus contrefaisants, que ce soit en *streaming* ou en téléchargement.

[13] Cette faculté judiciaire a été introduite par la loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet.

Ces procédures ne visent pas directement à engager la responsabilité de l'administrateur du service illicite concerné ni de la partie chargée de mettre en œuvre ces mesures de blocage ou de déréférencement. C'est pourquoi, elles ont été plébiscitées par les titulaires de droits et se sont révélées efficaces contre des services portant atteinte aux droits d'auteur, notamment lorsqu'ils sont hébergés à l'étranger, permettant ainsi d'obtenir des résultats notables dans la réduction des pratiques illicites à partir du territoire national. Un exemple marquant parmi les nombreuses actions en cessation est celle relative au site « *The Pirate Bay* »[14] : à la demande de la Société civile des producteurs phonographiques (SCPP), le tribunal de grande instance de Paris a enjoint aux FAI - Orange, Bouygues Télécom, Free et SFR - de prendre toutes les mesures nécessaires pour bloquer l'accès non seulement au site principal, mais aussi à ses sites dits miroirs de redirection et aux serveurs « proxy », et ce, pour une durée de douze mois. Ces procédures sont aujourd'hui encore largement utilisées par les titulaires de droits des secteurs du cinéma et de l'audiovisuel mais aussi ceux du jeu vidéo et de l'édition, dont plus particulièrement celui du manga[15].

Afin de renforcer l'effet de ces mesures contre le piratage, les procédures judiciaires ont concomitamment été couplées avec une approche plus pédagogique visant à responsabiliser les internautes. La procédure de réponse graduée, instituée par les lois n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (dite loi Hadopi 1) et n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet (dite loi Hadopi 2), a dès lors constitué un exemple original de collaboration entre l'autorité administrative et l'autorité judiciaire.

Ce mécanisme de prévention doit être initié par les ayants droit, en vertu de l'article L. 331-19 du CPI, après que ces derniers ont constaté des faits de mise à disposition par un internaute d'œuvres protégées sur les réseaux pair à pair[16] (P2P). Sur la base des constats qui lui sont ainsi fournies et les données qu'ils comportent, tout particulièrement l'adresse IP de l'abonné à internet concerné, l'Arcom (et précédemment l'Hadopi) peut solliciter des FAI l'identification de cet abonné. Après deux avertissements suivis de réitérations, une lettre de notification est envoyée, informant le titulaire de l'abonnement que des mises en partage d'œuvres protégées ont à nouveau été opérées depuis sa connexion et qu'il est passible de sanctions pénales[17].

Le membre de l'Arcom chargé de la mission de protection des œuvres peut ensuite décider de transmettre le dossier de l'abonné aux pratiques de piratage persistantes au procureur de la République compétent sur le fondement de la contravention de négligence caractérisée qui sanctionne le titulaire d'abonnement à internet n'ayant pas empêché l'utilisation de sa connexion à des fins de contrefaçon malgré les avertissements envoyés par l'Arcom[18]. Il encourt alors une peine maximale de 1 500 euros (ou 7 500 euros s'agissant d'une personne morale). Le fondement de la transmission des dossiers à l'autorité judiciaire peut aussi être celui du délit de contrefaçon. L'auteur des mises à disposition contrefaisantes (et non plus l'abonné à

[14] Voir D. Rapone, « De la régulation en matière de propriété littéraire et artistique : les pouvoirs de l'autorité de régulation de la communication audiovisuelle et numérique (Arcom) en faveur de la protection de la création », Revue internationale du droit d'auteur, n°276, avril 2023.
[15] Arcom (2025), « le manga et l'anime en France » - https://www.arcom.fr/se-documenter/etudes-et-donnees/etudes-bilans-et-rapports-de-larcom/le-manga-et-lanime-en-france-des-cases-aux-ecrans-panorama-et-perspectives-de-la-creation-graphique-japonaise
[16] Article L. 336-3 du CPI.
[17] Cette lettre invite également la personne concernée à faire valoir ses observations dans un délai de 15 jours et lui rappelle qu'elle peut, dans le même délai, solliciter une audition et qu'elle a le droit de se faire assister d'un conseil.
[18] Article R. 335-5 du CPI.

internet dont la connexion a permis ces mises à disposition) alors identifié lors de l'enquête encourt une peine maximale de trois ans d'emprisonnement et de 300 000 euros d'amende (ou 1 500 000 euros s'agissant d'une personne morale).

L'ensemble de ces mesures judiciaires et administratives ont permis des résultats significatifs. En particulier, la procédure de réponse graduée a fait ses preuves : à chaque étape de la procédure, 75 % des abonnés avertis ne réitèrent plus, si bien que le recours au pair à pair a sensiblement baissé parmi les modes de consommation illicite (8,3 millions d'internautes en 2009, réduits à 1,3 million en 2025, soit une baisse de plus de 80 % en plus de seize ans).

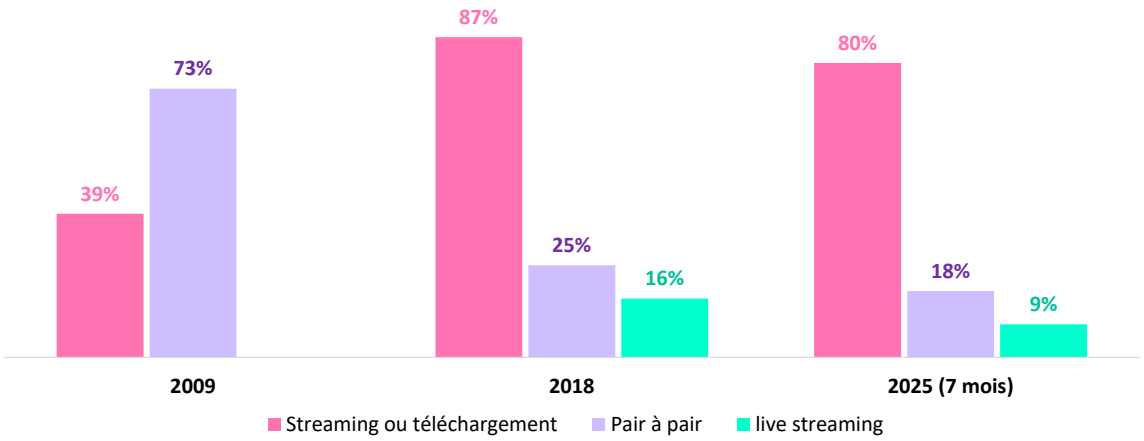
En outre, l'effet dissuasif de cette procédure se constate au regard du nombre de saisines reçues des titulaires de droits qui a fortement diminué ces dernières années (2,3 millions en 2024 contre plus de 14 millions en 2018), même si cette baisse peut également s'expliquer par l'essor du streaming et du téléchargement direct, en lien avec la progression des débits internet – débit relativement faible dans les années 2000 et 2010, quand le pair à pair se développait fortement. En 2025, on note que 17 %[19] des Français ont reçu personnellement ou connaissent quelqu'un ayant reçu un avertissement de la part de l'Arcom (ou anciennement de la part de l'Hadopi).

De même, les résultats du baromètre 2025 sur l'impact de la réponse graduée montrent que la réception des recommandations par les titulaires d'un abonnement à internet produit des effets non négligeables. Ces derniers prennent en effet des mesures concrètes pour mettre un terme aux actes de contrefaçon à la suite de la réception d'un avertissement de l'Arcom : 60 % en ont parlé autour d'eux, 65 % ont diminué leur consommation illicite de biens culturels dématérialisés, 57 % se sont tournés vers une offre légale, 50 % ont désinstallé les logiciels de pair à pair utilisés aux fins de piratage, 39 % ont paramétré et sécurisé leur wifi, 33 % ont mis en place un contrôle parental. Enfin, les suites judiciaires portées à la connaissance de l'Arcom sont également en progression : on dénombre 999 suites reçues en 2024 (contre 838 en 2023). Parmi les suites connues en 2024, près de la moitié a donné lieu à des sanctions pécuniaires, l'autre moitié regroupant les alternatives aux poursuites et les classements sans suite, cette tendance s'amplifiant sur le 1er semestre 2025 (les seules sanctions pécuniaires représentant même un peu plus de la moitié des suites connues).

Cette tendance positive s'est accompagnée au fil des années d'une réorganisation des pratiques illicites : le recours au *streaming* et au téléchargement direct a progressé – 23 % des internautes ayant des pratiques illégales y avaient recours en 2009 contre 80 % en 2025 - tandis que le pair à pair diminuait dans le même temps : s'il était le mode d'accès illicite majoritaire en 2009 (utilisé par 73 % des internautes illicites), il ne concerne plus que 18 % de ces mêmes internautes (Figure 1, données non encore publiées).

[19] Arcom (2025), « Baromètre de la notoriété de l'Arcom et de l'impact de la réponse graduée 2025 » (non encore publiée).

Figure 1 : Répartition des audiences moyennes mensuelles des sites et applications illicites par protocole d'accès (2009 à juillet 2025) - base : internautes ayant des pratiques illégales



Source : Arcom, retraitement données Médiamétrie / NetRatings

2. Malgré un bilan favorable, ces outils « classiques » de lutte contre le piratage se sont très vite heurtés à des obstacles juridiques et techniques, nécessitant des moyens d'action complémentaires.

Les répercussions des actions en cessation devant le tribunal judiciaire se sont retrouvées amoindries par les adaptations opérées par les sites contrefaisants en vue de contourner les mesures de blocage édictées, au premier rang desquelles le développement rapide de nombreux sites miroirs permis par l'actualisation des noms de domaine ou des chemins d'accès,. Jusqu'en 2022, les injonctions de blocage n'étaient pas « dynamiques » et les titulaires de droits n'avaient alors d'autre choix, face à l'apparition de ces nouveaux sites, que d'engager une nouvelle procédure judiciaire afin de faire actualiser les mesures de blocage, au fur et à mesure de l'apparition de ces sites miroirs pour la durée restante de la mesure d'injonction initialement ordonnée par le juge. La procédure judiciaire devenait alors particuièrement lourde .

À noter que les mesures de blocage induites par les injonctions judiciaires peuvent impliquer également des coûts qui sont exclusivement supportés par les intermédiaires (en l'espèce, essentiellement les FAI). La Cour de cassation a en effet affirmé, dans sa décision sur l'affaire « Allostreaming » du 6 juillet 2017, que les dispositions applicables aux mesures de blocage « *ne s'opposent pas à ce que le coût des mesures strictement nécessaires à la préservation des droits en cause, ordonnées sur le fondement de l'article L. 336-2 du code de la propriété intellectuelle, soit supporté par les intermédiaires techniques, quand bien même ces mesures sont susceptibles de représenter pour eux un coût important* »[20].

[20] La Cour de cassation considérant que la cour d'appel a retenu à bon droit que « *ce n'est que dans l'hypothèse où une mesure particulière devait s'avérer disproportionnée, eu égard à sa complexité, à son coût et à sa durée, au point de compromettre, à terme, la viabilité du modèle économique des intermédiaires techniques, qu'il conviendrait d'apprécier la nécessité d'en mettre le coût, en tout ou partie, à la charge des titulaires de droits* ».

1.2 Face à un impératif d'adaptation, la France s'inscrit depuis la loi du 25 octobre 2021 dans un modèle de lutte anti-piratage renouvelé qui renforce les procédures judiciaires et administratives pour mieux cibler les services illicites

1. Si la procédure de réponse graduée est maintenue et sa mise en peuvre transférée de l'Hadopi à l'Arcom, elle voit son déploiement connaître certaines améliorations mais vise des pratiques de piratage en pair à pair devenues minoritaires.

Son périmètre est élargi afin de pallier les limites constatées : désormais, tout ayant droit individuel peut saisir l'Arcom sur la base d'un constat d'huissier et le nom des œuvres mises en partage illégalement peut être mentionné directement dans l'avertissement adressé au titulaire de l'abonnement. Par ailleurs, l'Autorité est désormais autorisée à collecter et à traiter le port source, permettant ainsi de cibler un plus grand nombre d'abonnés à internet (le taux d'identification des adresses IP est passé de 59 % en 2021 à 91 % en 2025[21]).

Si la procédure de réponse graduée est, du fait de sa dimension pédagogique, un outil intéressant dans la lutte contre le piratage[22] - d'autant plus qu'elle reste à ce jour le seul mécanisme permettant de contacter directement l'utilisateur final afin de l'avertir qu'il met à disposition des contenus de manière illégale (et de l'orienter vers les pratiques légales) -, elle ne s'avère néanmoins efficace qu'à l'encontre des usages illicites en pair à pair, ce qui ne constitue plus aujourd'hui la pratique majoritaire pour le piratage des biens culturels dématérialisés. En 2025, ce mode de consommation illicite ne représente en effet plus qu'un cinquième des actes contrefaisants des internautes, loin derrière le *streaming* et le téléchargement direct. Par ailleurs, certains internautes ont mis en place des contremesures qui rendent plus complexe la mise en œuvre de la procédure de la réponse graduée : la Sacem estime ainsi que 15 à 30 % des infractions constatées quotidiennement dans le domaine musical proviennent notamment d'adresses IP correspondant à des équipements informatiques dits « *seedbox* »[23], localisés au sein de centre de données, et non plus simplement rattachées à une box classique. Enfin, les coûts de fonctionnement induits par la mise en œuvre de la réponse graduée sont importants, surtout concernant l'indemnisation des FAI par l'Arcom pour les demandes d'identification des abonnés et le fonctionnement du système d'information de l'Autorité pour la mise en œuvre de la réponse graduée. À cet égard, l'obligation de défraiement, qui avait été prévue par la loi du 12 juin 2009, pourrait être revue du moins partiellement s'agissant des surcoûts liés au déploiement et à l'adaptation des systèmes informatiques des FAI destinés à l'identification et à la transmission des coordonnées des titulaires d'abonnement, déploiement et adaptation que les FAI ont eu largement le temps d'amortir depuis la mise en place de ces systèmes.

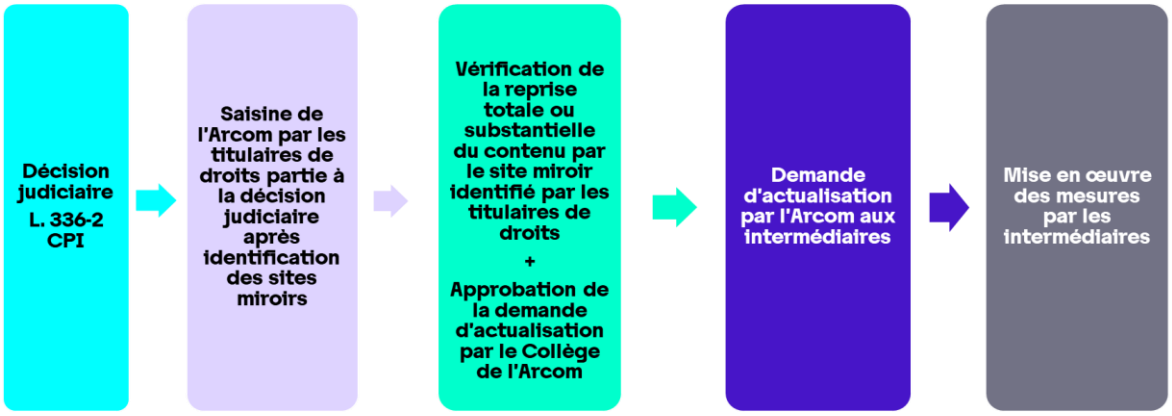
2. Dans ces conditions, tout en maintenant la procédure de réponse graduée et en y apportant quelques améliorations, la nécessité de doter

[21] Le taux d'identification des abonnés par les FAI avait peu à peu chuté en raison du nattage progressif des adresses IP par les FAI dû à une pénurie d'adresses IPV4.
[22] Voir D. Rapone, « De la régulation en matière de propriété littéraire et artistique : les pouvoirs de l'autorité de régulation de la communication audiovisuelle et numérique (Arcom) en faveur de la protection de la création », Revue internationale du droit d'auteur, n°276, avril 2023.
[23] Serveur informatique privé qui est dédié au stockage, au téléchargement et à l'émission de fichiers numériques généralement connecté aux réseaux pair à pair.

l'autorité administrative de nouveaux moyens d'action s'estt imposée. Avec la loi du 25 octobre 2021, l'Arcom intervient désormais dans le prolongement de l'action judiciaire par le traitement de demandes d'actualisation non coercitives. Pour ce faire, deux procédures distinctes ont été mises en place.

La première est une **procédure de lutte contre les sites miroirs dans le secteur culturel** qui confie à l'Arcom, au titre des articles L. 331-27 et R. 331-20 du CPI, la faculté d'actualisation des décisions judiciaires prises sur le fondement de l'article L. 336-2 du CPI, à la suite d'actions en cessation initiées par les titulaires de droits Dans le cadre de la protection du droit d'auteur et des droits voisins, l'autorité administrative peut ainsi demander, sur saisine de ces mêmes titulaires, à toute personne visée par la décision judiciaire le blocage ou le déréférencement d'un service de communication au public en ligne s'il reprend « en totalité ou de manière substantielle » le contenu d'un service visé par ladite décision (Figure 2).

Figure 2 : Schéma récapitulatif de mise en œuvre du dispositif de lutte contre les services miroirs (article L. 331-27 du CPI)



Source : Arcom

L'exécution dynamique des décisions judiciaires par l'Arcom contre les sites miroirs qui contrefont des contenus culturels a permis de bloquer 896 noms de domaine durant les seuls trois premiers trimestres de l'année 2025, soit déjà plus que pour l'ensemble de l'année 2024 (838 noms de domaine bloqués en 2024 contre 549 en 2023, en augmentation de 53 %), auxquels s'ajoutent 688 blocages ordonnés par le tribunal judiciaire de Paris (511 en 2024). De même, dans le cadre de ce dispositif, un traitement plus efficace des saisines a été déployé par l'Autorité concernant certains services spécifiques, le régulateur adaptant régulièrement ses procédés afin de faciliter les constats et les saisines par les ayants droits concernés. Il y a ainsi eu une augmentation du nombre de blocages de services IPTV depuis le début de la mission, ceux-ci représentant 6 % des demandes de blocage en 2023, 28 % en 2024 et 40 % sur les trois premiers trimestres de l'année 2025.

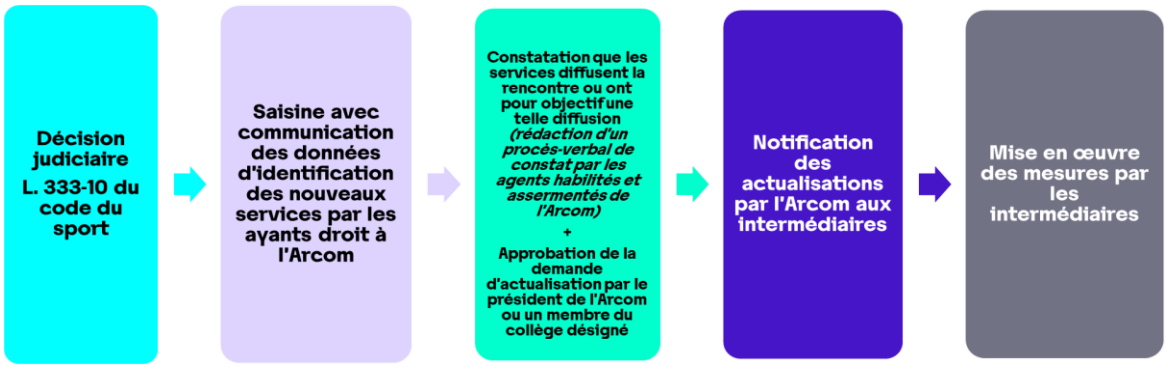
La seconde procédure concerne la **lutte contre la retransmission illicite des manifestations et compétitions sportives**.

Initialement, les mesures judiciaires de blocage ont été conçues pour lutter contre les services culturels contrefaisants, en se fondant sur l'article 8.3 de la directive 2001/29/CE, dite « directive DADVSI ». En France, cette directive a été transposée dans la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) et est reprise,

ainsi qu'il a été dit plus haut, à l'article L. 336-2 du CPI. Ce dispositif permet aux titulaires de droits d'auteur ou de droits voisins de demander en justice le blocage ou le déréférencement de services permettant l'accès à de contenus illicites en ligne : il s'agit donc d'un outil juridique centré sur la protection des œuvres culturelles. Si l'idée d'étendre ce régime aux contenus sportifs a été explorée, notamment à travers un projet d'article dans la directive européenne 2019/790 qui visait à créer un droit voisin au bénéfice des organisateurs d'événements sportifs, la CJUE, dans son arrêt « *Premier League* », a toutefois rappelé que les événements sportifs ne pouvaient pas être qualifiés d'œuvres protégées par le droit d'auteur[24], ce qui a conduit à l'abandon de cette disposition. Malgré cela, la Cour reconnaît que les États membres peuvent instaurer une protection spécifique dans leur ordre juridique interne : en droit français, les fédérations et organisateurs sportifs bénéficient d'un droit d'exploitation sur les compétitions qu'ils organisent (article L. 333-1 du code du sport), et les entreprises audiovisuelles disposent également d'un droit voisin (article L. 216-1 du CPI), offrant ainsi une certaine protection contre le piratage sportif.

Néanmoins, face à l'inefficacité partielle du cadre juridique alors existant pour endiguer la diffusion illégale des événements sportifs[25], la loi du 25 octobre 2021 a introduit un outil plus ciblé. Son article 3 a ajouté au code du sport les articles L. 333-10 et L. 333-11 qui prévoient une nouvelle procédure judiciaire s'appuyant sur des ordonnances dites « dynamiques », permettant à l'Autorité de bloquer ou de déréférencer les nouveaux services illicites pendant la durée d'une compétition ou d'une manifestation sportive. Dans ce dispositif, qui s'inscrit dans le droit-fil des orientations adoptées postérieurement par la Commission européenne dans sa recommandation du 4 mai 2023, l'Arcom joue un rôle clé dans le prolongement des actions judiciaires : elle est habilitée à actualiser les mesures ordonnées par le tribunal judiciaire, en adoptant *a posteriori* les décisions de blocage ou de déréférencement visant les acteurs techniques (comme les FAI ou les moteurs de recherche), afin de suivre l'évolution des sites de *streaming* sportifs illégaux (Figure 3).

Figure 3 : schéma récapitulatif de mise en œuvre du dispositif de lutte contre les retransmissions sportives illicites (articles L. 333-10 et L. 333-11 du Code du sport)



Source : Arcom

Les dispositions législatives précisent également que les frais liés aux mesures de blocage prononcées dans ce cadre doivent faire l'objet d'un accord entre les détenteurs de droits sportifs et les acteurs pouvant participer à la lutte contre les atteintes à ces droits. Dès lors, contrairement aux dispositions qui s'appliquent pour le blocage des

[24] CJUE, 04-10-2011, aff. C-403/08, Football Association Premier League Ltd c/ QC Leisure - https://curia.europa.eu/juris/liste.jsf?language=fr&num=C-403/08
[25] F. Rizzo « Le nouveau dispositif normatif de lutte contre le piratage des droits audiovisuels sportifs », Communication Commerce électronique n° 3, mars 2022, Source Lexis 360 Intelligence.

services culturels illicites, les coûts induits par ce dispositif ne sont donc pas intégralement supportés par les FAI.

Dans ce cadre, l'Arcom a été saisie, depuis 2022, concernant quatorze compétitions sportives (Coupe d'Afrique des Nations, Ligue des Champions, Ligue 1 française, Premier League anglaise, Rugby Top 14 français, Roland-Garros, Wimbledon, Formule 1, Moto GP, Coupe du monde de football, Bundesliga, WTA Tour, La Liga espagnole, Jeux olympiques Paris 2024). La procédure se révèle particulièrement efficace : en 2024, 32 % des internautes consommateurs de sport en *live streaming* ont été confrontés à des blocages de sites illicites, 15 % des internautes confrontés à un blocage se sont tournés vers l'offre légale et 37 % ont cessé leur consommation illicite. Depuis 2022, un total de 10 872 noms de domaine a été bloqué à la suite des notifications de l'Arcom auxquels s'ajoutent 1 976 blocages ordonnés par le tribunal judiciaire de Paris.

Les résultats associés à la mise en place de ces deux nouvelles procédures combinant action judiciaire et action administrative sont donc très prometteurs. Il faut souligner que ces dispositifs ne sont pas exclusifs l'un de l'autre. Ainsi les actions des ayants droit du secteur culturel et des titulaires de droits sportifs sont totalement complémentaires à l'égard notamment des services IPTV illicites. L'action de chacun bénéficie à l'ensemble des deux écosystèmes.

L'Arcom s'est vue par ailleurs dotée d'outils complémentaires pour assurer la protection des contenus culturels et sportifs.

Dans le cadre de la lutte contre les sites miroirs et contre la retransmission illégale des manifestations et compétitions sportives, la loi du 25 octobre 2021 a confié à l'Arcom le soin de proposer des modèles d'accords[26], destinés à être conclus entre les titulaires de droits et les acteurs pouvant contribuer à faire cesser les atteintes à ces droits, en vue d'instaurer un cadre contractuel préventif. Ainsi, le 18 janvier 2023, un modèle d'accord entre titulaires de droits sportifs et FAI visant à protéger les retransmissions sportives a été adopté par le collège plénier de l'Arcom. Le même jour, un accord entre les membres de la Fédération Française des Télécoms (FFTélécoms) et Free et les membres de l'Association pour la protection des programmes sportifs (APPS) a été signé.

3. **Enfin, depuis la loi du 25 octobre 2021, l'Arcom est chargée d'établir et de publier, en application de l'article L. 331-25 du CPI, une liste des services portant « *atteinte, de manière grave et répétée, aux droits d'auteur ou aux droits voisins* ».**

Évoquée dès 2018 dans le rapport de la mission d'information sur une nouvelle régulation de la communication audiovisuelle à l'ère numérique[27], elle vise à faciliter les actions en justice conduite par les ayants droit et le travail de caractérisation du juge mais également à assécher le financement de ces services en encourageant les intermédiaires, notamment ceux impliqués dans la publicité et les paiements en ligne, mais aussi toute autre entité ayant des liens commerciaux avec les services contrefaisants, à cesser ces relations avec les services ciblés afin de tarir leurs sources de financement (stratégie dite « *follow the money* »). Il s'agit enfin de sensibiliser les internautes pour les dissuader d'accéder à ces services pirates (stratégie dite « *name and shame* »)[28].

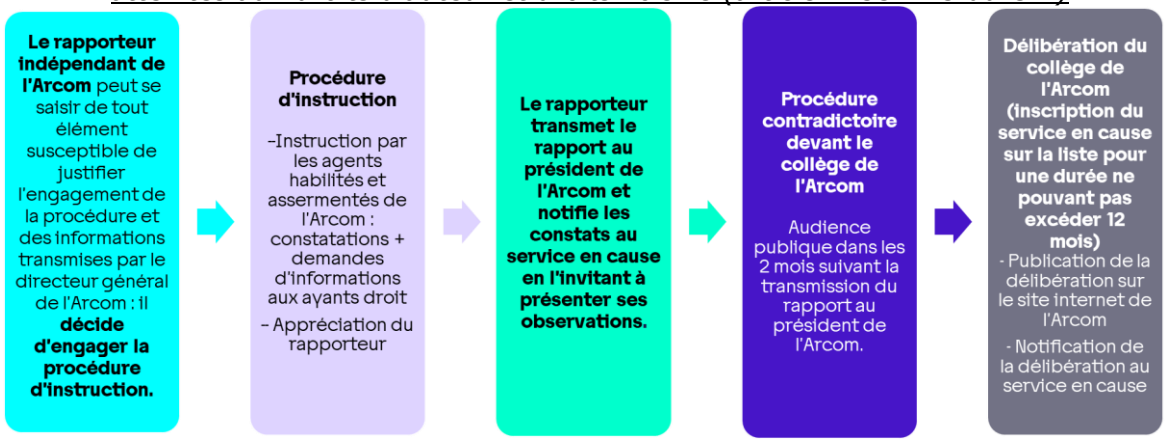
[26] Article L. 331-27, I du CPI et article L. 333-10, IV du code du sport.
[27] https://www.assemblee-nationale.fr/dyn/15/rapports/cion-cedu/l15b1292_rapport-information.pdf
[28] Voir D. Rapone, « De la régulation en matière de propriété littéraire et artistique : les pouvoirs de l'autorité de régulation de la communication audiovisuelle et numérique (Arcom) en faveur de la protection de la création », Revue internationale du droit d'auteur, n°276, avril 2023.

Cette dernière procédure implique l'intervention d'un rapporteur indépendant de l'Arcom pour le déclenchement et le suivi de celle-ci. La caractérisation de l'illicéité des services mis en cause repose sur un faisceau de critères et d'indices qui relèvent de la stratégie qu'il détermine. S'ilestime que les éléments transmis sont de nature à justifier l'inscription sur cette liste, l'Autorité convoque le service dans le cadre d'une procédure contradictoire et, le cas échéant, une délibération d'inscription sur la liste est prise à l'issue de la procédure pour une durée qui ne peut pas excéder 12 mois (Figure 4). Le service figurant sur la liste est en droit de solliciter à tout moment son retrait auprès de l'Arcom, sous réserve de prouver le respect des droits d'auteur et des droits voisins, conformément à l'article R. 331-19 du CPI.

Cette procédure relativement longue et complexe à mettre en œuvre n'a permis d'inscrire que peu de services sur la liste établie par l'Arcom : quatre services ont été inscrits le 26 avril 2023, pour une durée de 12 mois, neuf services l'ont été le 2 mai 2024[29], pour une même durée de douze mois, puis trois services le 13 novembre 2024[30], pour une durée de 12 mois également. Une demande de retrait a également été formulée par un service mais il a été décidé de ne pas y donner une suite favorable.

Les échanges avec le secteur et les institutions nationales et internationales attestent que la mission de caractérisation des services contrefaisants présente un intérêt certain à l'appui des procédures judiciaires. En témoignent les réquisitions faites à l'Arcom dans le cadre d'enquêtes pénales diligentées à l'encontre de certains services, par ailleurs inscrits sur la liste[31]. L'inscription d'un service sur la liste est également un élément probatoire avancé par les titulaires de droits à l'appui de leurs actions judiciaires.
Le faible nombre de services inscrits, en raison de la lourdeur de la procédure, n'a pas permis de donner sa pleine mesure au volet relatif à la signature d'accords volontaires au titre du V de l'article L. 331-25 du CPI. Il en est de même quant à l'objectif de sensiblisation du public. .

Figure 4 : Schéma récapitulatif de mise en œuvre de la mission de caractérisation des atteintes aux droits d'auteur et droits voisins (article L. 331-25 du CPI)



Source : Arcom

[29] 2ddl, Lossless, 33rapmp3, 33rapfrmp3, Sci-Hub, Libgen, Scanmanga-vf, NSW2U, Hdmusic
[30] 1001ebooks, Yggtorrent, Z-library
[31] Certains services ont depuis lors fait l'objet de mesures de fermeture, sur décision des autorités françaises ou étrangères
https://fr.ign.com/nintendo-switch-2/78642/news/le-fbi-se-tient-aux-cotes-de-nintendo-dans-sa-guerre-anti-piratage
https://www.lemonde.fr/pixels/article/2024/09/12/z-library-la-justice-ordonne-le-blocage-du-site-de-telechargement-illegal_6315099_4408996.html

4. La loi du 25 octobre 2021 a aussi été l'occasion de transposer l'article 17 de la directive droit d'auteur, élargissant le périmètre d'intervention de l'Arcom au contrôle de mesures techniques des plateformes de partage de contenus, permettant, *in fine*, de renforcer la diffusion légale de contenus protégés par le droit d'auteur.

L'article 17 de le directive européenne 2019/790 sur le droit d'auteur dans le marché unique numérique a instauré un régime spécifique pour les plateformes de partage de contenus en ligne, reconnaissant à ce titre le rôle clé qu'elles occupent dans la diffusion et la protection de contenus protégés par un droit d'auteur et revenant sur le régime de responsabilité allégé dont elles bénéficiaient en qualité d'hébergeur. Transposé par l'ordonnance n° 2021-580 du 12 mai 2021 aux articles L. 137-1 et L. 137-2 du CPI, le principe est posé que les plateformes qui stockent et donnent accès à un grand nombre d'œuvres protégées sont responsables des contenus mis en ligne par leurs utilisateurs. Elles doivent prouver qu'elles ont fait leurs meilleurs efforts pour obtenir des autorisations, empêcher la mise à disposition d'œuvres signalées et agir promptement en cas de notification d'atteinte aux droits d'auteur et droits voisins.

Ce dispositif vise à généraliser la conclusion d'accords de licence entre plateformes et ayants droit, et à renforcer la mise en œuvre d'outils techniques de protection (ou mesures techniques d'identification – MTI). La loi du 25 octobre 2021 a confié à l'Arcom une mission d'évaluation de l'efficacité de ces mesures, avec la possibilité de formuler des recommandations, de favoriser la coopération entre acteurs et de régler certains différends entre utilisateurs et titulaires de droits (article L. 331-18 du CPI).

Dans deux rapports publiés en 2023 et 2024, l'Arcom a émis plusieurs recommandations après avoir examiné une quarantaine de services, dont 23 relèvent du régime de l'article L. 137-1 du CPI, parmi lesquels certains grands acteurs (YouTube, Meta, TikTok, X, Dailymotion, Snapchat). Elle a constaté qu'un certain nombre d'entre eux ont déployé des outils de reconnaissance de contenus souvent basés sur des technologies d'empreintes numériques, qui montrent leur efficacité dans le secteur audiovisuel et musical, mais s'avèrent moins adaptées voire inadéquates pour l'édition (contenus écrits) et la photographie.

Les accords conclus avec les ayants droit, essentiellement dans les secteurs de l'audiovisuel et de la musique, portent majoritairement sur la monétisation et le blocage, mais leur extension reste limitée à quelques grandes plateformes.

Le traitement des notifications demeure perfectible, notamment en termes de délais et de contacts. Par ailleurs, les rapports de transparence ne permettent pas de savoir le temps moyen de réaction des plateformes pour traiter les signalements relatifs à des contenus portant atteinte à la propriété intellectuelle. Toutefois, on relèvera que les plateformes (hors boutiques d'applications) mettent pour la majorité d'entre elles moins de 24 heures pour traiter les signalements, tous types de contenus confondus.

5. En complément de ces nouvelles missions, la loi a pérennisé le rôle de l'Arcom en matière de sensibilisation des publics.

L'article L. 331-12 du CPI précise que l'Arcom « *mène des actions de sensibilisation et de prévention auprès de tous les publics, notamment auprès des publics scolaires et universitaires* ». Cette précision législative entérine et renforce les actions que réalisaient déjà, avant leur fusion, l'Hadopi et le CSA. En premier lieu, une convention

entre le président de l'Arcom et le ministère de l'Éducation nationale et de la Jeunesse a été signée le 17 janvier 2023, visant à renforcer les coopérations entre le ministère et le régulateur dans le domaine de l'éducation aux médias et à l'information (EMI), et faisant suite aux précédentes conventions signées avec l'Hadopi en 2019 et le CSA en 2020. Dans ce cadre, l'Arcom a accéléré la tenus d'ateliers de sensibilisation auprès des élèves des cycles 3 et 4 (école élémentaire et collège), qui ont rassemblé entre 2018 et 2024 environ 55 000 élèves sur l'ensemble du territoire, dont 6 500 pour la seule année 2024.

Dans une logique de coopération élargie, l'Arcom et ARTE Education ont signé le 16 janvier 2024 une convention de partenariat, visant à l'élaboration conjointe de ressources pédagogiques qui seront disponibles sur la plateforme Educ'ARTE. Dans le même temps, Arte EDUCATION est devenu partenaire du projet « documentaire de poche », mis en œuvre depuis 2015.

Enfin, l'Arcom réalise des campagnes de communication auprès du grand public, à l'instar de la campagne « *Merci !* », développée conjointement avec le Centre national du cinéma et de l'image animée (CNC) et diffusée dès le printemps 2023 sur les écrans, les antennes radios et sur les réseaux sociaux[32].

1.3 À la suite de la réforme de 2021, la consommation de sites illicites a diminué même si celle-ci continue à se maintenir à des niveaux significatifs

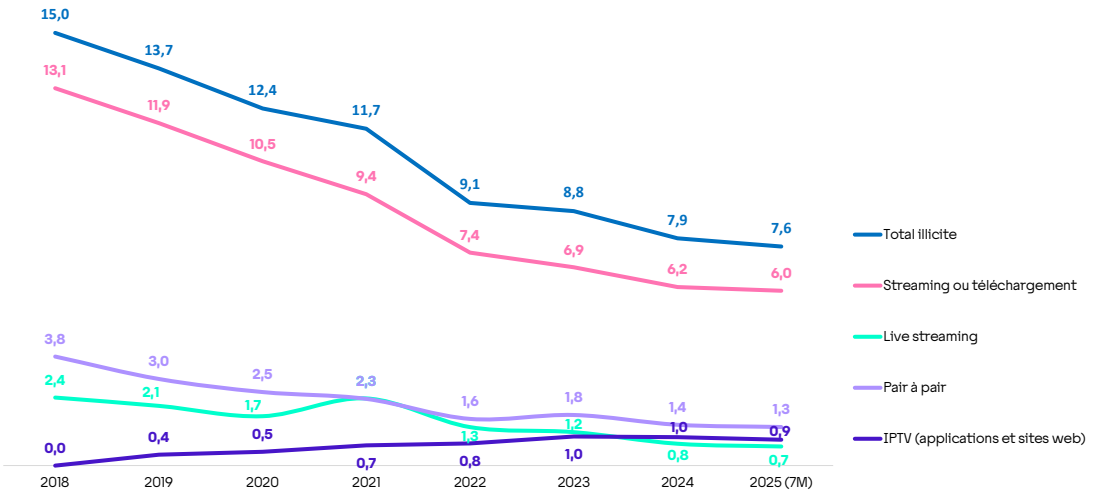
Le recours aux principaux modes de consommation illicite a fortement diminué depuis l'intervention de la loi du 25 octobre 2021 : entre 2021 et 2025, l'audience globale des sites et applications de pair à pair, de *streaming*, de *live streaming* et de téléchargement direct a baissé de 35 %, passant de 11,7 millions d'internautes à 7,6 millions, soit un taux de pénétration global de 13,5 % des internautes.

1. **L'audience de l'offre illégale est actuellement au niveau le plus bas jamais mesuré.**

L'élargissement des outils de lutte contre les usages illicites, qui a été précédemment décrit, a permis de maintenir, voire de renforcer, la baisse du recours à ces différents protocoles (Figure 5).

[32] https://www.arcom.fr/actualites/larcom-et-le-cnc-lancent-la-nouvelle-campagne-de-sensibilisation-la-lutte-contre-le-piratage

Figure 5 : Evolution de l'audience annuelle des sites et applications illicites par protocole d'accès (2018 à 2025), en millions d'internautes -



Source : Arcom, retraitement données Médiamétrie / NetRatings

La comparaison détaillée de l'évolution de l'audience illicite de ces services, entre la période 2018-2021 et la période 2021–2025, atteste de l'impact conséquent des actions de l'Autorité depuis 2022 (Tableau 1) :

- le recours au *streaming* et au téléchargement direct, que seuls les titulaires de droits en matière culturelle pouvaient combattre, a poursuivi sa baisse sensible, du fait de la possibilité pour l'Autorité de lutter contre les sites miroirs (baisse de 36 % depuis 2021 contre 28 % durant les quatre années précédentes) ;
- la très forte diminution des usages illicites du *live streaming* est patente, ce protocole, massivement utilisé afin de visionner illégalement des contenus sportifs en direct, ayant subi les milliers de blocage sportifs notifiés aux FAI par l'Autorité (diminution de 70 % contre 4 % avant la loi de 2021) ;
- et même la diminution de l'usage illicite du pair à pair se poursuit.

Tableau 1 : évolution de l'audience illicite, par protocole, en millions d'individus

	Audience illicite, en millions d'individus			***Evolution, en %***		
	2018	**2021**	**2025**	***2018-2021***	***2021-2025***	***2018-2025***
Audience totale	**15,0**	**11,7**	**7,6**	***-22%***	***-35%***	***-49%***
***Streaming* + téléchargement direct**	13,1	9,4	6,0	*-28%*	*-36%*	*-54%*
Pair à pair	3,8	2,3	1,3	*-39%*	*-43%*	*-66%*
Live streaming	2,4	2,3	0,7	*-4%*	*-70%*	*-71%*

Source : données Médiamétrie NetRatings, retraitement Arcom

La mesure de l'audience des sites et applications illicites, si elle permet de suivre finement les usages des principaux protocoles utilisés pour accéder aux biens culturels dématérialisés et retransmissions sportives, n'offre cependant pas une vision exhaustive des usages illicites. Certains usages ne sont pas, ou de manière incomplète, pris en

compte par les mesures d'audience internet : c'est le cas des pratiques physiques (telle que l'échange entre individus de clés USB ou de disques durs externes) mais surtout du recours à l'IPTV illicite (cf. annexe), dont la mesure d'audience (environ 900 000 utilisateurs comptabilisés sur les sept premiers mois de l'année 2025) n'intègre pas les usages de consommation illicite sur les téléviseurs au moyen de boitiers spécifiques ou directement sur un téléviseur connecté.

Le recours aux études déclaratives permet d'appréhender plus finement l'usage de l'IPTV illicite : d'après l'étude[33] de l'Arcom réalisée sur ce sujet en 2024, 11 % des internautes déclarent y avoir déjà recouru. Ce phénomène est plutôt récent, puisque les deux tiers (66 %) des utilisateurs d'IPTV illicite ont débuté cette pratique il y a moins de trois ans et concerne plus particulièrement des internautes ayant un profil plutôt masculin, issu des catégories socioprofessionnelles supérieures et un peu plus jeunes que la moyenne (35 ans en moyenne contre 38 ans pour les autres utilisateurs ayant des pratiques de consommation illicite de contenus audiovisuels).

Si l'Arcom peut lutter avec une réelle efficacité contre le pair à pair ou le *live streaming*, les usages IPTV illicites s'avèrent plus complexes à neutraliser (malgré une augmentation significative du nombre de blocages de noms de domaine permettant d'accéder à des services IPTV sur les 12 derniers mois).

Ainsi, en considérant l'ensemble des méthodes d'évaluation du piratage en France – mesures dite passives avec le suivi de l'audience illicite, mesures déclaratives avec des enquêtes quantitatives par sondage – ce sont environ 24 à 25 % des internautes français qui ont eu des pratiques illicites[34] durant les 12 derniers mois, les pratiques illicites « historiques » (13,5 % d'internautes y ayant recours) diminuant sur le long terme au profit de l'IPTV (11 % des internautes).

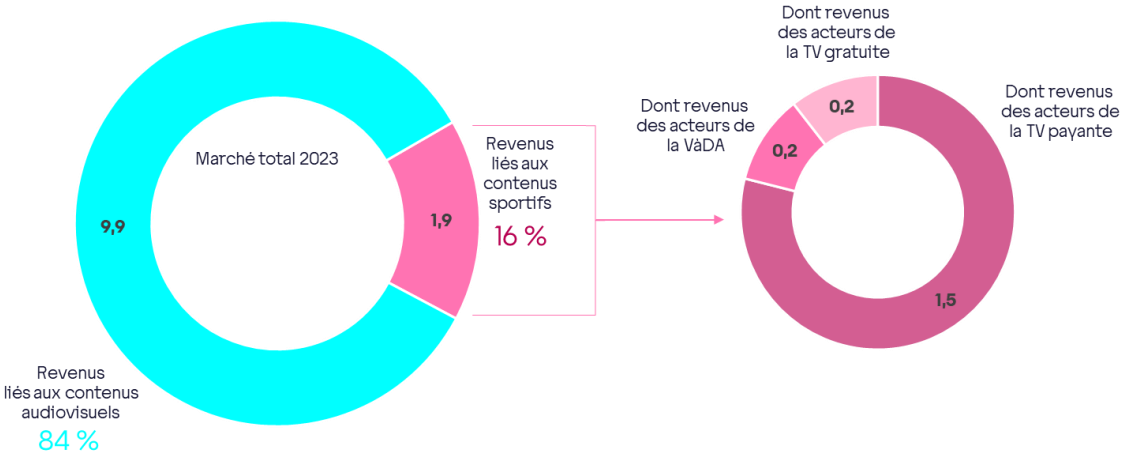
2. Le manque à gagner lié à la consommation illicite de contenus culturels et sportifs représente toutefois 12 % du marché audiovisuel légal actuel.

L'étude socioéconomique[35] menée pour l'Arcom par le cabinet de conseil PMP en 2023 montre que l'impact économique du piratage reste préoccupant. Le marché légal de la diffusion de contenus atteint 11,8 milliards d'euros en 2023, en croissance annuelle moyenne de +2,4 % depuis 2015 malgré la crise de la Covid-19.

Les revenus liés à la distribution de contenus sportifs représentent en 2023 environ 16 % des revenus totaux liés à la consommation de contenus, dont 13 % pour les acteurs de la télévision payante, 2 % pour les acteurs de la télévision gratuite et 2 % pour les acteurs de la vidéo à la demande (VàD) (Figure 6).

[33] Arcom (2024), « la consommation audiovisuelle illicite en IPTV », https://www.arcom.fr/sites/default/files/2024-11/Arcom-Consommation-audiovisuelle-illicite-en-IPTV-2024_0.pdf
[34] Arcom (2025) « baromètre de la consommation des contenus culturels et sportifs dématérialisés », https://www.arcom.fr/sites/default/files/2024-11/Arcom-Barometre-consommation-des-contenus-culturels-et-sportifs-dematerialises-2024_0.pdf
[35] Arcom (2024), « étude d'impact socioéconomique sur l'industrie audiovisuelle et les finances publiques de la consommation illicite en ligne », https://www.arcom.fr/sites/default/files/2024-12/Arcom-etude-impact-socioeconomique-industrie-audiovisuelle-et-finances-publiques-consommation-illicite-en-ligne-2024_0.pdf

Figure 6 : Répartition des revenus liés à la diffusion de contenus audiovisuels et sportifs | 2023, milliards d'euros



Données Arcom, CNC, Analyse et estimations PMP Strategy

Le manque à gagner total consécutif au piratage est estimé à 1,5 milliard d'euros en 2023 : 1,2 milliard d'euros pour l'audiovisuel (12 % du marché légal) et 290 millions d'euros pour le sport (15 %). Les pertes concernent producteurs, distributeurs, exploitants, clubs,organismes de gestion collective et Centre national du cinéma et de l'image animée (CNC), mais aussi les finances publiques : environ 230 millions d'euros de TVA non perçus, auxquels s'ajoutent 190 millions d'euros de cotisations sociales et impôts divers non perçus également.

3. Le détournement de l'usage des services de VPN et de DNS à des fins de consommation illicite constitue une pratique de plus en plus utilisée.

Les mesures de blocage mises en œuvre par les FAI ne sont effectives que pour les internautes utilisant les DNS de leur FAI. Ces mesures peuvent être contournées par le recours à des DNS alternatifs (parfois appelés DNS publics ou DNS tiers) ou des VPN, rendant le blocage ineffectif[36]. Par défaut, tout internaute utilise le DNS de son FAI. Néanmoins, les paramètres de son navigateur internet peuvent être modifiés afin de sélectionner un résolveur DNS alternatif. Ces DNS alternatifs proposent généralement une fonctionnalité de « DNS sécurisé », ou DoH (pour *DNS over HTTPS*) : ce mode permet de chiffrer les requêtes DNS de l'internaute.

La plupart des navigateurs web proposent aujourd'hui une présélection de services alternatifs de DNS sécurisés et publics. Aucune inscription n'est requise pour utiliser ces services et il n'est pas non plus nécessaire de valider des conditions générales d'utilisation ou des dispositions relatives aux données personnelles. Il suffit de choisir un fournisseur de services DNS dans la liste prédéfinie ou d'entrer les coordonnées d'un autre fournisseur sélectionné par l'internaute. L'activation du DNS est quasi immédiate : l'opération revient donc pour un internaute à consulter un autre « annuaire » que celui proposé par défaut par son FAI, tels que, par exemple, Google DNS, Cloudflare, Quad9.

[36] Cf. annexe technique – présentation détaillée du fonctionnement du DNS et du VPN.

Le VPN, quant à lui, permet généralement de chiffrer les communications électroniques des internautes (ce qui est particulièrement utile pour les usages professionnels et pour la protection de la vie privée). Son usage a néanmoins aussi pour conséquence de rendre possible l'accès à des sites bloqués. En effet, le VPN permet aux internautes de simuler une connexion depuis un pays différent (le « point de sortie ») de celui dans lequel ils se trouvent réellement, et d'accéder ainsi à des contenus bloqués localement. La plupart des VPN personnels offrent aux utilisateurs la possibilité d'installer directement sur leur ordinateur ou sur leur téléphone une application permettant d'activer ou de désactiver rapidement le VPN, ou encore de changer instantanément de point de sortie. Ces outils ergonomiques et grand public sont proposés majoritairement à des tarifs très attractifs : certains ont un coût de service qui ne dépasse pas 2,50 € par mois, par le biais de promotions ou de tarifs dégressifs.

L'étude réalisée par l'Arcom[37] montre que le recours à un VPN ou à un DNS alternatif concerne aujourd'hui 35 % des internautes français à titre personnel. Parmi ces deux outils, le VPN est le plus répandu : **29 % des internautes déclarent l'utiliser dans le cadre privé** (15 % l'utilisent régulièrement, et 14 % occasionnellement) contre 20 % s'agissant des DNS alternatifs, tandis que 14 % recourent aux deux.

Pour la grande majorité des utilisateurs, cette pratique est assez récente : 71 % des internautes utilisent un VPN depuis moins de trois ans (25 % depuis moins d'un an). S'agissant des DNS alternatifs, 73 % ont modifié leur DNS pour la première fois il y a moins de trois ans (32 % il y a moins d'un an).

En raison des possibilités de contournement des mesures légales de protection des contenus en ligne qu'ils permettent, le VPN et les DNS public alternatifs voient donc leur utilisation plus répandue chez les internautes ayant des pratiques illicites : plus d'un sur deux (57 %) utilisent un VPN et 46 % ont déjà modifié les paramètres DNS sur leurs équipements. Ainsi 66 % des consommateurs illicites utilisent le VPN ou les DNS alternatifs et 37 % ont recours aux deux, des usages encore plus marqués chez les 25-34 ans, qui sont 74 % à y recourir (67 % chez les 15-24 ans).

Au demeurant, les usages illicites font figure de catalyseur de recours aux VPN et DNS alternatifs : pour 21 % des utilisateurs de VPN (31 % de ceux ayant des usages contrefaisants) et 29 % des utilisateurs de DNS alternatifs (32 % auprès des consommateurs illicites), la réception d'une recommandation de l'Arcom ou la confrontation à un blocage de site internet ont constitué un élément déclencheur pour l'utilisation de l'outil.

À la lumière de ces éléments, le contexte d'adoption rapide des innovations technologiques par les contrefacteurs souligne la nécessité de doter les autorités publiques de nouveaux outils, tout en adaptant encore le cadre normatif.

[37] Arcom (2024), « usage des outils de sécurisation d'Internet à des fins d'accès illicites aux biens dématérialisés », https://www.arcom.fr/sites/default/files/2024-04/Arcom-Usage-des-outils-de-securisation-Internet-a-des-fins-acces-illicites-aux-biens-dematerialises-Rapport-etude-qualitative-et-quantitative-avril-2024.pdf

II. Si l'action du régulateur aux côtés de l'autorité judiciaire s'est révélée efficace, elle nécessite encore des adaptations face aux évolutions rapides des pratiques illicites en ligne

Une fois exposée la chronologie et la teneur des politiques de lutte contre le piratage en ligne, il convient désormais de s'attarder sur les facteurs exogènes à prendre en considération pour déterminer de futures mesures anti-piratage, tels que l'influence des autres modèles de lutte contre le piratage adoptés en Europe, les avancées technologiques du numérique, la résilience de l'écosystème illicite, les obstacles juridiques et le coût financier de ces politiques.

2.1 Le modèle français dual de lutte contre le piratage en ligne n'est pas une spécificité en Europe, même si les approches diffèrent d'un pays à l'autre en ce qui concerne le rôle attribué à l'autorité administrative nationale

1. **Comme en France, plusieurs Etats membres de l'Union ont choisi de mettre en place un système mixte de lutte contre le piratage de contenus sportifs en ligne dont certains peuvent, selon les pays, être aussi utilisés à des fins de lutte contre le piratage de biens culturels dématérialisés[38].**

Le modèle **belge** est celui qui s'apparente le plus à celui mis en œuvre en France : les décisions de blocage sont d'abord délivrées par le juge et l'intervention administrative intervient ensuite en application de cette décision. Depuis 2024, une procédure judiciaire accélérée permet aux titulaires de droits de saisir, en urgence, le président du tribunal de l'entreprise de Bruxelles qui peut ordonner des mesures provisoires visant à faire cesser une atteinte manifeste et substantielle à un droit d'auteur, à un droit voisin ou aux droits du producteur d'une base de données, lorsqu'elle est commise en ligne[39]. De même, depuis 2024, un service administratif spécialisé a été instauré au sein du Service public fédéral de l'Economie (équivalent du ministère de l'Economie) pour assurer la mise en œuvre effective des décisions judiciaires, sans en modifier la durée ou le contenu. Ce service peut définir les mesures concrètes à appliquer par les intermédiaires (FAI, moteurs de recherche…), les informer, recueillir leurs éventuelles observations sous trois jours, puis leur communiquer les mesures définitives à mettre en œuvre. Comme en France, le service peut également rendre les injonctions du juge dynamiques, en identifiant les sites miroirs et en communiquant la liste de ces sites aux services intermédiaires visés par l'injonction initiale. Fortement inspiré par le modèle français, la mise en œuvre opérationnelle de ce sytème a donné lieu à de nombreux échanges avec les équipes de l'Arcom.

En **Lituanie**, à l'inverse, c'est la procédure administrative qui précède l'intervention judiciaire. Agissant sous la supervision du ministère de la Culture, la Commission lituanienne de la radio et de la télévision (RTKL) est l'autorité centrale qui est responsable de l'émission d'injonctions de blocage. Elle peut ainsi émettre des

[38] Le dispositif italien d'injonctions dynamiques a été élargi à la protection de l'ensemble des évènements en direct et le dispositif grec à l'ensemble des retransmissions audiovisuelles. En juillet 2025, le SPF Economie belge a été chargé de l'actualisation d'une décision judiciaire concernant le piratage de livres numériques.
[39] https://economie.fgov.be/en/themes/intellectual-property/intellectual-property-rights/copyright-and-related-rights/sanctions-and-legal-actions/online-piracy

injonctions de blocage qui devront ensuite être validées par le tribunal administratif du comté de Vilnius, à l'exception des décisions de blocage dynamique.

Pour **l'Espagne**, la lutte contre le piratage sportif repose sur une coopération structurée entre les titulaires de droits, les FAI, le juge et une autorité administrative spécialisée, la division anti-piratage (ADP) de la deuxième section de la Commission de la propriété intellectuelle. Le processus débute par un signalement d'atteinte aux droits auprès de l'ADP par les ayants droit. Une instruction préliminaire est menée pour vérifier l'infraction et identifier les responsables. En cas de confirmation, une décision administrative impose à l'opérateur concerné de retirer le contenu sous 48 heures ou de présenter ses observations. Si aucun acteur n'est clairement identifié, l'ADP peut saisir le juge, qui est à même d'ordonner le blocage du service illicite. En l'absence de retrait dans les délais, l'ADP rend une décision finale imposant le blocage sous 24 heures. Si cette décision reste sans effet, elle est également soumise au juge pour exécution.

Au **Royaume-Uni**, le modèle est également mixte même si la base du dispositif de lutte contre le piratage en ligne repose sur des actions en justice. Les ayants droit peuvent saisir les tribunaux pour obtenir des injonctions ciblées contre les intermédiaires techniques (FAI, plateformes) afin de bloquer ou retirer l'accès à des contenus illicites. Ces injonctions sont délivrées par des juges après examen des demandes, garantissant un contrôle judiciaire strict. Les ayants droit peuvent également obtenir des injonctions en direct, principalement dans le domaine du sport[40]. Enfin, le modèle s'appuie sur une coopération volontaire et structurée entre ayants droit, intermédiaires et autorités, par des codes de conduite et des mécanismes de dialogue. Cette approche préventive vise à limiter les recours judiciaires souvent lourds, en favorisant des solutions rapides, proportionnées et concertées.

2. À côté des modèles mixtes, plusieurs Etat européens ont choisi de privilégier un système quasi exclusivement administratif. En pratique, ce système repose sur l'action d'autorités administratives ou publiques indépendantes qui agissent sans passer systématiquement par le juge. Si un tel modèle permet une action rapide et vise à endiguer le piratage à grande échelle sans surcharger les tribunaux, il peut néanmoins présenter des lacunes en matière de protection de la liberté de communication en ligne.

Le cas **italien** est particulièrement révélateur. En Italie, la lutte contre le piratage sportif complète un cadre judiciaire traditionnel (ordonnances judiciaires) par une procédure administrative spécifique confiée à l'AGCOM, le régulateur compétent, qui joue un rôle central, surtout depuis les réformes législatives de 2018 et 2023 renforçant ses pouvoirs, notamment pour les contenus diffusés en direct. À cet égard, l'Italie fait partie des premiers États membres à avoir déployé une plateforme automatisée, le *Piracy Shield*, facilitant les injonctions dynamiques de l'AGCOM[41] en permettant le blocage des services illicites sous 30 minutes, notamment par l'adresse IP et y compris *via* d'autres

[40] La première injonction de blocage en direct au Royaume-Uni a été accordée en 2017 dans le cadre d'une affaire portée devant les tribunaux par la Premier League. L'injonction visait les serveurs de streaming, mais uniquement pendant les périodes de diffusion en direct des matchs de Premier League, et sur la base d'une liste de serveurs cibles réactualisée chaque semaine. Première du genre au Royaume-Uni, cette injonction était de courte durée, couvrant les deux mois précédant la fin de la saison de football 2016/17. Depuis, d'autres injonctions similaires ont été prononcées en faveur de la Premier League et de l'UEFA.
[41] La résolution n° 189/23/CONS, ainsi que le décret Omnibus, constituent une mise à jour importante de la législation sur le droit d'auteur, en instaurant un système automatisé de lutte contre le piratage, avec un focus particulier sur les événements en direct.

intermédiaires que les FAI tels que les résolveurs DNS, les VPN ou les moteurs de recherche. Cependant, cette plateforme a suscité des critiques, notamment en raison de cas de surblocage[42]. Dans ce cas, les procédures judiciaires et administratives sont liées, la procédure administrative pouvant être suspendue en cas de recours formé devant le tribunal.

En outre, une réforme législative (résolution n° 47/25/CONS)[43] est en cours d'examen en Italie afin d'octroyer à l'AGCOM de nouvelles compétences pour mieux lutter contre le piratage en direct des événements sportifs. L'AGCOM serait habilitée à ordonner aux FAI, y compris les fournisseurs d'accès au service, de bloquer l'accès aux flux illicites par blocage DNS ou IP. Cette réforme introduirait également la possibilité pour les titulaires de droits d'obtenir le blocage de sites hébergeant majoritairement (et non exclusivement) des contenus illicites, et rendrait l'AGCOM compétente pour délivrer des injonctions à l'encontre des hébergeurs établis à l'étranger[44].

En **Grèce** et au **Portugal**, l'autorité administrative de régulation s'appuie également sur un système automatisé de blocage. En Grèce, la lutte contre le piratage repose sur un cadre administratif piloté principalement par l'Organisation Hellénique du Droit d'Auteur (OPI), placée sous la tutelle du ministère de la Culture, et par la commission pour la notification des atteintes aux droits d'auteur sur internet (EDPPI). La procédure administrative de blocage en direct repose sur un système automatisé permettant le blocage DNS, URL et IP, mis à jour en temps réel, même pendant la diffusion d'un événement. Les FAI doivent se conformer à ces injonctions de blocage dans un délai de 30 minutes. L'EDPPI veille aussi à éviter les cas de surblocage, chaque cas étant examiné individuellement. Enfin, conformément à l'article 9 du Règlement européen sur les services numériques (RSN), les FAI doivent notifier à l'EDPPI l'exécution de ses décisions et informer les administrateurs des noms de domaine et adresses IP visés.

Au Portugal, la plateforme automatisée, nommée PPDAC, permet d'analyser les plaintes concernant la diffusion illicite de contenus protégés. Si la plainte est jugée recevable, l'IGAC (*Inspeção-Geral das Atividades Culturais*), autorité publique rattachée au ministère de la culture, notifie le service illicite identifié afin qu'il cesse la diffusion et retire les contenus dans un délai de 48 heures. En cas de non application de la décision, l'IGAC ordonne aux FAI concernés de bloquer l'accès aux contenus illicites, *via* un blocage DNS ou URL. Les décisions de l'IGAC peuvent faire l'objet d'un recours devant le tribunal de la propriété intellectuelle puis devant la cour d'appel, dans un délai de 30 jours après la décision. S'agissant des évènements sportifs en direct, le juge a autorisé, dans la décision *Benfica TV* de 2021, le blocage IP pour lutter contre des retransmissions illicites. Il a considéré, toutefois, que le blocage IP ne s'appliquait qu'à des évènements sportifs spécifiques et uniquement pour la durée de leur diffusion en direct.

[42] Voir https://www.euroispa.org/2025/04/piracy-shield-a-flawed-approach-in-the-fight-against-online-piracy/
[43] https://merlin.obs.coe.int/article/10268
[44] La Commission Européenne a ainsi écrit au ministre des Affaires étrangères italien le 13 juin 2025 pour rappeler l'importance de la conformité du Piracy Shield avec le RSN - https://www.techradar.com/vpn/vpn-privacy-security/italys-privacy-shield-may-be-breaching-eu-law-according-to-lawmakers?utm_source=chatgpt.com / courrier mis en ligne par Torrent Freak : https://torrentfreak.com/images/EC-comments-to-Italy-Addressing-Concerns-250613-.pdf

3. **Enfin, certains dispositifs nationaux de lutte contre le piratage reposent avant tout sur l'action du juge judiciaire qui peut ordonner le blocage ou le déréférencement d'un service diffusant illégalement un contenu protégé. De cette manière, les systèmes judiciaires assurent un haut niveau de protection de la liberté de communication en ligne mais sont souvent plus lents et peu adaptés au piratage en direct des évènements sportifs.**

En **Allemagne**, la lutte contre le piratage repose sur des procédures d'injonctions judiciaires traditionnelles et, depuis 2021, ces dernières sont combinées avec un système volontaire structuré entre acteurs privés. Plus précisément, les titulaires de droits peuvent saisir le juge pour obtenir des injonctions de blocage, notamment à destination des FAI. Cependant, ces procédures se révélant souvent longues et complexes, un code de conduite a été conclu entre les titulaires de droits, les FAI et l'Agence fédérale des réseaux (BNetzA) en vue d'instaurer un mécanisme volontaire de blocage DNS encadré par la BNetzA agissant comme tiers de confiance. Un organisme indépendant allemand, la *Clearingstelle Urheberrecht im Internet* (CUII)[45], gère la mise en œuvre des injonctions de blocage DNS émises par les tribunaux à l'encontre des sites diffusant des contenus illicites. Ce dispositif permet de traiter plus efficacement les cas de sites dont plus de 82 % des contenus sont manifestement illicites, dans des délais compris entre deux et quatre mois. La CUII propose également une procédure accélérée, permettant de bloquer de nouveaux domaines en un à trois jours ouvrables. Cette procédure volontaire permet ainsi d'éviter des procédures judiciaires systématiques, tout en offrant des garanties juridiques et techniques solides. Néanmoins, il convient de noter qu'elle ne couvre que le blocage DNS. Les blocages en direct ne sont par ailleurs pas encore mis en œuvre en Allemagne.

Le **Danemark** recourt à des procédures judiciaires complétées par des mesures volontaires, illustrant une collaboration poussée entre les titulaires de droits, les FAI, les autorités et le juge. Le cadre juridique principal est la loi sur le droit d'auteur[46], qui permet au juge de prononcer des injonctions de blocage, y compris dynamiques. Depuis 2014, un code de conduite volontaire a été signé entre les titulaires de droits danois rassemblés dans la *Danish Rights Alliance* et l'association de l'industrie des télécommunications (*Teleindustrien*). Ce code permet à l'ensemble des FAI signataires de bloquer volontairement un service, dès lors que l'un d'entre eux a reçu une injonction de blocage à l'encontre de ce service. La *Danish Rights Alliance* dispose également de compétences étendues en matière de blocage dynamique depuis 2020 : elle peut signaler directement aux FAI des sites miroirs contenant le même contenu illicite que les sites déjà bloqués, et assume la responsabilité juridique en cas de blocage abusif. Une liste de services illicites automatisée a été mise en place en 2022 par l'association *Teleindustrien*, facilitant la mise à jour technique des mesures de blocage.

Aux **Pays-Bas**, la lutte contre le piratage repose principalement sur des procédures judiciaires, avec un recours croissant à des injonctions de blocage dynamiques et en direct à la fois pour les contenus sportifs et culturels. Lorsqu'un site ou un flux illicite est identifié, les titulaires de droits peuvent obtenir une injonction de blocage IP auprès du juge. Ces injonctions peuvent viser non seulement les FAI mais aussi les services d'hébergement ou les services fournissant l'accès à des serveurs. Une fois l'injonction émise, le blocage doit être mis en œuvre dans un délai de 30 minutes après notification par les titulaires de droits, pour une durée limitée, comme la durée d'un match de football, ce qui permet de limiter l'atteinte à la liberté de communication. En parallèle

[45] Organisme créé et financé conjointement par les fournisseurs d'accès à Internet et les titulaires de droits en Allemagne : https://cuii.info/en/about-us/
[46] Bekendtgørelse af lov om ophavsret LBK nr 1093 af 20/08/2023.

du cadre judiciaire, les Pays-Bas ont mis en place un mécanisme volontaire à travers la convention *One for All*, signée entre l'organisation privée de lutte contre le piratage BREIN (*Bescherming Rechten Entertainment Industrie Nederland*) et 95 % des FAI néerlandais. Grâce à cet accord, lorsqu'une décision judiciaire est obtenue contre un FAI, les autres FAI signataires bloquent également volontairement les sites visés, sans y être juridiquement contraints. L'accord précise que BREIN doit d'abord s'adresser au site et à l'hébergeur avant de solliciter les FAI en vue de faire cesser l'atteinte aux droits. L'accord impose également des précautions contre le surblocage.

Tableau 2 : Récapitulatif des dispositifs nationaux analysés

	Type de système	Procédure volontaire	Injonctions dynamiques	Injonctions en direct
Allemagne	**Procédure judiciaire**	OUI (Procédure volontaire avec intervention administrative)	OUI	NON
Belgique	**Procédure judiciaire puis intervention administrative**	OUI	OUI	*Information non disponible*
Danemark	**Procédure judiciaire** puis mesures volontaires	Code de Conduite (Danish Rights Alliance et Danish Telecom Industries)	OUI avec le soutien de la Danish Rights Alliance	*Information non disponible*
Espagne	Procédure judiciaire puis mesures volontaires ET **procédure administrative puis intervention judiciaire**	OUI	OUI	OUI
Grèce	**Procédure administrative**	OUI (sous l'égide de l'EDPPI)	OUI	OUI
Italie	Procédure judiciaire ET **procédure administrative**	OUI	OUI	Non (réforme législative en cours)
Lituanie	**Procédure administrative puis intervention judiciaire**	OUI (sous l'égide de la RTKL)	OUI	
Pays-Bas	**Procédure judiciaire**	OUI	OUI	OUI
Portugal	Procédure judiciaire ET **procédure administrative**	OUI	OUI	OUI
Royaume-Uni	Procédure judiciaire et administrative	OUI	OUI	OUI

L'analyse de ces différents modèles offre aux autorités françaises un éclairage sur les avantages et les limites d'outils encore peu exploités au niveau national, notamment les systèmes automatisés de blocage et les accords volontaires, tout en soulignant les mesures nécessaires pour prévenir des écueils tels que le surblocage. Il convient également de souligner qu'aucun de

ces systèmes ne se révèle pleinement efficace sur la résorption du piratage en ligne comme le relève une étude de l'EUIPO[47].

Par ailleurs, selon une étude du gouvernement britannique, dont le système est présenté par les titulaires de droits sportifs comme l'un des plus performants en matière de lutte contre les retransmissions illicites de compétitions sportives, 17 % des Britanniques ont regardé du sport en ligne durant les trois derniers mois et 38 % d'entre eux y ont accédé de manière illicite[48] soit un taux supérieur à celui des consommateurs français. En effet, selon une étude publiée par l'Arcom[49] : 62 % des Français déclarent regarder des contenus sportifs en ligne (sur les 12 derniers mois), et parmi eux, 29 % y accèdent de manière illicite. Cette différence peut s'expliquer par le champ d'intervention plus large en France et notamment le nombre de compétitions protégées (jusqu'à 14 et dans tous les domaines du sport) alors que le système britannique ne concerne que la Premier League (première division de football) et les coupes d'Europe.

2.2 Dans un environnement numérique en constante évolution, les titulaires de droit sont appelés à s'adapter aux stratégies adoptées par les services illicites pour les contrer

1. Les titulaires de droits sportifs élargissent leurs actions judiciaires aux moteurs de recherche, aux DNS alternatifs et aux VPN.

Afin de renforcer l'efficacité des mesures de blocage des noms de domaine, les titulaires de droits sportifs ont élargi dès 2023 leurs actions judiciaires aux exploitants de moteurs de recherche en demandant le déréférencement des noms de domaine visés par les demandes de blocage (Google et Microsoft, pour son moteur de recherche Bing). Ces intermédiaires sont désormais systématiquement impliqués dans les actions judiciaires engagées par chaque titulaire de droits sportifs pour la protection des compétitions sportives.

En réponse aux usages détournés des outils tels que les DNS alternatifs et les VPN par les internautes, les titulaires de droits sportifs ont également étendu la liste des intermédiaires techniques assignés devant le juge, au-delà des seuls FAI, en visant les plus importants de ces acteurs. Le code du sport permet en effet aux titulaires de droits de « *saisir le président du tribunal judiciaire pour [ordonner à] toute personne susceptible de contribuer à remédier [aux atteintes à leurs droits]* » de prendre « *toutes mesures proportionnées propres à prévenir ou à faire cesser* » une nouvelle atteinte.

Dans un premier temps, la société d'édition de Canal Plus (SECP) a esté en justice dès septembre 2024 contre Cisco, Cloudflare et Google (en tant que fournisseur de DNS alternatif), dans le cadre de la protection de ses droits d'exploitation des championnats de Formule 1 et de Moto GP. Depuis cette première assignation, la SECP, de même que d'autres titulaires de droits sportifs, assignent désormais systématiquement un

[47] EUIPO (2024), « *Online copyright infringement in the European Union – films, music, publications, software and TV (2017-2023)* », communiqué de presse en français : https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_online_copyright_infringement/2024_online_copyright_infringement_in_the_EU_PressR_fr.pdf
[48] https://www.gov.uk/government/publications/online-copyright-infringement-tracker-survey-13th-wave page 38 et suivante du rapport.
[49] Arcom (2025), « La consommation illicite de programmes sportifs en 2024 » - https://www.arcom.fr/se-documenter/etudes-et-donnees/etudes-bilans-et-rapports-de-larcom/la-consommation-illicite-des-programmes-sportifs-en-2024-resultats-detailles

échantillon élargi de DNS alternatifs, puisqu'au fil des décisions sont désormais impliqués Quad9 et Vercara. Cisco[50], en revanche, a décidé de suspendre son service de DNS (OpenDNS) en France.

Plus récemment, cinq fournisseurs de VPN ont fait l'objet d'actions judiciaires de la part du groupe Canal Plus, de la Ligue de Football Professionnel (LFP) et de beIN SPORTS : Cyberghost, ExpressCo, NordVPN, Surfshark et Proton ont été assignés au printemps 2025. Ainsi, depuis août 2024, des représentants de ces trois catégories d'acteurs, outre les FAI, sont également quasi-systématiquement impliqués dans les actions en cessation engagées par les titulaires de droits (moins fréquemment pour les compétitions courtes, notamment en tennis, voir Tableau 3).

Tableau 3 : Parties impliquées dans les décisions de justice relative à la protection des contenus sportifs, saison 2024-2025

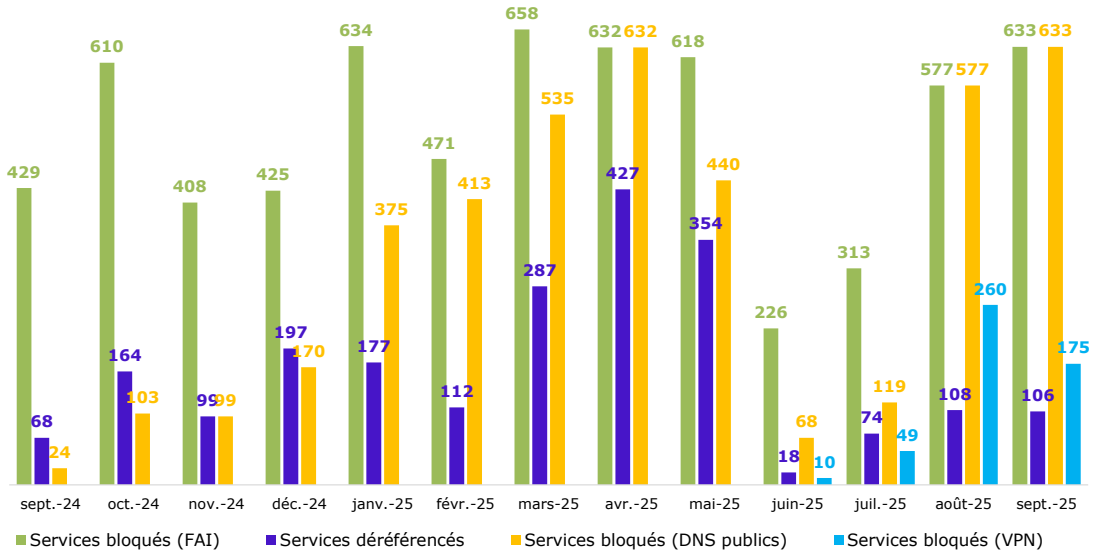
Compétitions (2024-2025)	FAI	Moteurs de recherche	DNS publics	VPN
Ligue 1-Ligue 2	X	X	X	X
Bundesliga	X		X	
EPL	X	X	X	X
TOP 14	X	X	X	X
UCL	X	X	X	X
Roland Garros	X			
Wimbledon	X			
F1	X	X	X	X
MOTO GP	X	X	X	X
WTA	X		X	X

Source : Arcom

Le blocage et le déréférencement des noms de domaine illicites progressent au fil des actions en justice des titulaires de droits : les mois d'août et de septembre 2025 ont connu le plus grand nombre d'intermédiaires s'étant vus notifier des demandes de blocage et de déréférencement. (Figure 9).

[50] https://support.opendns.com/hc/en-us/articles/27951404269204-OpenDNS-Service-Not-Available-To-Users-In-France-and-Portugal .

Figure 9 : Évolution du nombre mensuel de demandes de blocage et de déréférencement notifiées par l'Arcom, depuis janvier 2024



Source : Arcom

Finalement, au-delà des ajustements mensuels, 80 % des blocages DNS demandés aux FAI depuis janvier 2025 l'ont aussi été auprès des DNS alternatifs. Quant aux mesures de déréférencement, elles concernent 35 % des noms de domaine faisant l'objet d'une demande de blocage auprès des FAI (Tableau 4).

Tableau 4 : Comparaison du nombre demandes de blocage et de déréférencement entre 2024 et 2025 (en nombre et en % du nombre total de demande de blocages DNS)

Actions	Janvier-sept. 2024	Janvier-sept. 2025
Total demande de blocages DNS	**2 351**	**4 762**
dont demandes de déréférencement auprès des moteurs de recherche	*625 (27 %)*	*1 663 (35 %)*
dont demandes de blocage auprès des DNS alternatifs	-	*3 792 (80 %)*
dont demandes de blocage auprès des VPN	-	*494 (10 %)*

Source : Arcom

Les FAI et les exploitants de moteurs de recherche exécutent l'ensemble des mesures notifiées par l'Arcom, dans des délais très courts pour les FAI signataires de l'accord (quelques minutes seulement) et dans un délai d'environ trois jours ouvrés en moyenne pour les exploitants de moteurs de recherche.

En revanche, s'agissant des DNS alternatifs - même s'ils sont désormais parfaitement intégrés au dispositif – l'exécution des mesures de blocage est partielle, tout comme pour les VPN.

2. Les DNS alternatifs et les VPN restent encore des acteurs difficiles à impliquer dans les actions anti-piratage.

Une implication systématique des DNS et des VPN aux côtés des FAI et des exploitants de moteurs de recherche semble être envisagée par les titulaires de droits sportifs au vu des nombreux contentieux en cours devant le Tribunal judiciaire de Paris. Les DNS alternatifs comme les VPN ont d'ailleurs fait appel de l'ensemble des décisions prononcées à leur encontre en première instance. Pour autant, ces appels sur lesquels la cour d'appel de Paris n'a pas encore statué ne sont pas suspensifs et les mesures de blocage prononcées par le Tribunal judiciaire sont exécutoires.

Dans ce contexte, la mise en œuvre des mesures de blocage par les fournisseurs de DNS alternatifs ou de VPN en France peut être considérée comme insatisfaisante. En effet, certains de ces intermédiaires techniques, parmi les plus importants acteurs du secteur, n'appliquent que très partiellement les mesures visant à empêcher l'accès aux services illicites, que ce soit en application des décisions de justice ou à la demande de l'Arcom. Ils arguent principalement de leur incapacité à géolocaliser les blocages, fonctionnalité que certains DNS alternatifs sont pourtant déjà en mesure de déployer en France ou semblent pouvoir mettre en œuvre dans d'autres pays[51]. Les fournisseurs de VPN personnels et les DNS alternatifs paraissent encore réticents à l'idée de devoir bloquer l'accès à des services illicites dans les pays où ils opèrent, même s'ils pourraient peiner à justifier durablement leur refus de coopérer. Certains VPN font valoir leur incapacité à agir en précisant qu'ils examinent cependant si d'autres mesures techniques sont envisageables.

La simultanéité de mise en œuvre des différentes mesures est un impératif d'efficacité du dispositif. Deux leviers pourraient permettre d'atteindre cet objectif.

Comme certains FAI, les autres intermédiaires techniques (tels que les fournisseurs de VPN, les DNS alternatifs, les moteurs de recherche,les hébergeurs ainsi que les fournisseurs de réseaux de distribution de contenus) pourraient être incités à conclure des accords volontaires pour faciliter la mise en œuvre des mesures qui leur seraient ordonnées sur le fondement du II de l'article L. 333-10 du code du sport ou qu'ils souhaiteraient mettre en œuvre de façon totalement volontaire (par exemple pour éviter les actions judiciaires).

Si leur volonté de coopération apparaît limitée, il faut rappeler que l'article L. 333-10 du code du sport prévoit que le juge peut, au besoin, ordonner la mise en œuvre des mesures sous astreinte à l'égard des intermédiaires visés. Cette possibilité n'a pas encore été actionnée, à la connaissance de l'Arcom. Cela pourrait être un facteur d'accélération de la réflexion de ces acteurs sur les modalités techniques à mettre en œuvre. Toutefois, cette mesure d'exécution ne pourrait s'appliquer qu'aux données d'identification des services figurant dans la décision judiciaire et non aux demandes transmises par l'Arcom, qui en représentent la très grande majorité (90 % des noms de domaine adressés à ces acteurs).

[51] Annexe: CAA Paris, 22 juillet 2025, n°25PA02012 (§30) - https://paris.cour-administrative-appel.fr/Media/mediatheque-caa-paris/documents/2025/arret-cloudflare.

2.3 Au-delà des limites structurelles des dispositifs actuels, le cadre législatif et règlementaire pourrait, à droit constant, peser sur l'efficacité des actions anti-piratage

1. Tout d'abord, le dispositif actuel n'est pas parfaitement adapté pour lutter contre le piratage en direct : il convient donc de le faire évoluer.

Depuis la loi n° 2021-1382 du 25 octobre 2021, les articles L. 333-10 et suivants du code du sport instaurent un mécanisme original de lutte contre le piratage des manifestations et des compétitions sportives qui repose sur des injonctions dynamiques. Toutefois, au regard des exemples étrangers, et dans un contexte de diversification des services manifestement illicites (services IPTV ou sites de *live streaming* notamment et autres services d'infrastructure), l'automatisation d'une partie de ce dispositif se révèle être une piste d'évolution nécessaire pour répondre aux attentes du secteur.

Depuis juin 2024, l'Arcom dispose d'un système d'information (une application informatique) à usage interne permettant d'automatiser la réception des saisines, une partie de leur traitement et le déploiement des mesures de blocage, notamment le soir et le weekend. Ce système a permis une amélioration du traitement des saisines et par conséquent une augmentation du volume de noms de domaine bloqués. Il est néanmoins jugé insuffisant par le sénateur Laurent Lafon, auteur de la proposition de loi relative à l'organisation, à la gestion et au financement du sport professionnel : *« Plus de 7 000 noms de domaine ont été bloqués à ce titre depuis 2022, ce qui constitue une avancée importante, mais insuffisante compte tenu de la diversité des pratiques de piratage et de l'agilité des fournisseurs de tels services. Étant donné l'ampleur prise par le phénomène, des mesures sont nécessaires pour l'endiguer de façon plus efficace. Ces mesures sont nécessaires mais pas suffisantes*[52]*. »* C'est pourquoi, un dispositif plus général visant à automatiser une partie des injonctions dynamiques figure au nouveau III bis de l'article L. 333-10 prévu par cette proposition de loi.

Pour rappel, en vertu de l'article L. 333-10 du code du sport, le juge judiciaire a la possibilité de prononcer des mesures proportionnées propres à prévenir ou faire cesser les atteintes aux droits telles que le blocage de l'accès aux services diffusant illicitement des rencontres sportives ou ayant pour objectif une telle diffusion. Cette décision judiciaire peut s'appliquer aussi bien à des services identifiés par les titulaires au cours de l'instance judiciaire (concernés par les mesures prononcées par le juge) qu'à de nouveaux services qui apparaitraient dans un second temps (concernés par les mesures notifiées par l'Arcom).

Si la constitutionnalité de la loi du 25 octobre 2021 a bien été soumise à l'examen du Conseil constitutionnel, la décision ne se prononce pas sur ce dispositif en tant que tel, le Conseil n'ayant pas été saisi de grief le concernant. Le Conseil d'Etat, dans ses formations consultatives, a estimé qu'il assurait un juste équilibre entre l'objectif à valeur constitutionnelle de sauvegarde de l'ordre public et les atteintes à la liberté de communication, laquelle recouvre la liberté d'accéder à des services en ligne[53] (CE, Avis, AG, 1er avril 2021, 402564 ; et pour la première ébauche du dispositif, Avis, AG, n° 398829 des 27 et 28 novembre 2019). Cette mise en balance des intérêts, droits et libertés en présence constitutionnellement garantis, est assurée avec soin par ce dispositif – qui se distingue par ailleurs de mesures de blocage purement

[52] Voir l'exposé des motifs de la PPL : https://www.senat.fr/dossier-legislatif/ppl24-456.html
[53] Décision n° 2009-580 DC du 10 juin 2009, Loi favorisant la diffusion et la protection de la création sur internet, cons. 12.

administratives. Cette attention se manifeste notamment par le fait que le blocage de l'accès aux services ne peut intervenir qu'en exécution d'une décision préalable du juge judiciaire.

En outre, plusieurs autres éléments assurent la proportionnalité du dispositif : le champ d'application temporel et territorial limité de l'ordonnance judiciaire (empêcher l'accès aux services à partir du territoire français pendant la durée de compétition ou manifestation sportive), le fait que le juge judiciaire ne peut prononcer des mesures qu'afin de prévenir ou faire cesser des « *atteintes graves et répétées au droit d'exploitation audiovisuelle* » et qu'il peut ordonner « *toute mesure proportionnée* » pour répondre à ces atteintes, laissant à l'intermédiaire technique un délai d'exécution ainsi que le choix des conditions techniques concrètes de mise en œuvre des mesures. Pour finir, le rôle confié par la loi à l'Arcom, autorité publique indépendante, contribue grandement à la proportionnalité du mécanisme.

C'est ce dernier aspect qui requiert toutefois une attention particulière dans le cadre de la mise en place, soutenue par la proposition de loi sénatoriale, d'un dispositif de blocage dynamique en temps réel s'appuyant sur un système automatisé. Cette proposition de loi prévoit que l'Arcom mette en place un système automatisé, placé sous son contrôle, permettant aux titulaires de droits de communiquer les données d'identification des services pour lesquels les mesures sont demandées aux intermédiaires techniques. L'Arcom aurait la responsabilité du contrôle continu de ce système et ses agents habilités pourraient suspendre les mesures irrégulières. Dans un tel système de blocage automatisé où l'Arcom demanderait aux FAI de mettre en œuvre « en temps réel » les mesures ordonnées par le juge judiciaire contre les services non encore identifiés à la date de son ordonnance, il n'est pas prévu d'intervention des agents habilités et assermentés de l'Autorité pour constater, comme ils le font aujourd'hui, que le service diffuse illicitement la compétition ou la manifestation sportive.

Cela étant, à l'aune des risques juridiques éventuels que serait susceptible de présenter le dispositif envisagé, il apparait douteux que puisse être considéré que la circonstance de l'absence d'intervention des agents assermentés de l'Arcom suffise à porter atteinte à la constitutionnalité du dispositif, dès lors que tous les autres éléments assurant déjà sa proportionnalité continueraient d'exister. Au nombre de ces éléments, doit tout particulièrement être mentionné le fait que les mesures seraient autorisées par le juge judiciaire, et pour une durée limitée – celle de la retransmission de l'événement sportif, soit une durée de deux heures environ pour la grande majorité d'entre elles. Par ailleurs, en matière de piratage des retransmissions sportives, l'appréciation des actes illicites en présence est peu sujette à incertitudes : l'appréciation de la diffusion d'un contenu illégal revient *in fine* à analyser si un évènement sportif est diffusé ou non par un diffuseur autorisé. Ainsi, si une diffusion d'un évènement sportif n'est pas effectuée par un diffuseur autorisé, elle est assurément illicite, ce qui explique pourquoi l'intervention du juge « *n'est pas jugée nécessaire au-delà de l'ordonnance initiale* »[54].

Afin de limiter la perte de pouvoir d'appréciation de l'Autorité, la teneur du contrôle exercé par l'Arcom, en particulier sur le dispositif automatisé introduit par la proposition de loi, a été précisée. Le contrôle exercé par l'Arcom est en effet une garantie essentielle dans l'équilibre des droits et libertés fondamentaux en présence dans ce dispositif.

Ensuite, s'agissant du blocage des sites miroirs en application des articles L. 331-27 et R. 331-20 du CPI, il convient de supprimer la condition du passage « en force de chose jugée » de la décision judiciaire initiale.

[54] Voir étude d'impact accompagnant le projet de loi de 2021 introduisant l'article L. 333-10.

Il résulte de l'article L. 331-27 du CPI que l'actualisation de la liste des services bloqués au titre de l'article L. 336-2 du même code se fait sur le fondement d'une décision judiciaire « passée en force de chose jugée ». Ces dispositions posent toutefois actuellement deux difficultés.

En opportunité, l'interprétation littérale de ces dispositions présente un inconvénient pratique pour les titulaires de droits qui paraît même contraire à l'esprit du législateur[55] : les sites miroirs apparaissant dès que les décisions judiciaires sont édictées, voire même avant, tout délai supplémentaire dans l'actualisation de la mesure de blocage rend le dispositif peu pertinent et en affecte la portée.

En droit, cette condition expose l'autorité à des risques. Dans une décision récente, le Conseil d'État a estimé que les décisions prises selon la procédure accélérée au fond, qui bénéficient de plein droit à l'exécution provisoire, doivent être considérées comme passées en force de chose jugée au regard des articles L. 331-27 et R. 331-20 du CPI. Par conséquent, l'Arcom ne peut refuser de satisfaire aux demandes de mise à jour des sites à bloquer en exigeant un certificat de non-appel ou une preuve d'acceptation du jugement.

Dès lors, il faudrait plus directement retenir que constituent des décisions en force de chose jugée, pour l'application de l'article L. 331-27 du CPI, des décisions rendues exécutoires.

2. Enfin, de fortes incertitudes d'ordre juridique pèsent sur la pérennité de la procédure de réponse graduée.

Dès lors que la procédure de réponse graduée nécessite le recueil et la conservation de données personnelles relatives à des infractions (contravention de négligence caractérisée, délit de contrefaçon), catégorie de données particulièrement protégées par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ce traitement porte atteinte à la vie privée des intéressés, pour un motif d'intérêt général de protection des droits de propriété intellectuelle sur les œuvres et, plus généralement, de protection de la création. Or, cette atteinte doit être proportionnée au but poursuivi et elle est, de ce fait, encadrée, par des normes constitutionnelles et européennes.

Si, par son arrêt rendu en formation d'Assemblée plénière le 30 avril 2024 dans l'affaire préjudicielle C-470/21 La Quadrature du Net e.a. (dite « Hadopi »), la Cour de justice de l'Union Européenne admet qu'une autorité publique nationale chargée de la lutte contre les contrefaçons commises en ligne puisse accéder à des données d'identification à partir d'une adresse IP, cet arrêt va néanmoins probablement appeler des évolutions dans la procédure de réponse graduée car il impose des exigences nouvelles entourant les modalités de conservation des données par les FAI et les modalités d'accès à celles-ci. Plus précisément, la Cour impose une « *séparation effectivement étanche* » des différentes catégories de données conservées (les données d'identification et les adresses IP) ainsi que l'encadrement de la troisième phase de la procédure par un

[55] En ce sens, le rapport parlementaire d'information n°1292 de l'Assemblée nationale présenté par Mme Aurore Bergé en octobre 2018, directement à l'origine de ces dispositions législatives, soulignait que la décision du juge devait être rendue « *immédiatement exécutoire pour avoir la moindre efficacité* ». https://www.assemblee-nationale.fr/dyn/15/rapports/cion-cedu/l15b1292_rapport-information#_Toc256000003

contrôle préalable par une juridiction ou une autorité administrative dans certaines situations dites « atypiques »[56].

Ainsi, la mise en œuvre pratique de ces exigences soulève des interrogations dont l'issue dépendra de l'appréciation finale du Conseil d'Etat ayant saisi la CJUE au titre d'une question préjudicielle, notamment en ce qui concerne l'obligation de conservation des adresses IP prévue par l'article L. 34-1 du code des postes et des communications électroniques (CPCE), la sensibilité des données transmises par les organismes d'ayants droit à l'Arcom ainsi que le respect des garanties de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 (« directive police-justice »).

2.4 Sur le plan financier, par ailleurs, le coût de la lutte contre le piratage appelle à un nécessaire rééquilibrage afin de garantir la soutenabilité des dispositifs

1. **Le coût total de la mise en œuvre des différentes missions de lutte contre le piratage par l'Autorité est estimé à environ 2,2 millions d'euros en 2024.**

Ce coût se décompose en deux postes :
- la masse salariale pèse pour près des deux tiers (64 %), soit 1,4 millions d'euros, représentant une vingtaine d'agents opérationnels (19,6 ETP) ;
- les coûts externes sont majoritairement dus aux frais de mise en œuvre de la procédure de réponse graduée (détaillés ci-après), auxquels ils convient d'ajouter les investissements informatiques (recours à des prestataires informatiques pour le développement, la maintenance et les évolutions d'applications spécifiques).

Ce montant de dépenses publiques doit néanmoins être analysé à l'aune du manque à gagner dû au piratage, qui s'élève à 1,5 milliard d'euros. Le préjudice subi pour les seules finances publiques est estimé, ainsi qu'il a été précédemment mentionné, à 230 millions d'euros (perte de TVA) : la lutte contre le piratage en représente moins de 2 %.

Par ailleurs, la lutte contre le piratage représente une infime part du budget de l'Autorité : rapportée au montant total exécuté de 56,65 millions d'euros pour l'exercice 2024, ces missions n'en représentent que 3,8 %. Reposant sur de nombreuses tâches encore manuelles (réalisation de constats, envoi de dossiers aux tribunaux dans le cadre de la réponse graduée, etc.), elles nécessitent proportionnellement un nombre relativement important d'agents (5,4 % des équivalents temps plein (ETP) de l'ensemble de l'Arcom, Tableau 5).

[56] Par situations « atypiques », la Cour vise la mise à disposition « répétée, voire à grande échelle » d'œuvres de types particuliers, qui seraient susceptibles de révéler des informations sensibles sur des aspects de la vie privée de la personne en cause, par exemple en établissant son profil détaillé. *(point 112 de l'arrêt CJUE du 30/04/2024).*

Tableau 5 : Estimation du coût annuel des missions de lutte contre le piratage de l'Arcom, pour l'année 2024

Mission	ETP Arcom	Masse salariale	Coûts externes	Coût total
Réponse graduée	9,0	600 k€	730, 2 k€	1 330 k€
Piratage sportif	8,0	620 k€	50 k€	670 k€
Lutte sites miroirs	2,2	150 k€	-	150 k€
Caract. des sites illicites	0,4	30 k€	-	30 k€
Evaluation MTI / offre légale	1,2	90 k€	-	90 k€
Total des missions de lutte contre le piratage	**20,8**	**1 490 k€**	**780 k€**	**2 270 k€**
Total Arcom 2024*	363,0	32 400 k€		56 650 k€
% des missions de lutte contre le piratage	*5,7 %*	*4,6 %*		*4 %*

*budget exécuté en 2024, incluant l'opération exceptionnelle d'aménagement de la nouvelle implantation du siège parisien de l'Arcom dans le 12e arrondissement de Paris.

Source : rapport annuel Arcom 2024 / estimations internes

Dans le détail, deux missions représentent la quasi-totalité des coûts.

La **procédure de réponse graduée**, avec un budget de fonctionnement de 1,3 million d'euros, absorbe **59 % du budget total de l'Arcom consacré à la lutte contre le piratage**. Ce coût est d'autant plus élevé que plus de la moitié (730 k€) est due à des dépenses externes. La procédure implique l'envoi chaque année de plusieurs dizaines de milliers d'avertissements aux internautes, d'abord par courriel, puis par courrier papier, ce qui nécessite des coûts d'infrastructure et d'hébergement, d'acheminement, d'impression et d'envois postaux.

Mais surtout, la loi impose à l'Arcom d'indemniser les FAI pour compenser les surcoûts engendrés par le traitement automatisé des demandes d'identification des titulaires d'abonnement à internet à partir des adresses IP[57]. Ce montant, fixé par un arrêté conjoint des ministres chargés du Budget et de la Culture, s'élève à 96 k€ TTC par FAI, auquel s'ajoute un coût unitaire de 192 € TTC par fichier de demandes d'identification traité (qui peut comprendre jusqu'à 40 000 IP par jour). De tels montants compensent les surcoûts liés à la conception, au déploiement, à l'adaptation, au fonctionnement et à la maintenance des systèmes d'information des FAI, outre les surcoûts de personnel liés au traitement des demandes d'identification des abonnés. Au total, **l'indemnisation des FAI représente un budget de plus de 400 k€ TTC par an pour l'Autorité** (413 k€ TTC pour 2024, estimation de 428 k€ TTC pour l'année 2025).

La mission de lutte contre le piratage sportif est le deuxième poste, pour 670 k€ - dû majoritairement à des frais de personnel, le dispositif découlant du cadre légal prévu par l'article L. 333-10 du code du sport nécessitant de nombreuses étapes réalisées manuellement, de manière plus ou moins automatisée (rédaction des constats, validation de ceux-ci, etc.). Les dépenses externes, d'un montant de 50 k€ TTC, représentent les évolutions informatiques d'une application métier dédiée. Ce poste devra nécessairement progresser à court et moyen terme : l'automatisation des procédés est nécessaire pour pouvoir traiter, à nombre d'agents équivalents, un nombre toujours plus important de demandes de blocages émanant des titulaires de droits

[57] En application des dispositions de l'article L. 34-1 du CPCE, les modalités de compensation des surcoûts identifiables et spécifiques des prestations assurées par les FAI à la demande de l'Arcom sont déterminées par le décret n°2017-313 du 9 mars 2017 (codifié dans le code de la propriété intellectuelle à l'article R. 331-9). Les tarifs applicables à ces prestations sont fixés par arrêté du 23 mars 2017. Quatre FAI sont concernés : Orange, Bouygues Telecom, Free et SFR/SFR Fibre).

sportifs, avec un quasi doublement des demandes chaque année (de 772 blocages réalisés à la demande de l'Arcom en 2022 à 3 794 en 2024) et une augmentation du nombre d'intermédiaires techniques visés.

2. Aux côtés de l'Arcom, la lutte contre le piratage implique d'autres acteurs, publics et privés : ministère de la Justice – tribunaux sollicités par les titulaires de droits, intervention des parquets dans le cadre de la réponse graduée -, organismes de gestion collective, associations spécifiques (ALPA, APPS), titulaires de droits sportifs.

D'une part, s'agissant des actions des titulaires de droits, les ayants droit des secteurs diffusant des œuvres culturelles de manière dématérialisée disposent en interne de ressources humaines dédiées à la lutte contre le piratage en ligne de leurs contenus. C'est le cas des principaux éditeurs TV (Canal+, France Télévisions, TF1, par exemple), auxquels il convient d'ajouter l'Association de lutte contre la piraterie audiovisuelle (ALPA), qui agit au nom de ses membres (éditeurs TV, services de VàDA, producteurs de cinéma), les distributeurs de films et aussi, dans une moindre mesure, le syndicat national de l'édition (SNE), qui centralisent des actions judiciaires pour le compte de leurs membres. C'est aussi le cas des titulaires de droits sportifs, que ce soit les organisateurs de compétitions sportives (Ligue de football, Fédération française de tennis qui organise le tournoi de Roland-Garros, etc.) ou les diffuseurs (beIN SPORTS, DAZN, entre autres, les autres éditeurs agissant tant pour les contenus sportifs que culturels dont ils détiennent les droits).

Ces équipes peuvent consister en une personne (souvent un juriste, rattaché à la direction juridique) ou être une entité dédiée, de plusieurs personnes, prenant en charge de multiples tâches : coordination d'un ou plusieurs prestataires techniques de lutte contre le piratage (prestaire d'identification des flux piratés en IPTV, sur les réseaux sociaux, etc.), mise en œuvre et suivi des actions judiciaires, en lien avec un cabinet d'avocat, lien avec l'Arcom, réalisation ou acquisition d'études de suivi des usages illicites des internautes, etc., et, pour les seuls titulaires de droits sportifs, la contribution financière aux actions de blocage des FAI, selon l'accord signé par l'Association pour la protection des programmes sportifs (APPS) avec la Fédération française des télécoms (FFT).

Au total, au-delà du manque à gagner, la lutte contre le piratage représente, pour l'ensemble des titulaires de droits des secteurs audiovisuels et sportifs, des dépenses agrégées pouvant se compter en millions d'euros.

D'autre part, s'agissant de l'action de l'autorité judiciaire, l'ensemble des parquets des juridictions du territoire national, en matière pénale, est sollicité pour le traitement d'environ 1 400 dossiers de procédure de réponse graduée en moyenne par an.

En matière civile, le tribunal judiciaire de Paris, et particulièrement la 3e section de la 3e chambre, concentre la totalité des actions en matière de lutte contre le piratage sur internet. L'Arcom a été informée depuis septembre 2024 d'une vingtaine de décisions rendues sur des actions en cessation (article L. 336-2 du CPI) et près de trente-cinq décisions rendues sur le fondement de l'article L. 333-10 du code du sport. En fonction de la stratégie contentieuse et du nombre d'intermédiaires visés, il peut y avoir jusqu'à huit décisions pour la protection d'une seule et même compétition.

Cette inflation de procédures liée au nombre croissant de compétitions protégées mais également à la nécessité d'assigner toujours plus d'acteurs pour les titulaires de droits

peut aboutir à un engorgement de cette juridiction. La sollicitation est d'autant plus forte que compte tenu de la durée limitée de certaines compétitions (exemple : tournoi de Roland-Garros), la décision du juge doit intervenir dans des délais particulièrement contraints. Cela aboutit à une mobilisation accrue des ressources humaines au sein de la juridiction judiciaire.

Il faut rappeler que les parties assignées dans ces procédures ne sont pas les services ayant une activité illicite mais les intermédiaires techniques à même de pouvoir contribuer à faire cesser les atteintes.

Dès lors, l'ensemble de ces éléments militent en faveur d'un allègement des procédures, aussi bien pour faciliter les actions des titulaires de droits que pour la préservation des ressources de l'autorité judiciaire. Il pourrait s'agir notamment de l'autorisation du recours à la procédure simplifiée de l'ordonnance sur requête[58], en cas d'atteintes déjà constatées.

[58] Code de procédure civile, article 493 et suivants.

III. L'action du régulateur aux côtés des ayants droit : vers un modèle renouvelé de régulation pour accompagner les titulaires de droits et pour encourager l'autorégulation ainsi que l'implication des services intermédiaires, sous réserve du respect des contraintes constitutionnelles

3.1 Une révision du paradigme de contrôle permettrait d'envisager un modèle renouvelé de régulation

1. En amont, plusieurs évolutions sont souhaitables afin de faciliter les conditions de saisine de l'Autorité par l'ensemble des parties prenantes dans le secteur culturel.

Ainsi qu'il a été dit, la loi du 25 octobre 2021 a renforcé le dispositif de lutte contre le piratage, notamment par l'introduction d'un article L. 331-27 dans le CPI visant à instaurer un mécanisme spécifique de lutte contre les sites miroirs. Entré en vigueur en octobre 2022, ce dispositif produit des résultats encourageants à la faveur d'une forte mobilisation de l'Autorité. Toutefois, certains services illicites, notoires et installés depuis plus de dix ans, résistent aux blocages successifs du juge et de l'Autorité grâce à leur capacité à se répliquer avec une particulière célérité et à assurer rapidement la promotion de leurs services alternatifs – il s'agit principalement des sites de téléchargement direct, s'adressant à des internautes plus technophiles. Dans ce contexte, il apparaît indispensable d'accélérer la capacité d'intervention de l'Autorité afin de renforcer l'efficacité de la lutte contre le piratage. L'actuelle proposition de loi visant à conforter la filière cinématographique en France semble constituer le véhicule législatif adapté.

En premier lieu, afin de permettre une plus grande efficacité de la procédure contre les sites miroirs, il est nécessaire de faciliter la mise en œuvre de la demande de blocage ou de déréférencement en n'imposant plus qu'elle relève de la compétence du collège de l'Arcom mais simplement de son président ou, en cas d'empêchement, d'un membre du collège désigné par lui - à l'instar du *modus operandi* mis en place dans le cadre de l'article L. 333-10 du code du sport. En outre, au regard de ce qui a été exposé plus haut, la condition du passage en force de chose jugée de la décision judiciaire initiale ayant ordonné le blocage d'un site en application de l'article L. 336-2 du CPI doit être supprimée : une simple copie de la signification de la décision judiciaire attestant de sa force exécutoire pourrait être transmise à l'Autorité lors de sa saisine.

En deuxième lieu, la liste des personnes habilitées à saisir l'Arcom aux fins d'obtenir le blocage ou le déréférencement de sites miroirs doit être élargie en cohérence avec le champ des personnes habilitées à saisir le juge pour obtenir le blocage ou le déréférencement du site initial en application de l'article L. 336-2 du CPI. En effet, en l'état actuel de la rédaction de cette disposition, seuls les titulaires de droits parties à la décision judiciaire sont habilités à saisir l'Autorité afin d'en obtenir l'actualisation. Leurs ayants droit, les organismes de gestion collective, les organismes de défense professionnelle et le CNC ne sont pas inclus dans le dispositif de lutte contre les sites miroirs, alors qu'ils ont la capacité d'intenter une action en cessation des atteintes à un droit d'auteur ou à un droit voisin, sur le fondement de l'article L. 336-2 du CPI.

En dernier lieu, afin de faciliter l'exécution des accords pouvant être conclus pour remédier aux atteintes aux droits d'auteur et droits voisins, il est proposé que l'Arcom

tienne à jour une liste des sites miroirs pour lesquels elle a demandé un blocage ou un déréférencement et la mette à disposition des signataires de tels accords.

L'ensemble de ces propositions visant à simplifier la saisine de l'Autorité sont formalisées sous forme d'amendements à la proposition de loi visant à conforter la filière cinématographique en France[59].

<u>Propositions</u> (telles que figurant dans les amendements à la proposition de loi visant à conforter la filière cinématographique en France) : 1) faciliter la saisine de l'Arcom (L. 331-27 du CPI) en supprimant la condition du passage en force de chose jugée ; 2) prévoir que la mise en œuvre de la demande de blocage ne relève plus du collège de l'Arcom mais de son président ou d'un membre du collège ; 3) élargir la liste des personnes habilitées à saisir l'Arcom (notamment les organisations professionnelles) en cohérence avec le champ des personnes habilitées à saisir le juge en application de l'article L. 336-2 du CPI ; 4) prévoir que l'Arcom tienne à jour une liste des adresses de sites miroirs pour lesquels elle a demandé un blocage ou un déréférencement et qu'elle puisse la partager avec des tiers, complétée des adresses des sites dont le juge aura initialement demandé le blocage ou le déréférencement.

2. **En outre, à l'image de ce qui est proposé pour les sites miroirs, l'Arcom pourrait tenir à jour une liste des adresses donnant accès à des services illicites de retransmission sportive qui serait mise à disposition des signataires d'accords volontaires.**

En effet, l'alinéa IV de l'article L. 333-10 du code du sport dispose que l'Arcom « *adopte des modèles d'accord que les titulaires de droits mentionnés au I, la ligue professionnelle, l'entreprise de communication audiovisuelle ayant acquis un droit à titre exclusif et toute personne susceptible de contribuer à remédier aux atteintes mentionnées au même I sont invités à conclure.* ». Ces accords ont, d'une part, pour objectif initial de fluidifier le dispositif d'actualisation en permettant de faciliter la mise en place des mesures ordonnées par le juge à l'encontre des sites non encore identifiés à la date de la décision judiciaire.

Ils ont, d'autre part, pour objectif d'impliquer plus largement l'ensemble des intermédiaires techniques de l'écosystème d'internet, tels que notamment :

- les fournisseurs de systèmes de résolution de noms de domaine ;
- les fournisseurs de services de réseaux privés virtuels (VPN) ;
- les services d'hébergement et les réseaux de diffusion de contenus ;
- les magasins d'application qui proposent des applications manifestement destinées à des fins illicites, ainsi que les places de marché donnant accès à des boîtiers IPTV illicites ;
- les exploitants de moteurs de recherche, en particulier en raison de leur activité de régie publicitaire ;
- les registres de noms de domaine, les bureaux d'enregistrement de noms de domaine, les éditeurs de système d'exploitation ;
- les acteurs de la publicité et du paiement en ligne au titre de l'approche dite « *Follow the money* ».

Cette proposition s'inscrit par ailleurs dans la lignée des recommandations faites par la Commission européenne dans sa recommandation du 4 mai 2023 sur la lutte contre le piratage en ligne des manifestations sportives et autres évènements en direct, qui vise

[59] Proposition de loi adoptée à l'unanimité par le Sénat le 14 février 2024 et transmise à l'Assemblée nationale - https://www.assemblee-nationale.fr/dyn/16/textes/l16b2218_proposition-loi.pdf

à favoriser l'implication des fournisseurs de services intermédiaires et d'autres acteurs du marché tels que les prestataires de services de publicité et de paiement en ligne. De plus, la Commission européenne encourage les autorités publiques à échanger de manière proactive des informations sur les services dont l'accès a été bloqué. Cette possibilité, offerte par un amendement à la proposition de loi relative à l'organisation, à la gestion et au financement du sport professionnel, permettrait à l'Arcom de renforcer son rôle, au niveau européen, de régulateur pleinement engagé dans la lutte contre le piratage sportif.

Par ailleurs, pour inciter à la signature de tels accords, les intermédiaires volontaires pourraient, en cas d'accord entre les parties, ne pas être assignés systématiquement pour mettre en œuvre les mesures en acceptant volontairement d'appliquer une décision impliquant d'autres intermédiaires.

Propositions : 1) (telle que figurant dans les amendements à la proposition de loi relative à l'organisation, à la gestion et au financement du sport professionnel) prévoir que l'Arcom tienne à jour une liste des adresses de services visés par une demande, de l'Arcom ou du juge,de blocage ou de déréférencement au titre de l'article L. 333-10 du code du sport et qu'elle puisse la partager avec des tiers ; 2) permettre plus largement que dans certains accords volontaires, lorsqu'une décision judiciaire est obtenue à l'encontre d'un intermédiaire, les autres signataires de l'accord puissent également volontairement mettre en œuvre les mesures à l'encontre des services visés.

3. En plus de ces simplifications paramétriques, la mise en place d'un dispositif de blocage dynamique en temps réel des services illicites sportifs pourrait impliquer de faire évoluer le cadre de responsabilité de l'Arcom.

Le système mis en place dans le cadre juridique actuel implique la vérification systématique par les agents habilités et assermentés de l'Arcom de tous les noms de domaine faisant l'objet d'une demande de blocage par les ayants droit. Concrètement, environ 150 à 200 noms de domaine peuvent être bloqués chaque semaine, le processus de constatations, l'élaboration des procès-verbaux (un pour chaque nom de domaine) et la validation des blocages prenant plusieurs jours ouvrés aux agents de l'Autorité et au membre du collège désigné à cet effet par le président de l'Autorité. Ce cadre ne présage pas des modalités de blocage : le blocage d'adresses IP est donc envisageable et l'ensemble des parties prenantes (FAI, titulaires de droits sportifs et Arcom) s'y préparent pour une mise en œuvre opérationnelle au plus tard avant la fin du premier semestre 2026 (dans le cadre prévu par un avenant à l'accord entre les FAI et l'APPS, signé en mai 2025).

Néanmoins, à droit constant, et compte tenu de ce *modus operandi*, le blocage d'adresses IP se fera dans des volumes similaires – de l'ordre de la centaine de demandes de blocage par semaine, quel que soit le nombre de retransmissions sportives, et après un travail préalable de validation de plusieurs jours. Or, dans le cadre du blocage IP (au vu des blocages IP déjà déployés dans d'autres pays européens), les adresses à bloquer ne se chiffrent plus en centaines, mais en milliers, compte tenu de la possibilité pour les services illicites de changer d'adresse IP en quelques minutes.

Le cadre actuel n'est donc pas pleinement adapté dans le cas de blocages dynamiques en temps réel, où l'Autorité devra, dans un laps de temps limité – une à deux heures, le temps d'une retransmission sportive – vérifier l'illicéité d'un nom de domaine ou d'une

adresse IP, faire décider par le Président de l'Autorité ou le membre désigné son blocage, puis transmettre cette décision aux FAI.

La proposition de loi relative à l'organisation, à la gestion et au financement du sport professionnel introduit un dispositif de blocage dynamique en temps réel, dédié principalement à la mise en œuvre de blocages par l'adresse IP. Celui-ci place l'Arcom au centre du mécanisme et ce, à toutes les étapes (amont/direct/aval), tant s'agissant du contrôle (du système automatisé et des mesures de blocage) que de sa responsabilité.

Sur le plan opérationnel, l'actuelle proposition de loi intègre un ensemble de garde-fous pour sécuriser le dispositif envisagé. Le nouveau III bis de l'article L. 333-10 du code du sport précise en particulier ce que doit contenir la délibération de l'Arcom, notamment s'agissant de son contrôle sur les modalités selon lesquelles les procédés de collecte des données d'identification par les ayants droit sont soumis à l'accord de l'Autorité, les modalités de communication de ces données à l'Autorité, les conditions de validité des saisines des titulaires de droits, les modalités de collecte et de conservation des éléments de preuve par les titulaires de droits. Il confère en outre aux agents habilités et assermentés de l'Arcom des pouvoirs contraignants (ils « *peuvent à tout moment et par tout moyen s'assurer de la conformité des mesures prises* », ils les « *suspendent sans délai* ») si cette conformité n'est pas assurée, pour garantir une atteinte proportionnée à la liberté de communication en ligne. Il est également prévu que l'Arcom puisse « *adresser, à tout moment, aux titulaires de droits toute recommandation qu'elle juge nécessaire aux fins d'assurer la conformité des mesures prises par l'intermédiaire du système automatisé* » à sa délibération et qu'elle soit « *informée sans délai des suites données à ces recommandations* ». Enfin, un recours administratif porté devant l'Arcom est prévu pour renforcer le contrôle exercé par l'Autorité et garantir l'équilibre du dispositif.

Cette approche « en temps réel » est inspirée des systèmes automatisés anglais et italien. En Angleterre, après une décision cadre du juge qui vaut pour une saison sportive, les ayants droit signalent en direct aux FAI les adresses IP des services à bloquer (de façon entièrement automatisée, sans intervention d'une autorité publique). Sans que les montants ne soient connus, il est admis que ce système a nécessité des investissements importants (en millions d'euros) et une mise en place progressive. En Italie, les ayants droit autorisés par l'AGCOM notifient directement les adresses IP à bloquer aux FAI. Les services bloqués peuvent ultérieurement introduire un recours devant l'autorité italienne. Ce système prévoit des blocages pérennes, ce que la proposition de loi écarte pour limiter les risques de surblocage (les mesures ne seraient effectives que pendant la durée de l'événement sportif).

La mise en place d'un tel dispositif en France impliquerait à moyen terme de faire évoluer les responsabilités de l'Arcom sans recourir, pour autant, à une automatisation intégrale comme celle observée avec l'outil *Piracy Shield* italien, qui pourrait, appliqué au cadre juridique français, présenter des risques d'inconstitutionnalité. À cet égard, le modèle britannique offre un cadre de référence intéressant, fondé sur une collaboration étroite entre ayants droit et intermédiaires techniques. En conséquence, s'il est recommandé d'instaurer une procédure automatisée pour la mise en œuvre des injonctions dynamiques « en temps réel », l'intervention humaine restera nécessaire, et celle-ci pourra être satisfaite par la possibilité donnée aux agents assermentés de l'Arcom de contrôler les mesures. De ce fait, la mise en place de ces contrôles sécurisera fortement le nouveau dispositif, en renforçant la proportionnalité de l'atteinte au principe de liberté de communication en ligne qu'il organise. Relevons également que si la Cour

européenne des droits de l'Homme[60] a censuré un dispositif présentant de forts risques de surblocage, c'est parce qu'il avait lieu durant une durée indéterminée et sans aucun encadrement. Ainsi, ce nouveau cadre pourrait garantir une lutte contre le piratage à la fois rapide, efficace et respectueuse des droits, condition indispensable à un environnement numérique équilibré et sécurisé.

Un tel dispositif implique nécessairement une évolution des tâches de l'Arcom : si aujourd'hui, la responsabilité de l'Autorité consiste à attester l'illicéité des services qui lui sont soumis par les titulaires de droits, dans ce nouveau cadre, l'Arcom sera responsable de la définition, en amont, des conditions techniques garantissant le plus haut niveau de sécurité concernant l'identification et le signalement, par les titulaires de droits, des services illicites ; en aval, l'Arcom devra vérifier la qualité des saisines des titulaires de droits et, dans le cas de saisines de moindre qualité – voire de cas de surblocage – identifier les éventuelles déficiences des systèmes de détection des services illicites mis en place par les titulaires de droits et faire en sorte, le cas échéant, que ces dysfonctionnements cessent promptement.

L'évolution des responsabilités de l'Arcom implique pour l'Autorité un renforcement de son expertise technique – et donc de celle de ses agents, que ce soit par la formation interne ou, éventuellement, par le recrutement d'ingénieurs spécialisés dans les infrastructures informatiques. Ce dispositif nécessitera aussi des investissements pour faire évoluer le système automatisé déjà déployé dans le cadre actuel, investissements pouvant se chiffrer en centaines de milliers d'euros.

Proposition (actuellement dans la proposition de loi relative à l'organisation, à la gestion et au financement du sport professionnel) : la nécessaire mise en place d'un dispositif de blocage dynamique en temps réel des services illicites sportifs (destiné notamment au blocage IP, en complément des blocages DNS mis en œuvre dans le cadre du système actuel) inspiré de certains modèles étrangers, implique de faire évoluer les responsabilités de l'Arcom.

4. **Plus généralement, la simplification des procédures de blocage d'accès aux services illicites constitue un enjeu stratégique, tant du point de vue de la célérité que de l'effectivité des décisions prises en matière de lutte contre les services illicites.**

Au fil des années, de nombreux dispositifs législatifs se sont mis en place en France, impliquant des mesures judiciaires ou administratives de blocage de services de communication au public en ligne (initialement ordonnées aux FAI puis - selon les cas - à une multitude d'autres acteurs).

Ces mesures présentent des caractéristiques et des modes de fonctionnement différents. Certains dispositifs ciblent uniquement certains intermédiaires et pas d'autres, alors que le contexte et les problématiques sont assez similaires. En résultent une situation complexe à appréhender d'un point de vue technique et juridique, ainsi qu'un empilement de dispositifs pointé par les FAI, en première ligne. Ces derniers redoutent que la multiplicité et la disparité des mécanismes à l'œuvre aboutissent à des dysfonctionnements et à des erreurs dont les conséquences peuvent être sévères. Les incidents survenus en France (concernant *Google.fr* en 2016[61] ou *Telegram* en 2023[62])

[60] CEDH, 18 décembre 2012, Ahmet Yildrim, 3111/10
[61] https://next.ink/12171/101786-google-fr-bloque-pour-apologie-terrorisme-orange-invoque-erreur-humaine/
[62] https://next.ink/1122/les-url-telegram-temporairement-bloquees-samedi-par-police/

et plus récemment en Italie (concernant *Cloudflare* en février 2024[63] et *Google Docs* en octobre 2024[64]) sont des exemples éloquents des risques liés au blocage de noms de domaines ou d'adresses IP. Ces incidents sont de nature à remettre en cause la confiance dans les mécanismes de blocage. Par ailleurs, une telle complexité (une vingtaine de dispositifs coexistent, tous distincts et avec des variations qui ne sont pas forcément justifiées ou explicables) engendre des délais incompatibles avec l'urgence souvent requise face à la prolifération de sites ou de services illicites.

Pour remédier à ces difficultés, l'harmonisation des procédures de blocage pourrait à terme s'avérer nécessaire : la mise en place d'un *modus operandi* unifié pour l'ensemble des demandes de blocage, à l'image du modèle centralisé allemand géré par la *Clearingstelle Urheberrecht im Internet* (CUII), permettrait de réduire significativement les risques d'erreurs ou de confusion entre les acteurs impliqués, les vulnérabilités techniques induites par la diversité des protocoles, ainsi que, potentiellement, les coûts des mesures pour les intermédiaires techniques comme pour l'Etat.

Proposition : envisager la conduite d'une mission transversale sur les dispositifs de blocage actuellement en place et étudier les pistes en faveur de leur harmonisation.

5. En aval, l'attribution à l'Arcom d'un pouvoir coercitif en cas de non-application des demandes de blocage par les intermédiaires techniques présente un intérêt pour la crédibilité de l'Autorité dans l'espace numérique.

L'absence de mécanismes contraignants ou de sanctions en cas de non-exécution des injonctions de blocage limite la portée dissuasive des actions de l'Arcom, notamment face à des acteurs récalcitrants ou peu coopératifs. L'Autorité peut uniquement, en cas de difficulté de mise en œuvre des mesures, demander aux services de se justifier.

Doter d'un caractère coercitif les décisions de l'Autorité dans ce domaine, notamment par la fixation d'une mesure d'astreinte, pourrait donc s'avérer pertinent. La loi pourrait prévoir que si le juge - comme le prévoit le dispositif - prononce une astreinte, celle-ci s'appliquerait de plein de droit à l'égard des intermédiaires destinataires des données d'identification transmises par l'Autorité, à l'instar du dispositif mis en œuvre en Belgique[65]. Ce levier supplémentaire s'inscrirait dans une logique de responsabilisation des intermédiaires techniques et de consolidation de la régulation numérique, étant précisé que l'Arcom, soucieuse de faciliter l'exécution des décisions par les intermédiaires techniques, propose, autant que faire se peut, des dispositifs d'interfaçage et d'interconnexion avec les acteurs qui le souhaitent.

Alternativement, un dispositif de sanction à l'encontre des intermédiaires n'appliquant pas les demandes de blocage ou de déréférencement de l'Autorité (tels que ceux prévus aux articles 2 et 14 de la loi visant à sécuriser et à réguler l'espace numérique en matière de protection des mineurs à l'égard de l'exposition aux contenus pornographiques et d'application des sanctions européennes) pourrait être envisagé.

---

63 https://torrentfreak.com/piracy-shield-cloudflare-disaster-blocks-countless-sites-fires-up-opposition-240226/

64 https://techguru.fr/2024/10/30/erreur-alarmante-le-chaos-du-blocage-de-google-drive-en-italie-souleve-des-inquietudes/

65 Tribunal de l'entreprise francophone de Bruxelles, 25 mars 2025, ordonnance prise sur le fondement de l'article XVII.34/1.§8 du code de droit économique. L'astreinte prononcée est de 100.000 par jour de retard. Cette mesure est également appliquée par le ministère de l'économie belge dans sa décision du 1er avril 2025 relative aux sites miroirs : https://economie.fgov.be/sites/default/files/Files/Intellectual-property/Decision-250401-BAPO-D-FR-001-FR.pdf

Proposition : la loi prévoyant que des astreintes peuvent être prononcées par le juge, l'Arcom pourrait être autorisée à appliquer ces mesures d'exécution à ses propres demandes. Un dispositif de sanction en cas d'inexécution des demandes de l'Autorité pourrait être également prévu.

6. Enfin, la liste des services illicites prévue à l'article L. 331-25 du CPI constitue également un outil pertinent, mais qui nécessite d'être repensé.

Pour l'heure, trois services sont inscrits sur la « liste noire » des services contrefaisants (1001ebooks, Yggtorrent, Z-library). Ce nombre très réduit d'inscriptions reflète la longueur et la lourdeur de la procédure, inadaptée à la nature même des services qu'elle vise.

Tout d'abord, il apparaît pertinent de substituer à l'intervention du rapporteur indépendant celle du membre désigné de l'Arcom en application du IV de l'article 4 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, ou de son suppléant. Cette modification permettrait de diminuer les délais de lancement de la procédure d'instruction préalable à l'inscription sur la liste, puis, une fois les procédures lancées, de transmission des dossiers au président de l'Autorité.

Par ailleurs, les ayants droit, qui estiment cette procédure très utile à des fins probatoires dans les actions judiciaires qu'ils engagent, souhaitent qu'elle soit sensiblement simplifiée, en particulier sa phase contradictoire dans les situations où l'éditeur d'un service en cours d'examen ne répond pas aux sollicitations de l'Autorité (les mentions obligatoires de la LCEN ne sont souvent pas respectées par les services en cause).

Dans l'optique d'optimiser le dispositif, il apparaît en particulier pertinent de reconsidérer l'organisation de la phase contradictoire. Une suppression pure et simple de la convocation à une audition contradictoire pourrait être envisagée mais elle présente un risque constitutionnel potentiel : dès lors que les conséquences économiques d'un tel classement affectent la liberté d'entreprendre, l'absence de procédure contradictoire pourrait être censurée, le Conseil constitutionnel imposant des garanties procédurales strictes avant toute atteinte à une liberté fondamentale. Alternativement, un allègement de cette procédure pourrait être mis en place, en laissant au service concerné la faculté de demander une audition contradictoire, sans que celle-ci soit systématique, ou alors, en cas d'absence de réponse de la part du service à la convocation, celui-ci serait automatiquement inscrit sur la liste des services contrefaisants, ce qui offrirait une plus grande souplesse en évitant les blocages liés à des convocations obligatoires.

Propositions : 1) substitution à l'intervention du rapporteur indépendant de celle du membre désigné de l'Arcom en application du IV de l'article 4 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, ou de son suppléant ; 2) modification du mode d'information des services pour lesquels le site internet ne mentionne pas d'informations de contact (prévoir, le cas échéant, que la convocation des services concernés soit faite par l'intermédiaire de la publication de la convocation sur le site de l'Arcom) ; 3) allégement de la procédure de convocation à une audition contradictoire ; 4) allongement de la durée maximale d'inscription sur la liste de 12 à 18 mois et allègement de la procédure en cas de prorogation de l'inscription.

3.2 Un modèle de régulation plus fédérateur permettrait de concilier la protection de la création et des évènements sportifs avec l' innovation.

1. En premier lieu, de nouveaux acteurs doivent être encouragés à s'engager volontairement dans la lutte contre le piratage.

Le mécanisme d'encouragement à la signature d'accords volontaires se présente comme un dispositif propice pour associer davantage d'acteurs, notamment un plus grand nombre de services intermédiaires. Certains acteurs permettant l'accès à l'écosystème illicite pourraient être amenés à s'impliquer de manière volontaire dans la lutte contre le piratage (hébergeurs, moteurs de recherche, systèmes de paiement en ligne, DNS alternatifs, VPN, etc.). Eu égard à cette considération, en vertu de l'article L. 331-12 alinéa 6 du CPI et de l'article L. 333-10 du code du sport, l'Arcom bénéficie d'une compétence générale lui permettant de mettre en place diverses actions (telles que des recommandations, des guides de bonnes pratiques, ou encore des modèles et clauses types) afin de faciliter la conclusion d'accords volontaires visant à garantir la protection des droits d'auteur et des droits voisins.

La portée de cette mesure est étendue[66], ce qui signifie que ces accords peuvent concerner tout acteur souhaitant s'engager volontairement dans la lutte contre le piratage à l'encontre de divers services illicites. Le but de tels accords est de favoriser une participation élargie des intermédiaires, au-delà des seuls FAI, à ce jour seuls signataires d'un accord visant à faciliter la mise en œuvre des mesures de blocage qui leur sont ordonnées par le tribunal judiciaire puis par l'Arcom. À cet effet, l'Arcom cible particulièrement certains acteurs stratégiques tels que les moteurs de recherche, les DNS alternatifs, les VPN, les fournisseurs de réseaux de distribution de contenus ou les proxies inverses, les plateformes d'hébergement, les régies publicitaires ainsi que les prestataires de services de publicité et de paiement en ligne, qu'ils aient ou non déjà été attraits en justice dans des actions en cessation par les titulaires de droits, dans l'objectif de rassembler un maximum de partenaires susceptibles de contribuer efficacement à la prévention du piratage sur l'ensemble de la chaîne de diffusion des contenus.

L'expérience de régulation de l'Arcom montre que le dialogue entretenu avec les intermédiaires techniques permet de limiter significativement les obstacles à leur implication dans les dispositifs nationaux de régulation.

À cet égard, l'Arcom a pu avoir des échanges techniques avec les membres de l'i2Coalition (internet infrastuctre coalition) qui regroupe à l'international les acteurs des infrastructures numériques (DNS, VPN, FAI, etc.) ainsi que plus particulièrement avec les représentants de DNS4EU, un réseau d'infrastructures sécurisées cofondé par l'Union européenne, notamment utilisé par le VPN récemment lancé par Free et couplé à son offre mobile[67].

D'une façon générale, à l'exception des FAI et des moteurs de recherche, partenaires de longue date de la régulation, les intermédiaires techniques font état à la fois de difficultés techniques (par exemple, pour circonscrire une mesure de blocage à un territoire national ou pour identifier la localisation géographique d'une connexion initiale) et d'appréhensions de principe (la crainte d'une « régulation censure »). Les

[66] Aucune liste des intermédiaires susceptibles d'être incités à conclure de tels accords n'est précisée dans les textes, ni les actions qu'ils pourraient entreprendre dans ce cadre.
[67] Communiqué de presse du groupe iliad : https://www.iliad.fr/media/CP_160925_c3274edb1e.pdf

échanges menés et les premiers résultats obtenus pour l'application de mesures de blocage par de nouveaux intermédiaires techniques en matière de lutte contre le piratage montrent que ces difficultés ne sont pas insurmontables mais qu'elles nécessitent qu'une attention particulière soit portée à la qualité du dialogue entretenu ainsi qu'aux difficultés dont ces acteurs font état.

Les acteurs des infrastructures numériques ont vocation à être des partenaires de la régulation.

Proposition : en complément des mesures contraignantes à prévoir pour que les demandes de blocage ou de déréférencement de l'Arcom ou du juge soient appliquées par les intermédaires techniques, maintenir avec ces derniers un dialogue technique de proximité pour tenir compte de leurs difficultés ; encourager la conclusion d'accords permettant la prise en compte des spécificités des différents acteurs impliqués.

2. Par ailleurs, la possibilité d'accéder à des services pirates bloqués en France ne devrait plus pouvoir être utilisée comme argument de vente par des intermédiaires techniques

Les actions judiciaires et administratives, tout comme les démarches de sensibilisation du grand public au respect du droit d'auteur et des droits sportifs, ne peuvent être mises à mal par des messages promouvant ou normalisant l'utilisation de services illicites ou de moyens de contournement des mesures de blocage. En particulier, plusieurs fournisseurs de VPN ont conclu des partenariats commerciaux avec des influenceurs français et construisent leur message promotionnel sur la possibilité offerte de contourner les mesures de blocage nationales.

Si la loi du 9 juin 2023[68] offre désormais un cadre permettant de réguler l'activité d'influence commerciale et de lutter contre certaines dérives constatées sur les réseaux sociaux, il semble nécessaire de renforcer les moyens d'action visant à interdire la promotion, directe ou indirecte, en faveur de pratiques de piratage ou d'abonnement à des services illicites ou permettant de contourner des mesures de blocage, au même titre que des pratiques proscrites par la loi en matière de santé publique, environnement, ou encore de pronostics sportifs.

Proposition : modifier l'article 4 de la loi visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux pour interdire aux personnes exerçant l'activité d'influence commerciale par voie électronique toute promotion, directe ou indirecte, des actes, des procédés, des techniques et des méthodes permettant d'accéder à des diffusions non autorisées en France de compétitions sportives ou d'œuvres ou objet protégées par un droit d'auteur ou un droit voisin.

[68] Loi n° 2023-451 du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000047663185/2025-10-15

3. **En outre, à l'égard des fournisseurs de services de partage de contenus, le régulateur pourrait disposer d'un pouvoir renforcé en matière d'évaluation des mesures techniques d'identification (MTI) qu'ils mettent en œuvre. Ces technologies pourraient d'ailleurs à court terme jouer un rôle essentiel pour assurer un développement des systèmes d'IA compatible avec le respect du droit d'auteur.**

La directive 2019/790 du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique présente la spécificité de déroger au principe européen de l'irresponsabilité liée au statut d'hébergeur, telle que définie par la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (dite « *directive sur le commerce électronique* ») : comme évoqué précédemment, l'article 17 de la directive droit d'auteur crée une exception à ce régime particulier, les fournisseurs de services de partage de contenus étant désormais tenus pour responsables de la diffusion de contenus sans autorisation des titulaires de droits. Cette directive a de même imposé à ces fournisseurs de services le principe du pays de destination, au lieu du principe du pays d'origine qui est la norme dans l'Union Européenne.

Sa transposition en droit national a été particulièrement ambitieuse, confiant à l'Arcom la mission d'émettre des recommandations sur le niveau d'efficacité des mesures de protection des œuvres et des objets protégés prises par les fournisseurs de services de partage de contenus en ligne au regard de leur aptitude à assurer la protection des œuvres et des objets protégés. Elle encourage également la coopération entre titulaires de droits et fournisseurs de services de partage de contenus en ligne en vue d'assurer la disponibilité sur le service des contenus téléversés par les utilisateurs qui ne portent pas atteinte au droit d'auteur et aux droits voisins.

Toutefois, du fait d'un accès limité aux outils de protection, l'Arcom ne peut donner une pleine efficacité à son action. En effet, certains services refusent l'accès direct à leurs systèmes de reconnaissance, réservés exclusivement aux ayants droit. En l'absence de droit d'accès autonome, l'Arcom doit donc recourir à des méthodes indirectes, en passant par les titulaires de droits, ce qui rend l'évaluation lourde et incomplète. Cet obstacle juridique bride la capacité de l'Arcom à mener des analyses techniques approfondies sur ces outils.

De plus, il est à noter que la gestion des droits afférents à une œuvre est aujourd'hui rendue possible à très grande échelle sur les plateformes de partage de contenus par le biais des mesures techniques d'identification (MTI). Ces technologies pourraient également trouver à s'appliquer dans le cas du droit d'opposition (ou *opt-out*) accordé aux titulaires de droit qui refusent que leurs œuvres soient notamment utilisées pour l'entrainement de modèles d'intelligence artificielle (IA) ou dans le cas de licences accordées par les titulaires de droit aux systèmes d'IA, le cas échéant sous conditions.

Elles pourraient également s'appliquer lorsque des contenus protégés sont utilisés par les système d'IA au moment de la phase d'inférence (lorsque le système d'IA répond à l'utilisateur) pour permettre l'identification des usages et la rémunération des ayants droit. L'étude de l'efficacité des outils de reconnaissance des œuvres et objets protégés, et leur éventuelle application étendue aux usages relatifs à l'intelligence artificielle, revêt donc aujourd'hui un intérêt croissant en vue de permettre un développement de l'IA compatible avec la protection du droit d'auteur.

La généralisation des mesures techniques d'identification et le renforcement du contrôle de leur efficacité par l'Autorité permettrait ainsi d'assurer un haut niveau de protection du droit d'auteur sans freiner le développement des outils d'intelligence articifielle. Les fournisseurs de système d'IA et plus généralement de services numériques pourraient ainsi être mieux associés à la lutte contre le piratage.

Proposition : permettre à l'Arcom d'accéder aux outils de reconnaissance de contenus mis en place par les services numériques pour contrôler leur efficacité.

4. **Plus généralement, les actions de régulation numérique ne peuvent plus se passer d'investigations techniques. Le régulateur devrait être autorisé à collecter et traiter des données de façon automatisée dans le cadre de ses missions légales.**

Aujourd'hui, une majorité d'internautes français (53 %) accède à des contenus protégés par l'intermédiaire des réseaux sociaux et des plateformes de partage de vidéo. Les ayants droit ont la possibilité de demander le retrait des contenus diffusés sans leur autorisation, ce qui représente plusieurs millions de contenus par an. Mais, d'une part, signaler ces contenus protégés représente une charge considérable (détection, analyse) qui n'est pas toujours suivie d'effet, et, d'autre part, les utilisateurs utilisent de plus en plus de stratégies de contournement consistant à ne pas diffuser le contenu protégé mais un lien vers une autre plateforme, moins notoire, permettant d'y accéder.

La prolifération de ces liens vers des services illicites par l'intermédiaire des réseaux sociaux revêt tous les aspects d'un risque systémique, contre lequel les grandes plateformes en ligne devraient prendre des mesures dans le cadre du Règlement sur les services numériques. Pour le caractériser, le régulateur devrait être en capacité d'en analyser l'ampleur et les mécanismes de diffusion. Compte tenu de la quantité infinie de contenus concernés, une telle démarche ne saurait se passer du recours, par l'Arcom, à des outils de collecte et de traitement automatisés de données ainsi qu'à la création de comptes sur les réseaux lui permettant de les mettre en œuvre. Des dispositions devraient bien sûr être prévues pour encadrer le recours à de tels outils, notamment pour garantir la protection des données personnelles susceptibles d'être incidemment collectées.

La conduite d'investigations techniques par les autorités de régulation, au service des missions que leur confie la loi, dépasse d'ailleurs largement les enjeux liés au seul droit d'auteur et pourrait trouver des applications sur d'autres champs de régulation, telle que la lutte contre la haine en ligne, la manipulation de l'information ou les enjeux liés à la protection des mineurs, par exemple[69].

Proposition : prévoir la possibilité pour l'Arcom d'utiliser des outils de collecte et de traitement automatisés de données ainsi que de créer des comptes destinés à l'analyse des phénomènes de propagation des contenus illicites, notamment en matière de protection du droit d'auteur et du droit des organisateurs de manifestation sportives.

[69] Des freins à l'accès des régulateurs aux plateformes numériques sont en effet constatés de manière plus globale : l'utilisation des plateformes et des outils qu'elles développent, la création de comptes de test et l'automatisation de certaines actions à des fins d'évaluation, ainsi que la collecte et le traitement automatisé de données disponibles sur les plateformes peuvent s'avérer complexe voire impossible. Or de telles capacités pourraient faciliter la mise en évidence de certains phénomènes, par exemple en amont d'alertes émises dans le cadre du règlement européen sur les services numériques (RSN) ou lorsque la Commission européenne sollicite les régulateurs européens dans le cadre d'enquêtes portant sur les très grandes plateformes.

5. **Enfin, la sensibilisation du public au respect des droits d'auteur, des droits voisins et des droits des organisateurs de manifestations sportives reste indispensable et devrait être renforcée notamment dans l'éventualité où le législateur envisagerait une mise en œuvre *a minima* de la procédure de réponse graduée, voire sa suppression.**

Comme indiqué précédemment, de fortes incertitudes juridiques pèsent sur l'avenir de la réponse graduée dans sa forme actuelle. Le scénario le plus défavorable, aboutissant à la suppression de ce dispositif, ne peut être écarté. Une telle situation entraînerait la disparition d'une mesure pédagogique majeure à l'égard des internautes, qu'il conviendrait de compenser par le déploiement de dispositifs alternatifs de sensibilisation et de prévention.

Relevons, à cet égard, que l'Arcom joue un rôle central dans la promotion de l'offre légale conformément à l'article L. 331-17 du CPI. Cette mission vise à encourager l'accès et la diffusion des contenus protégés par le droit d'auteur au moyen des plateformes et services autorisés. Par des campagnes de sensibilisation, des partenariats avec les acteurs du secteur (comme avec le Centre national du cinéma et de l'image animée – CNC[70] ou avec l'Association pour la protection des programmes sportifs - APPS) et la mise en place d'actions pédagogiques, l'Arcom contribue à orienter le public vers des usages légaux, réduisant ainsi le recours aux pratiques illicites. Dans le cadre de cette mission, l'Arcom recense actuellement 512 sites et services proposant des contenus dématérialisés (films, musiques, retransmissions sportives, podcasts, livres numériques, jeux vidéo, etc.) qu'elle considère comme respectueux du droit d'auteur et des droits voisins[71]. Grâce à ce moteur de recherche, il est ainsi possible de trouver un service conforme aux droits d'auteur ou, plus simplement, de vérifier si un service est référencé par l'Arcom. Chaque mois, 9 000 visiteurs uniques en moyenne consultent le portail de référencement, ce qui constitue l'un des espaces les plus consultés du site de l'Arcom.

Cette promotion de l'offre légale, qui constitue un levier essentiel pour soutenir la création et assurer l'équilibre entre accès aux contenus et respect des droits, doit être activement poursuivie à court et à moyen termes, voire renforcée, avec l'appui de l'ensemble des pouvoirs publics et acteurs privés concernés.

Enfin depuis le mois de septembre 2025, en cas de blocage d'un nom de domaine dans le cadre du dispositif et de l'accord de lutte contre les retransmissions sportives illicites conclu entre les fournisseurs d'accès et l'APPS, l'internaute qui cherche à accéder au service en cause est dirigé, avec le concours de l'Arcom, vers une page expliquant le motif du blocage et l'orientant vers l'offre légale. Sous réserves de considérations opérationnelles et techniques, l'extension de ce dispositif serait également envisageable à d'autres domaines et à d'autres intermédiaires.

Proposition : renforcement des actions de sensibilisation et de promotion de l'offre légale auprès du grand public en collaboration avec les acteurs publics et privés des secteurs concernés.

[70] https://www.arcom.fr/actualites/la-campagne-du-cnc-et-de-larcom-sur-vos-ecrans-antennes-et-reseaux-sociaux-du-30-septembre-au-13-octobre
[71] https://www.arcom.fr/sites-plateformes

3.3 De façon complémentaire à la régulation nationale, le droit pénal et le droit européen pourraient être davantage mobilisés.

1. **En premier lieu, il convient de relever qu'il n'existe pas d'infraction propre aux atteintes aux droits sportifs comme c'est le cas en matière d'atteintes au droit d'auteur ou aux droits voisins.**

En matière de lutte contre le piratage des contenus sportifs, les procédures pénales restent ainsi limitées en l'absence d'infraction propre aux atteintes aux droits sportifs, ce à quoi la proposition de loi relative à l'organisation, à la gestion et au financement du sport professionnel entend remédier. Elle prévoit, à cette fin, l'introduction dans le code du sport d'infractions pénales spécifiques, calquées sur le modèle de la contrefaçon de droits d'auteur et de droits voisins telle que définie dans le CPI. Ces nouvelles infractions auraient un double objectif : d'une part, permettre une répression plus efficace des atteintes aux droits d'exploitation audiovisuelle au-delà des atteintes aux droits voisins détenus par les entreprises de communication audiovisuelle sur leurs programmes[72] et, d'autre part, faciliter l'obtention d'éléments de preuve pour identifier les auteurs de ces atteintes. En effet, la reconnaissance d'une infraction pénale ouvrirait la voie à l'utilisation des mesures d'instruction préalables prévues à l'article 145 du code de procédure civile.

Cette évolution législative s'inscrit dans le sens de la recommandation de la Commission européenne du 4 mai 2023 relative à la lutte contre le piratage en ligne des événements sportifs et autres manifestations diffusées en direct. Cette recommandation invite en effet les États membres à faciliter les investigations et à adopter des mesures concrètes à l'encontre des acteurs impliqués dans la diffusion non autorisée de contenus sportifs à grande échelle, y compris par la participation active aux dispositifs transfrontaliers de répression déjà existants. La lutte contre la criminalité liée à la propriété intellectuelle fait partie en outre des priorités des Etats membres, au titre de l'EMPACT (programme européen contre la criminalité organisée et internationale grave).

Qu'il s'agisse de piratage de contenus culturels ou sportifs, l'effet pédagogique et dissuasif de l'existence d'incriminations relatives à la diffusion illicite de contenus et à la promotion de tels usages et, *a fortiori*, d'une réponse pénale efficace, ne doit pas être négligé.

Proposition : pénaliser l'atteinte aux droits des organisateurs de manifestations sportives, tel que le prévoit la proposition de loi relative à l'organisation, à la gestion et au financement du sport professionnel.

[72] En matière de retransmissions illicites de compétitions sportives, les actions pénales pouvant être engagées le sont sur le fondement du délit de contrefaçon, au titre des droits voisins des entreprises de communication audiovisuelle sur leurs programmes ou des producteurs de vidéogrammes dans l'hypothèse où l'organisateur d'une manifestation sportive produit lui-même les images des matchs de cette manifestation, ce qui est loin d'être systématique. De ce fait, les titulaires de droits d'exploitation audiovisuelle (telles que les ligues ou les fédérations) se trouvent privés de moyens d'action au plan pénal.

2. **Pour mettre en œuvre une lutte efficace contre les services illicites, les outils de la justice pénale[73] se révèlent indispensables dès lors qu'ils ont l'avantage de cibler directement l'éditeur ou l'administrateur du service illicite et de permettre, ce faisant, une fermeture plus durable du site concerné**.

Il importe de préciser que les réflexions ici présentées sont sans préjudice de considérations budgétaires et du strict respect de la définition des orientations de politique pénale et de conduite de l'action publique propres à l'institution judiciaire.

En matière de répression des atteintes aux droits d'auteur et droits voisins, il n'existe pas de juridictions, pôles ou parquets spécialisés (à l'instar du Pôle national de lutte contre la haine en ligne par exemple, ou du Parquet national financier), ni de structures policières spécialisées possédant des attributions précises, tels que l'Office central pour la répression du faux-monnayage (OCRFM), compétent en matière de lutte contre la contrefaçon industrielle (tabac, marques, etc.), ou encore l'Office central de lutte contre le trafic de biens culturels (OCBC), en charge des affaires liées au vol et à la contrebande d'objets culturels. Par conséquent, les affaires de contrefaçon sont traitées par les juridictions saisies selon les règles de procédure pénale classiques, en s'appuyant, le cas échéant et selon la nature et la complexité des faits en cause, sur des brigades ou services spécialisés disposant de compétences spécifiques en matière de cybercriminalité ou de criminalité organisée par exemple[74].

On notera par ailleurs le constat de plus en plus fréquent, relayé notamment par Europol, des liens existants entre la criminalité liée à la violation des droits de propriété intellectuelle et d'autres activités cybercriminelles, y compris en bande organisée : blanchiment d'argent, fraudes aux cryptoactifs, atteintes aux systèmes automatisés de données (STAD)[75]. Plusieurs opérations récentes, impliquant l'intervention d'autorités de divers pays, ont abouti au démantèlement de réseaux IPTV et de *streaming* illégaux, démontrant l'ampleur du phénomène et sa dimension transnationale[76].

Par ailleurs, bien qu'il ne vise pas directement le droit d'auteur ou les droits voisins, le nouveau délit d'administration illicite de plateforme, prévu à l'article 323-3-2 du code

[73] Plusieurs dispositions du code de la propriété intellectuelle visent à sanctionner le délit de contrefaçon, que ce soit en matière de droits d'auteur ou de droits voisins. Les actions pénales initiées par les ayants droit portent généralement sur la reproduction illégale et la communication non autorisée d'œuvres (articles L. 335-2, L. 335-4, L. 335-3 du CPI). Par ailleurs, d'autres infractions peuvent également être poursuivies, telles que la violation des mesures techniques de protection (articles L. 335-3-1 et L. 335-4-1 du CPI), la mise à disposition de logiciels manifestement destinés à faciliter la contrefaçon (article L. 335-2-1 du CPI), ou encore la captation illicite en salle de cinéma (article L. 335-3, alinéa 3, du CPI). En outre, la loi pour la confiance dans l'économie numérique (LCEN) n°2004-575 du 21 juin 2004, notamment son article 6 et les suivants, établit la responsabilité pénale d'un hébergeur en cas de complicité de contrefaçon, lorsqu'il ne supprime pas des œuvres contrefaites après notification des ayants droit.

[74] Voir en ce sens : circulaire relative à l'articulation des pouvoirs de l'Arcom et de l'autorité judiciaire et au traitement pénal du téléchargement illicite, CRIM-2024-2/G1-06/02/2024, février 2024, page 9 (https://www.justice.gouv.fr/documentation/bulletin-officiel/circulaire-relative-larticulation-pouvoirs-larcom-lautorite-judiciaire-au)

[75] *Uncovering the ecosystem of intellectual property crime*, Rapport d'analyse stratégique conjoint de l'EUIPO et d'Europol produit dans le cadre de l'EMPACT, Octobre 2024.Etude publiée en 2024 par Europol et l'EUIPO (Office de l'Union européenne pour la propriété intellectuelle) ; *The changing DNA of serious and organised crime*, Europol, 2025, https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime#downloads

[76] https://www.clubic.com/actualite-578070-milliard-de-visites-en-un-an-le-mastodonte-du-streaming-pirate-ferme-en-egypte.html
https://www.bfmtv.com/tech/actualites/streaming/plus-de-100-000-films-et-series-illegaux-un-vaste-reseau-d-iptv-demantele-par-les-autorites_AV-202508110374.html
https://www.lesnumeriques.com/societe-numerique/900-000-pirates-vont-etre-identifies-l-italie-frappe-un-coup-d-envergure-contre-l-iptv-illegale-n243318.html

pénal, complète utilement l'arsenal pénal de lutte contre le piratage, en ce qu'il cible tout administrateur d'un service de plateforme en ligne qui permet sciemment la diffusion ou la vente de contenus manifestement illicites, en restreignant l'accès à la plateforme aux utilisateurs ayant recours à des techniques d'anonymisation des connexions, ou en ne respectant pas les obligations d'identification imposées par la LCEN ou le RSN. Est également incriminé le fait de proposer des prestations d'intermédiation ou de séquestre dont l'objet unique ou principal est de mettre en œuvre, dissimuler ou faciliter les opérations illicites précitées. Instaurant une responsabilité accrue de ces services, qui jusqu'alors pouvaient invoquer le bénéfice d'un régime atténué de responsabilité lié au statut d'hébergeur, la loi entend cibler les plateformes qui facilitent sciemment les comportements illicites et amplifier l'effet dissuasif au regard des peines significatives encourues, notamment en bande organisée.

Combinée aux dispositions existantes, cette infraction devrait contribuer à une lutte renforcée contre les atteintes aux droits de propriété intellectuelle en dépassant les limites liées aux procédures de notification aux fins de retrait des contenus illicites et en incriminant l'organisation et la gestion des services qui facilitent les pratiques manifestement illicites.

Des échanges fructueux sont déjà mis en place entre les services de l'Arcom et les autorités judiciaires, depuis plusieurs années, qu'il s'agisse de réunions régulières avec les parquets généraux et les parquets concernant la mise en œuvre de la réponse graduée et, plus récemment, avec le Tribunal judiciaire de Paris dans le cadre notamment des dispositifs d'injonctions dynamiques. Plus largement, forte de sa connaissance de l'écosystème illicite et des spécificités techniques des services dédiés au piratage, l'Arcom entend poursuivre toute forme de coopération avec les services judiciaires compétents.

Proposition : poursuivre et intensifier la coopération avec les autorités judiciaires compétentes en matière de lutte contre le piratage des contenus culturels et sportifs.

3. **Pour aller plus loin, le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité[77], communément dénommé « Loi Cyberrésilience », présente un intérêt notable** en matière de facilitation de l'accès aux données d'enregistrement des noms de domaine auprès des offices et bureaux d'enregistrement de noms de domaine, conformément aux dispositions de son article 22.

Ainsi, l'intégration d'un amendement au sein de ce texte, destiné à simplifier et sécuriser les procédures permettant aux agents habilités en application de l'article L. 331-2 du CPI et aux auxiliaires de justice d'obtenir rapidement et efficacement ces informations, essentielles pour l'identification des responsables en cas d'activités illicites en ligne, contribuerait à renforcer la lutte contre le piratage et les infractions liées aux noms de domaine.

Proposition (notamment par amendement au projet de loi relatif à la résilience des entités essentielles face aux cybermenaces) : autoriser les agents assermentés des ayants droit à obtenir les données relatives aux noms de domaine auprès des offices et bureaux d'enregistrement de noms de domaine.

[77] https://www.assemblee-nationale.fr/dyn/17/dossiers/DLR5L17N50731

4. Si le RSN s'applique sans préjudice des lois spéciales, comme celles relatives à la protection du droit d'auteur, il a vocation à renforcer la lutte contre la diffusion des contenus illicites et préjudiciables sur internet et peut à ce titre être mobilisé en renfort au service de la lutte contre le piratage.

Le Règlement sur les services numériques (RSN) a pour objectif de garantir le respect des droits fondamentaux des utilisateurs en ligne ainsi que leur sécurité. Il vient compléter et renforcer le cadre juridique existant, hérité notamment de la directive sur le commerce électronique de 2000. À cette fin, il impose des obligations accrues de transparence à l'ensemble des fournisseurs de services intermédiaires et introduit de nouvelles responsabilités à l'égard des plateformes en ligne, en particulier en matière de modération des contenus illicites. Par ailleurs, des exigences spécifiques en matière de prévention des risques systémiques sont désormais applicables aux très grandes plateformes en ligne (VLOP) et aux très grands moteurs de recherche (VLOSE). Le texte prévoit également une implication élargie de la société civile, notamment à travers la reconnaissance des signaleurs de confiance.

Dans ce cadre, les personnes morales (associations, entités, organisations professionnelles, etc.) reconnues pour leur expertise et leurs compétences en matière de signalement de contenus illicites en ligne peuvent demander au « coordinateur pour les services numériques de l'État membre » (en France, l'Arcom) le statut de « signaleur de confiance ».

De nombreux ayants droit ont manifesté leur intérêt pour ce régime : ils y voient notamment une opportunité pour obtenir un traitement plus rapide des notifications soumises aux plateformes. À cet égard, le RSN mentionne (article 22 paragraphe 1) que les signalements soumis par les futurs signaleurs de confiance devront être traités dans les « *meilleurs délais* ». Les ayants droit s'attendent ainsi à ce que leurs notifications donnent lieu à des actions de modération urgentes des plateformes, comme ces dernières y sont invitées par les considérants 18 et 19 ainsi que par l'article 5 de la Recommandation 2023/1018 de la Commission du 4 mai 2023 sur la lutte contre le piratage en ligne des manifestations sportives et autres événements en direct.

À ce jour, s'agissant de la lutte contre le piratage, seule l'ALPA a été désignée comme signaleur de confiance par l'Arcom. D'autres candidatures, émanant d'ayants droit « individuels » (type diffuseur ou ligue professionnel sportive, ou encore prestataire de lutte anti-piratage) ont été reçues.

La question du nombre de signaleurs est soulevée dans le considérant 61 du RSN qui souligne que l'octroi du statut à un trop grand nombre d'entités risquerait de diminuer la valeur ajoutée du mécanisme. Par ailleurs, le même considérant encourage les membres d'associations professionnelles à se regrouper au sein de fédérations, sans pour autant exclure la possibilité qu'ils candidatent au statut à titre individuel.

Plusieurs ayants droit font valoir qu'il y aurait lieu de distinguer, d'une part, les ayants droit, nécessairement en nombre réduit, assurant de façon autonome et de longue date la défense de leurs droits en ligne et disposant en conséquence d'équipes en propre, formées à la gestion des signalements, et, d'autre part, les ayants droit désireux de s'engager dans la protection de leurs droits en ligne sans disposer d'équipes dédiées. Dans cette approche, les ayants droit experts pourraient disposer du statut à titre individuel ; les autres seraient invités à se fédérer. La Commission européenne semble confirmer cette lecture dans le cadre des recommandations du 19 mars 2024 sur la lutte contre la contrefaçon et du 4 mai 2023 sur les industries culturelles et créatives.

L'Arcom a décidé de surseoir à statuer en attendant des lignes directrices et des règles harmonisées de la Commission européenne pour ce type d'acteurs. Elle envisage parallèlement un mécanisme offrant la possibilité aux ayants droit de se fédérer et de préparer des signalements de contenus qui seront ensuite envoyés de manière automatisée aux plateformes concernées par une association professionnelle ou une fédération ayant obtenu le statut de signaleur de confiance. Des lignes directrices de la Commission sont attendues pour clarifier cette question.

En complément de ce dispositif, il faut souligner que les ayants droit disposent de **la possibilité de solliciter l'Autorité en tant que régulateur des services numériques pour transmettre des plaintes** à l'encontre de services non diligents.

S'agissant des très grandes plateformes en ligne et des très grands moteurs de recherche, les éléments relevés par les ayants droit (délai de retrait des contenus signalés, réapparition systématique des contenus contrevenants, etc.) pourraient également permettre à l'Arcom de documenter les travaux de la Commission sur l'analyse des risques systémiques. Les acteurs numériques concernés devraient alors prendre des mesures pour les atténuer.

Proposition : accompagner les ayants droit culturels et sportifs dans la prise en main des outils nouvellement à leur disposition dans le cadre du Règlement sur les services numériques.

5. **Toutefois, le cadre ainsi prévu par le RSN est jugé encore insuffisant par les titulaires de droits, notamment s'agissant de l'exécution des injonctions par certains intermédiaires techniques et de la notification aux hébergeurs et aux réseaux de diffusion de contenu (CDN).**

Les injonctions de blocage prévues à l'article 9 du RSN présentent une complémentarité intéressante pour le système national de lutte contre le piratage.

L'article 9 du RSN définit un cadre spécifique pour l'envoi des injonctions judiciaires ou administratives adressées aux intermédiaires numériques. Ces injonctions visent à leur demander d'agir contre des contenus illicites diffusés sur leurs services. Toutefois, cet article n'instaure pas un nouveau régime juridique autonome : les injonctions doivent être émises en application du droit national de l'État concerné (par exemple, le droit français).

Le RSN introduit cependant deux particularités à la charge des fournisseurs de services :
- une obligation de réception et de réponse à l'injonction reçue (accusé de réception et indication des suites données) ;
- une absence d'obligation d'exécution automatique : l'exécution effective de l'injonction reste de la responsabilité des autorités nationales compétentes, conformément à leur propre cadre juridique.

Enfin, le régulateur national du numérique (en France, l'Arcom) doit être informé par les fournisseurs de services de la réception des injonctions et des actions mises en œuvre en réponse à celles-ci.

Dans ce contexte, le dispositif européen constitue un complément utile aux mesures françaises de lutte contre le piratage, en particulier lorsque certains intermédiaires numériques tardent ou refusent de se conformer à une injonction de blocage.

Sur le plan opérationnel, le droit européen leur impose en effet l'obligation d'informer le régulateur national des actions entreprises à la suite de la réception d'une telle injonction, ce qui constitue une incitation supplémentaire pour appliquer les mesures de blocages émises par le juge ou par l'Arcom.

Il ne leur impose pas, en revanche, de les exécuter et n'encadre pas les délais d'exécution.

Or d'après les retours des ayants droit, **la fixation d'un délai maximum sous lequel les intermédiaires (compris comme tout acteur susceptible de remédier à une atteinte aux droits des titulaires de droits) doivent donner une réponse aux notifications dont ils sont destinataires est indispensable pour assurer leur protection effective**, en particulier lorsqu'il s'agit d'une transmission en direct de contenus illicites. A cet égard, si le RSN prévoit aujourd'hui que les hébergeurs doivent agir « promptement », son considérant 52 indiquant que « *les fournisseurs de services d'hébergement devraient réagir rapidement aux notifications, notamment en tenant compte du type de contenu illicite notifié et de l'urgence d'agir* », aucun délai correspondant n'a cependant été précisé. Or, il apparait que les notifications ne sont pas traitées de façon diligente par les hébergeurs. En effet, une étude réalisée au niveau européen par Grant Thornton[78] montre que :

- 81 % des notifications adressées par les titulaires de droits en 2024 n'ont pas entraîné la suspension par l'hébergeur de la retransmission illégale ;
- Seules 2,7 % de ces notifications ont fait l'objet d'une action dans les 30 minutes.

C'est pourquoi, les ayants droit demandent qu'une législation au niveau européen vienne imposer aux hébergeurs de traiter immédiatement les notifications qui leur sont adressées lorsqu'elles portent sur des contenus diffusés en direct. Des demandes similaires adressées par les ayants droits visent également les réseaux de diffusion de contenu (CDN, voir ci-dessous), mentionnés au considérant 28 du RSN.

Les réseaux de diffusion de contenu (CDN – *Content Delivery Networks*)

Les réseaux de diffusion de contenu (CDN – *Content Delivery Networks*) et les services de proxy inverse interviennent en amont des hébergeurs, dans la chaîne technique de transmission des contenus sur internet. Ils jouent un rôle d'intermédiaires en assurant la distribution rapide et efficace des contenus, notamment grâce à la mise en cache des données au plus près des utilisateurs finaux. Plus précisément :

- ces infrastructures ajoutent de l'opacité au trafic des données sur internet, ce qui a notamment pour effet de masquer les adresses IP des serveurs d'origine des contenus (souvent ceux des hébergeurs) ;
- elles contribuent à protéger l'infrastructure source contre les attaques, rendant l'identification des acteurs réellement responsables plus complexe ;
- elles contribuent également à gêner les mesures de blocage IP car une même adresse IP appartenant à un CDN peut être simultanément utilisée par de très nombreux services, notamment licites.

D'un point de vue juridique :

[78] Grant Thornton, « The European Commission Recommendation on combatting online piracy of live events has limited impact after 17 months », février 2025.

- les CDN et les services de proxy inverse ne sont généralement pas directement visés dans les procédures judiciaires liées au retrait ou au blocage de contenus illicites [79] ;
- il est difficile de démontrer leur responsabilité directe, car ils ne créent ni ne stockent durablement les contenus ;
- néanmoins, leur rôle dans la diffusion des contenus litigieux peut être stratégique, et il est important de ne pas les exclure de l'analyse globale dans la lutte contre le piratage.

Propositions : étudier les conditions d'une application de l'article 9 du RSN pour améliorer la prise en compte par les intermédiaires techniques des injonctions ; inciter les CDN et les fournisseurs de services d'hébergement, en s'appuyant sur leur obligation de connaitre leurs clients, à interrompre sur le fondement de leurs conditions générales le service qui serait signalé comme illégal à plusieurs reprises par les titulaires des droits ou les autorités publiques et à partager avec eux les informations dont ils disposent en ce qui concerne l'identification des sources non autorisées, y compris, le cas échéant, l'adresse IP d'origine des serveurs ; contribuer à une réflexion à l'échelle européenne pour permettre une meilleure prise en compte des injonctions adressées aux intermédiaires et envisager de prévoir des délais contraints, en particulier s'agissant des contenus diffusés en direct.

[79] Seules deux décisions à l'encontre la société Cloudflare inc ont été portée à la connaissance de l'Arcom et visent notamment le service de CDN fourni par cet intermédiaire (Tribunal judiciaire de Paris, Canal Plus c. Cloudflare 28 mars et 18 juin 2025).

Conclusion

Eu égard à l'extrême diversité des atteintes aux droits d'auteur et aux droits voisins dans les pratiques en ligne des internautes, il apparaît urgent de renforcer l'efficacité des outils de lutte contre le piratage dans les secteurs culturel et sportif. Si les mesures instituées jusqu'à présent ont permis d'obtenir des résultats particulièrement satisfaisants, celles-ci se heurtent désormais aux capacités d'adaptation des sites contrefaisants qui ont adopté des stratégies de contournement rapides en réponse aux mesures de blocage édictées.

À cette fin, des évolutions, d'ordre « paramétrique », sont à envisager pour faciliter les mesures susceptibles d'être prises par l'Autorité. Celles-ci viseraient, pour l'essentiel, à simplifier la saisine de l'Autorité, en particulier s'agissant de la mise en œuvre des demandes de blocage ou de déréférencement. Plusieurs recommandations en ce sens sont présentées sous forme d'amendements à la proposition de loi visant à conforter la filière cinématographique en France ainsi qu'à la proposition de loi relative à l'organisation, à la gestion et au financement du sport professionnel.

Au-delà de ces pistes, une approche plus réformatrice peut être imaginée en vue de répondre de manière globale à la résistance des sites frauduleux. Selon l'adage latin *si vis pacem, para bellum* (« Si tu veux la paix, prépare la guerre » en français), il est essentiel de concevoir un cadre de régulation plus flexible, capable d'anticiper les enjeux à venir, de s'adapter aux évolutions de l'écosystème illicite et de construire en amont des réponses efficaces, plutôt que de réagir au fil de l'eau aux évolutions inévitables des pratiques contrefaisantes. Dans cette perspective, le renforcement du rôle de l'Arcom en tant que cheffe de file de la lutte contre le piratage constitue une orientation ambitieuse. Elle permettrait de recentrer l'action de l'Autorité sur les étapes stratégiques de cette lutte, en définissant un cadre d'intervention en amont et en assurant, en aval, le contrôle de son respect. Ce positionnement favoriserait une responsabilisation accrue des acteurs impliqués sur les maillons intermédiaires de la chaîne, tout en s'appuyant sur des procédures simplifiées.

Le recours au droit souple apparaît aussi comme une piste prometteuse pour faciliter la mise en place de ce modèle. En offrant un cadre moins contraignant que la réglementation traditionnelle, le droit souple se révèle en effet intéressant pour soutenir une régulation pragmatique, capable d'impliquer efficacement les différents acteurs, tout en garantissant un équilibre entre encadrement et souplesse. Cette approche pourrait contribuer à renforcer la cohérence et l'efficacité de l'action de l'Autorité dans la lutte contre les atteintes aux droits, en complétant les dispositifs juridiques existants par des outils plus modulables.

Par ailleurs, qu'elles relèvent d'ajustements ciblés ou de transformations plus systémiques, l'ensemble des avancées présentées impose une adaptation du cadre juridique existant. Celui-ci pourrait utilement s'inspirer de pratiques mises en œuvre dans d'autres États européens, ou encore des orientations issues du droit de l'Union européenne. En tout état de cause, le dispositif retenu, ou les réformes qui en découleront, devra être conçu dans le respect des exigences constitutionnelles, garantissant ainsi sa légitimité juridique et sa pérennité.

Enfin, il importe de s'assurer que le cadre juridique facilite la coopération et la transmission d'informations entre l'Autorité et l'institution judiciaire, qu'il s'agisse de la lutte directe contre les services illicites, au moyen de procédures pénales, ou des mécanismes d'injonctions de blocage dynamiques combinant l'action judiciaire civile et l'intervention administrative.

La mise en œuvre de ces évolutions doit impérativement s'inscrire dans le respect de plusieurs exigences fondamentales.

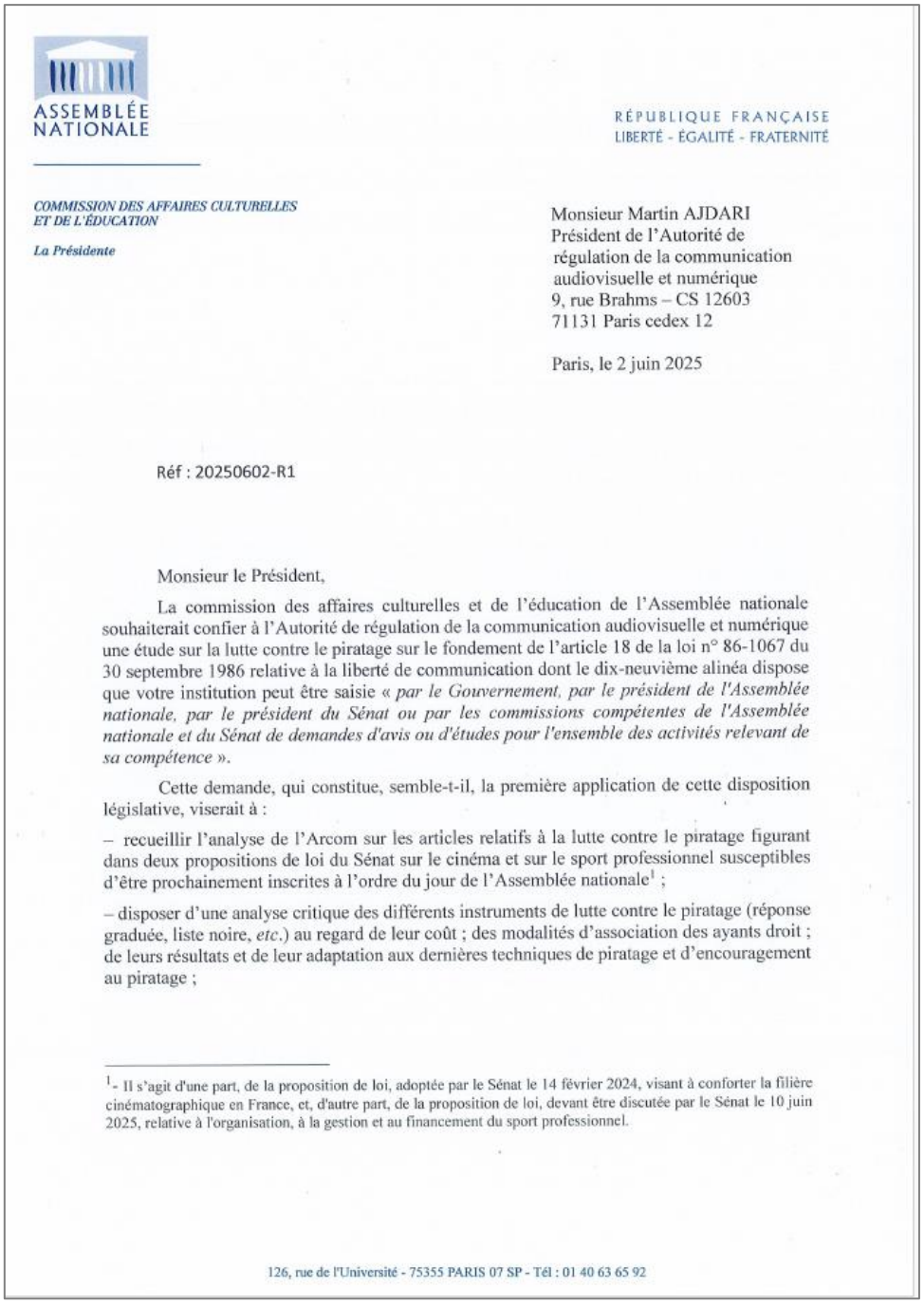
L'équilibre entre protection des droits et respect des libertés fondamentales constitue la première de ces exigences. Toute mesure de blocage porte atteinte à la liberté de communication en ligne, qui englobe la liberté d'accéder à des services en ligne. Le Conseil constitutionnel et le Conseil d'État veillent à ce que cet équilibre soit préservé, dans le respect du droit européen. L'introduction d'un système automatisé de blocage en temps réel, si elle répond à un impératif d'efficacité, ne doit pas conduire à une automatisation intégrale qui pourrait être censurée. Le maintien d'un contrôle humain par les agents assermentés de l'Arcom, la limitation temporelle stricte des mesures à la durée de l'événement sportif et la possibilité de recours constituent autant de garanties indispensables.

La proportionnalité des mesures constitue la deuxième exigence. Les incidents de surblocage qui ont pu survenir dans certains pays rappellent les risques inhérents aux dispositifs de blocage, particulièrement lorsqu'ils reposent sur le blocage d'adresses IP pouvant être utilisées par de multiples services. La responsabilité de l'Arcom en cas de surblocage impose une vigilance particulière dans la définition des critères techniques d'identification des services illicites et dans le contrôle de leur mise en œuvre par les titulaires de droits, en complément du cadre défini dans l'ordonnance judiciaire initiale.

L'agilité et la réactivité représentent la troisième condition de succès. Dans un environnement numérique en constante évolution, où les services illicites s'adaptent en permanence aux mesures prises, la capacité de réaction rapide des pouvoirs publics est déterminante. L'automatisation partielle des procédures, la simplification des conditions de saisine de l'Arcom, l'harmonisation des dispositifs de blocage répondent à cet impératif. Cette agilité ne doit toutefois pas se faire au détriment de la sécurité juridique : des garde-fous clairs doivent encadrer l'action administrative pour prévenir toute atteinte disproportionnée aux droits et libertés en présence.

Annexes

1. Lettre de mission



ASSEMBLÉE NATIONALE

RÉPUBLIQUE FRANÇAISE
LIBERTÉ - ÉGALITÉ - FRATERNITÉ

COMMISSION DES AFFAIRES CULTURELLES ET DE L'ÉDUCATION

La Présidente

Monsieur Martin AJDARI
Président de l'Autorité de régulation de la communication audiovisuelle et numérique
9, rue Brahms – CS 12603
71131 Paris cedex 12

Paris, le 2 juin 2025

Réf : 20250602-R1

Monsieur le Président,

La commission des affaires culturelles et de l'éducation de l'Assemblée nationale souhaiterait confier à l'Autorité de régulation de la communication audiovisuelle et numérique une étude sur la lutte contre le piratage sur le fondement de l'article 18 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication dont le dix-neuvième alinéa dispose que votre institution peut être saisie « *par le Gouvernement, par le président de l'Assemblée nationale, par le président du Sénat ou par les commissions compétentes de l'Assemblée nationale et du Sénat de demandes d'avis ou d'études pour l'ensemble des activités relevant de sa compétence* ».

Cette demande, qui constitue, semble-t-il, la première application de cette disposition législative, viserait à :

– recueillir l'analyse de l'Arcom sur les articles relatifs à la lutte contre le piratage figurant dans deux propositions de loi du Sénat sur le cinéma et sur le sport professionnel susceptibles d'être prochainement inscrites à l'ordre du jour de l'Assemblée nationale[1] ;

– disposer d'une analyse critique des différents instruments de lutte contre le piratage (réponse graduée, liste noire, *etc.*) au regard de leur coût ; des modalités d'association des ayants droit ; de leurs résultats et de leur adaptation aux dernières techniques de piratage et d'encouragement au piratage ;

[1]- Il s'agit d'une part, de la proposition de loi, adoptée par le Sénat le 14 février 2024, visant à conforter la filière cinématographique en France, et, d'autre part, de la proposition de loi, devant être discutée par le Sénat le 10 juin 2025, relative à l'organisation, à la gestion et au financement du sport professionnel.

126, rue de l'Université - 75355 PARIS 07 SP - Tél : 01 40 63 65 92

– connaître votre appréciation sur l'incidence du développement des systèmes de nom de domaine alternatifs et des réseaux privés virtuels sur l'effectivité de l'action de l'Arcom en matière de lutte contre le piratage ;

– recueillir votre appréciation sur les conditions de mobilisation des différentes possibilités ouvertes par le droit européen en matière de lutte contre le piratage.

Les conclusions de cette étude pourraient être portées à la connaissance de la commission au début du mois d'octobre 2025 dans le prolongement de la présentation du rapport d'activité de votre institution également prévu par l'article 18 de la loi précitée.

Je vous remercie pour le concours que l'Arcom apporterait ainsi aux travaux du Parlement et vous prie de croire, Monsieur le Président, en l'expression de ma considération distinguée.

Fatiha Keloua Hachi
Présidente de la Commission des Affaires culturelles et de l'Éducation
Députée de la Seine-Saint-Denis

2. Textes juridiques en vigueur

a) Mission générale de protection des œuvres sur internet

Article L. 331-12 du code de la propriété intellectuelle

L'Autorité de régulation de la communication audiovisuelle et numérique assure :

1° Une mission de protection des œuvres et des objets auxquels sont attachés un droit d'auteur, un droit voisin ou un droit d'exploitation audiovisuelle mentionné à l'article L. 333-10 du code du sport, à l'égard des atteintes à ces droits commises sur les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne.

Elle mène des actions de sensibilisation et de prévention auprès de tous les publics, notamment auprès des publics scolaires et universitaires ;

2° Une mission d'encouragement au développement de l'offre légale et d'observation de l'utilisation licite et illicite des œuvres et des objets protégés par un droit d'auteur, un droit voisin ou un droit d'exploitation audiovisuelle mentionné au même article L. 333-10 sur les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne ;

3° Une mission de régulation et de veille dans le domaine des mesures techniques de protection et d'identification des œuvres et des objets protégés.

Au titre de ces missions, l'autorité prend toute mesure, notamment par l'adoption de recommandations, de guides de bonnes pratiques, de modèles et de clauses types ainsi que de codes de conduite visant à favoriser, d'une part, l'information du public sur l'existence des moyens de sécurisation mentionnés à l'article L. 331-20 du présent code et, d'autre part, la signature d'accords volontaires susceptibles de contribuer à remédier aux atteintes au droit d'auteur et aux droits voisins ou aux droits d'exploitation audiovisuelle mentionnés à l'article L. 333-10 du code du sport sur les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne.

L'autorité évalue l'efficacité des accords qui ont été conclus. A cette fin, elle peut solliciter des parties toutes informations utiles relatives à leur mise en œuvre. Elle peut formuler des recommandations pour promouvoir la conclusion de tels accords et des propositions pour pallier les éventuelles difficultés rencontrées dans leur exécution ou au stade de leur conclusion.

b) Lutte contre les sites miroirs

Article L. 336-2 du code de la propriété intellectuelle

En présence d'une atteinte à un droit d'auteur ou à un droit voisin occasionnée par le contenu d'un service de communication au public en ligne, le président du tribunal judiciaire statuant selon la procédure accélérée au fond peut ordonner à la demande des titulaires de droits sur les œuvres et objets protégés, de leurs ayants droit, des organismes de gestion collective régis par le titre II du livre III ou des organismes de défense professionnelle visés à l'article L. 331-1, toutes mesures propres à prévenir ou à faire cesser une telle atteinte à un droit d'auteur ou un droit voisin, à l'encontre de

toute personne susceptible de contribuer à y remédier. La demande peut également être effectuée par le Centre national du cinéma et de l'image animée.

Article L. 331-27 du code de la propriété intellectuelle

I.- Lorsqu'une décision judiciaire passée en force de chose jugée a ordonné toute mesure propre à empêcher l'accès à un service de communication au public en ligne en application de l'article L. 336-2, l'Autorité de régulation de la communication audiovisuelle et numérique, saisie par un titulaire de droits partie à la décision judiciaire, peut demander à toute personne visée par cette décision, pour une durée ne pouvant excéder celle restant à courir pour les mesures ordonnées par le juge, d'empêcher l'accès à tout service de communication au public en ligne reprenant en totalité ou de manière substantielle le contenu du service mentionné par ladite décision. Pour l'application du présent I, l'Autorité de régulation de la communication audiovisuelle et numérique communique précisément les données d'identification du service en cause, selon les modalités qu'elle définit.

Dans les mêmes conditions, l'autorité peut également demander à tout exploitant de moteur de recherche, annuaire ou autre service de référencement de faire cesser le référencement des adresses électroniques donnant accès à ces services de communication au public en ligne.

Pour faciliter l'exécution des décisions judiciaires mentionnées à l'article L. 336-2, l'autorité adopte des modèles d'accord, qu'elle invite les ayants droit et toute personne susceptible de contribuer à remédier aux atteintes aux droits d'auteur et droits voisins en ligne à conclure. L'accord détermine notamment les conditions d'information réciproque des parties sur l'existence de tout service de communication au public en ligne reprenant en totalité ou de manière substantielle le contenu du service visé par la décision. Il engage toute personne susceptible de contribuer à remédier aux atteintes aux droits d'auteur et droits voisins en ligne, partie à l'accord, à prendre les mesures prévues par la décision judiciaire.

II.- En cas de difficulté relative à l'application des premiers ou deuxième alinéa du I, l'Autorité de régulation de la communication audiovisuelle et numérique peut demander aux services de se justifier. Sans préjudice d'une telle demande, l'autorité judiciaire peut être saisie, en référé ou sur requête, pour ordonner toute mesure destinée à faire cesser l'accès à ces services. Cette saisine s'effectue sans préjudice de la saisine prévue à l'article L. 336-2.

Article R. 331-20 du code de la propriété intellectuelle

I.- La saisine adressée à l'Autorité de régulation de la communication audiovisuelle et numérique par un titulaire de droits dans les conditions prévues au I de l'article L. 331-27 a lieu par lettre recommandée avec demande d'avis de réception ou par tout autre moyen permettant d'attester de la date de réception et de l'identité du destinataire, y compris par voie électronique. Elle comporte :

1° Une copie de la décision judiciaire passée en force de chose jugée, à laquelle le titulaire de droits est partie, ordonnant toutes mesures propres à prévenir ou à faire cesser une atteinte à un droit d'auteur ou un droit voisin, à l'encontre de toute personne susceptible de contribuer à y remédier en application de l'article L. 336-2 ;

2° Les données d'identification du service de communication au public en ligne reprenant en totalité ou de manière substantielle le contenu du service mentionné par la décision mentionnée au 1° ;

3° Une déclaration sur l'honneur selon laquelle l'auteur de la saisine est titulaire de droits ou a qualité pour agir au nom du titulaire de droits sur une œuvre ou un objet protégé concernés par la reprise mentionnée au 2° et, le cas échéant, tout document justifiant des droits.

II.- Dès réception du dossier complet, l'autorité en accuse réception par voie électronique.

Elle peut préalablement demander au titulaire de droits d'apporter, dans un délai qu'elle fixe, les éléments nécessaires.

L'autorité ne donne pas suite à une saisine non complétée conformément aux dispositions du I.

c) Lutte contre les retransmissions sportives illicites

Article L. 333-10 du code du sport

I.- Lorsqu'ont été constatées des atteintes graves et répétées au droit d'exploitation audiovisuelle prévu à l'article L. 333-1 du présent code, au droit voisin d'une entreprise de communication audiovisuelle prévu à l'article L. 216-1 du code de la propriété intellectuelle, dès lors que le programme concerné est constitué d'une manifestation ou d'une compétition sportive, ou à un droit acquis à titre exclusif par contrat ou accord d'exploitation audiovisuelle d'une compétition ou manifestation sportive, occasionnées par le contenu d'un service de communication au public en ligne dont l'objectif principal ou l'un des objectifs principaux est la diffusion sans autorisation de compétitions ou manifestations sportives, et afin de prévenir ou de remédier à une nouvelle atteinte grave et irrémédiable à ces mêmes droits, le titulaire de ce droit peut saisir le président du tribunal judiciaire, statuant selon la procédure accélérée au fond ou en référé, aux fins d'obtenir toutes mesures proportionnées propres à prévenir ou à faire cesser cette atteinte, à l'encontre de toute personne susceptible de contribuer à y remédier.

Peuvent également à ce titre saisir le président du tribunal judiciaire, dans les conditions prévues au premier alinéa du présent I :
1° Une ligue sportive professionnelle, dans le cas où elle commercialise les droits d'exploitation audiovisuelle de compétitions sportives professionnelles, susceptibles de faire l'objet ou faisant l'objet de l'atteinte mentionnée au même premier alinéa ;
2° L'entreprise de communication audiovisuelle, dans le cas où elle a acquis un droit à titre exclusif, par contrat ou accord d'exploitation audiovisuelle, sur une compétition ou manifestation sportive, que cette compétition ou manifestation sportive soit organisée sur le territoire français ou à l'étranger, dès lors que ce droit est susceptible de faire l'objet ou fait l'objet de l'atteinte mentionnée audit premier alinéa.

II.- Le président du tribunal judiciaire peut notamment ordonner, au besoin sous astreinte, la mise en œuvre, pour chacune des journées figurant au calendrier officiel de la compétition ou de la manifestation sportive, dans la limite d'une durée de douze mois, de toutes mesures proportionnées, telles que des mesures de blocage ou de retrait ou de déréférencement, propres à empêcher l'accès à partir du territoire français à tout service de communication au public en ligne, identifié ou qui n'a pas été identifié à la date de ladite ordonnance, diffusant illicitement la compétition ou manifestation sportive ou dont l'objectif principal ou l'un des objectifs principaux est la diffusion sans autorisation de la compétition ou manifestation sportive. Les mesures ordonnées par le président du tribunal judiciaire prennent fin, pour chacune des journées figurant au

calendrier officiel de la compétition ou de la manifestation sportive, à l'issue de la diffusion autorisée par le titulaire du droit d'exploitation de cette compétition ou de cette manifestation.

Le président du tribunal judiciaire peut ordonner toute mesure de publicité de la décision, notamment son affichage ou sa publication intégrale ou par extraits dans les journaux ou sur les services de communication au public en ligne qu'il désigne, selon les modalités qu'il précise.

III.- Pour la mise en œuvre des mesures ordonnées sur le fondement du II portant sur un service de communication au public en ligne non encore identifié à la date de l'ordonnance, et pendant toute la durée de ces mesures restant à courir, le titulaire de droits concerné communique à l'Autorité de régulation de la communication audiovisuelle et numérique les données d'identification du service en cause, selon les modalités définies par l'autorité.

Lorsque les agents habilités et assermentés de l'autorité mentionnés à l'article L. 331-14 du code de la propriété intellectuelle constatent que le service mentionné au premier alinéa du présent III diffuse illicitement la compétition ou la manifestation sportive ou a pour objectif principal ou parmi ses objectifs principaux une telle diffusion, le président de l'autorité ou, en cas d'empêchement, tout membre du collège de l'autorité désigné par lui notifie les données d'identification de ce service aux personnes mentionnées par l'ordonnance prévue au II afin qu'elles prennent les mesures ordonnées à l'égard de ce service pendant toute la durée de ces mesures restant à courir.

En cas de difficulté relative à l'application du deuxième alinéa du présent III, l'Autorité de régulation de la communication audiovisuelle et numérique peut demander aux services de se justifier. Sans préjudice d'une telle demande, le président du tribunal judiciaire peut être saisi, en référé ou sur requête, pour ordonner toute mesure propre à faire cesser l'accès à ces services.

IV.- L'Autorité de régulation de la communication audiovisuelle et numérique adopte des modèles d'accord que les titulaires de droits mentionnés au I, la ligue professionnelle, l'entreprise de communication audiovisuelle ayant acquis un droit à titre exclusif et toute personne susceptible de contribuer à remédier aux atteintes mentionnées au même I sont invités à conclure. L'accord conclu entre les parties précise les mesures qu'elles s'engagent à prendre pour faire cesser d'éventuelles violations de l'exclusivité du droit d'exploitation audiovisuelle de la manifestation ou compétition sportive et la répartition du coût des mesures ordonnées sur le fondement du II.

Article L. 333-11 du code du sport

Les agents habilités et assermentés de l'Autorité de régulation de la communication audiovisuelle et numérique peuvent constater les faits susceptibles de constituer des atteintes aux droits mentionnés à l'article L. 333-10.
Dans ce cadre, ces agents peuvent, sans en être tenus pénalement responsables :

1° Participer, sous un pseudonyme, à des échanges électroniques susceptibles de se rapporter aux atteintes aux droits mentionnés au même article L. 333-10 ;

2° Reproduire des manifestations ou des compétitions sportives diffusées sur les services de communication au public en ligne ;

3° Extraire, acquérir ou conserver par ce moyen des éléments de preuve sur ces services aux fins de la caractérisation des faits susceptibles de constituer des atteintes aux droits ;

4° Acquérir et étudier les matériels et logiciels propres à faciliter la commission des atteintes aux droits mentionnés audit article L. 333-10.

A peine de nullité, ces actes ne peuvent avoir pour effet d'inciter autrui à commettre une infraction.

Les agents consignent les informations ainsi recueillies dans un procès-verbal, qui rend compte des conditions dans lesquelles les facultés reconnues aux 1° à 4° du présent article ont été employées.

d) Caractérisation des atteintes aux droits - liste des services contrefaisants

Article L. 331-25 du code de la propriété intellectuelle

I.- Au titre de la mission mentionnée au 1° de l'article L. 331-12, l'Autorité de régulation de la communication audiovisuelle et numérique peut rendre publique l'inscription sur une liste du nom et des agissements de ceux des services de communication au public en ligne ayant fait l'objet d'une délibération dans le cadre de laquelle il a été constaté que ces services portaient atteinte, de manière grave et répétée, aux droits d'auteur ou aux droits voisins.

II.- L'engagement de la procédure d'instruction préalable à l'inscription sur la liste mentionnée au I du présent article est assuré par le rapporteur mentionné à l'article 42-7 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication ou par l'un de ses adjoints.

Sont qualifiés pour procéder, sur demande du rapporteur, à la recherche et à la constatation d'une atteinte aux droits d'auteur ou aux droits voisins les agents habilités et assermentés mentionnés au III de l'article L. 331-14 du présent code.

Ces agents, qui disposent des pouvoirs d'enquête reconnus à l'autorité par l'article 19 de la loi n° 86-1067 du 30 septembre 1986 précitée, peuvent prendre en compte tout élément utile et solliciter des titulaires de droits d'auteur ou de droits voisins toute information relative :

1° Aux autorisations d'exploitation que lesdits titulaires ont consenties à des services de communication au public en ligne ;

2° Aux notifications qu'ils ont adressées aux services de communication au public en ligne ou aux autres éléments permettant de constater l'exploitation illicite sur ces services d'œuvres ou d'objets protégés ;

3° Aux constats effectués par les agents agréés et assermentés mentionnés à l'article L. 331-2 du présent code.

Les constats des agents font l'objet de procès-verbaux, qui sont communiqués au rapporteur. S'il estime que les éléments recueillis justifient l'inscription sur la liste mentionnée au I du présent article, le rapporteur transmet le dossier à cette fin au président de l'autorité.

III.- L'autorité convoque le responsable du service de communication au public en ligne en cause à une séance publique pour le mettre en mesure de faire valoir ses observations et de produire tout élément justificatif. Cette convocation est effectuée par voie électronique sur la base des informations mentionnées au 2° de l'article 19 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ; lorsque ces informations ne sont pas disponibles, l'autorité informe le service concerné par l'intermédiaire de son site internet. Dans tous les cas, la convocation est adressée au moins quinze jours avant la date de la séance publique.

A la date fixée pour cette séance publique, le responsable du service en cause comparaît en personne ou par l'intermédiaire d'un représentant. Le défaut de comparution personnelle ou de représentation ne fait pas obstacle à la poursuite de la procédure.

IV.- A l'issue de la séance publique mentionnée au III, l'autorité délibère sur l'inscription du service de communication au public en ligne sur la liste mentionnée au I. L'autorité délibère hors la présence du rapporteur.

La délibération, prise après procédure contradictoire, par laquelle l'autorité estime qu'un service de communication au public en ligne a porté atteinte, de manière grave et répétée, aux droits d'auteur ou aux droits voisins et par laquelle elle décide, en conséquence, de l'inscrire sur la liste mentionnée au même I est motivée. L'autorité fixe la durée de l'inscription sur la liste mentionnée audit I, qui ne peut excéder douze mois.

La délibération est publiée sur le site internet de l'autorité et notifiée au service en cause par voie électronique, dans les conditions prévues au premier alinéa du III.

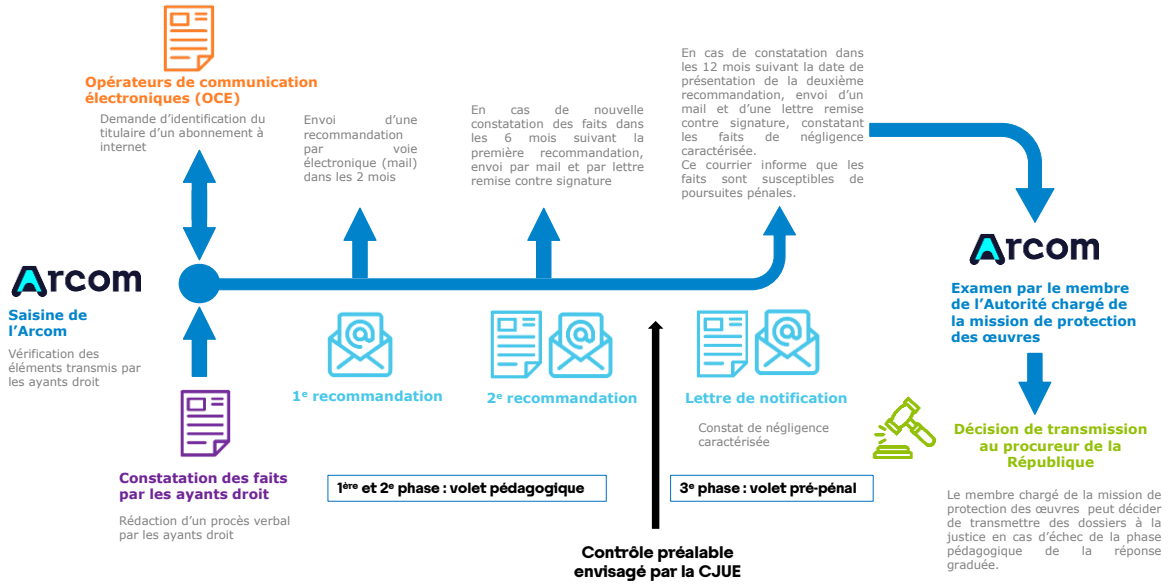
À tout moment, le service de communication au public en ligne peut demander à l'autorité d'être retiré de la liste mentionnée au I dès lors qu'il justifie du respect des droits d'auteur et des droits voisins. L'autorité statue sur cette demande par une décision motivée rendue après une séance publique organisée selon les modalités définies au III.

V.- La liste mentionnée au I peut être utilisée par les signataires des accords volontaires prévus à l'article L. 331-12. Pendant toute la durée de l'inscription sur cette liste, les annonceurs, leurs mandataires, les services mentionnés au 2° du II de l'article 299 du code général des impôts et toute autre personne en relation commerciale avec les services mentionnés au I du présent article, notamment pour pratiquer des insertions publicitaires ou procurer des moyens de paiement, rendent publique, au moins une fois par an, dans des conditions précisées par l'autorité, l'existence de ces relations et les mentionnent, le cas échéant, dans le rapport de gestion prévu au II de l'article L. 232-1 du code de commerce.

VI.- L'inscription, par l'autorité, sur la liste prévue au I du présent article ne constitue pas une étape préalable nécessaire à toute sanction ou voie de droit que les titulaires de droits peuvent directement solliciter auprès du juge.

e) Procédure de réponse graduée

Figure 10 : schéma de la procédure de réponse graduée



Source : Arcom

Article L. 336-3 du code de la propriété intellectuelle

La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise.
Le manquement de la personne titulaire de l'accès à l'obligation définie au premier alinéa n'a pas pour effet d'engager la responsabilité pénale de l'intéressé, sous réserve des articles L. 335-7 et L. 335-7-1.

Article L. 331-19 du code de la propriété intellectuelle

L'Autorité de régulation de la communication audiovisuelle et numérique agit sur saisine d'agents assermentés et agréés dans les conditions définies à l'article L. 331-2 qui sont désignés par :

- les organismes de défense professionnelle régulièrement constitués ;
- les organismes de gestion collective ;
- le Centre national du cinéma et de l'image animée.

L'autorité peut également agir sur la base d'informations qui lui sont transmises par le procureur de la République ou sur la base d'un constat d'huissier établi à la demande d'un ayant droit.
Elle ne peut être saisie de faits remontant à plus de six mois. Ce délai est de douze mois s'agissant des informations transmises par le procureur de la République.

Article L. 331-20 du code de la propriété intellectuelle

Lorsqu'elle est saisie de faits susceptibles de constituer un manquement à l'obligation définie à l'article L. 336-3, l'Autorité de régulation de la communication audiovisuelle et numérique peut envoyer à l'abonné, sous son timbre et pour son compte, par la voie électronique et par l'intermédiaire de la personne dont l'activité est d'offrir un accès à des services de communication au public en ligne ayant conclu un contrat avec l'abonné ou par lettre simple, une recommandation lui rappelant les dispositions de l'article L. 336-3, lui enjoignant de respecter l'obligation qu'elles définissent et l'avertissant des sanctions encourues en application des articles L. 335-7 et L. 335-7-1. Cette recommandation contient également une information de l'abonné sur l'offre légale de contenus culturels en ligne, sur l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation définie à l'article L. 336-3 ainsi que sur les dangers pour le renouvellement de la création artistique et pour l'économie du secteur culturel des pratiques ne respectant pas le droit d'auteur et les droits voisins.

En cas de renouvellement, dans un délai de six mois à compter de l'envoi de la recommandation visée au premier alinéa, de faits susceptibles de constituer un manquement à l'obligation définie à l'article L. 336-3, l'autorité peut adresser une nouvelle recommandation comportant les mêmes informations que la précédente par la voie électronique dans les conditions prévues au premier alinéa. Elle doit assortir cette recommandation d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date de présentation de cette recommandation.

Les recommandations adressées sur le fondement du présent article mentionnent la date et l'heure auxquelles les faits susceptibles de constituer un manquement à l'obligation définie à l'article L. 336-3 ont été constatés. Elles précisent le contenu des œuvres ou objets protégés concernés par ce manquement. Elles indiquent les coordonnées postales et électroniques où leur destinataire peut adresser, s'il le souhaite, des observations à l'autorité.

Article L. 331-21 du code de la propriété intellectuelle

Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne font figurer, dans les contrats conclus avec leurs abonnés, la mention claire et lisible des dispositions de l'article L. 336-3 et des mesures qui peuvent être prises par l'Autorité de régulation de la communication audiovisuelle et numérique. Elles font également figurer, dans les contrats conclus avec leurs abonnés, les sanctions pénales et civiles encourues en cas de violation des droits d'auteur et des droits voisins et en application de l'article L. 335-7-1.

En outre, les personnes visées au premier alinéa du présent article informent leurs nouveaux abonnés et les personnes reconduisant leur contrat d'abonnement sur l'offre légale de contenus culturels en ligne, sur l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation définie à l'article L. 336-3 ainsi que sur les dangers pour le renouvellement de la création artistique et pour l'économie du secteur culturel des pratiques ne respectant pas le droit d'auteur et les droits voisins.

Article L. 331-22 du code de la propriété intellectuelle

L'Autorité de régulation de la communication audiovisuelle et numérique peut conserver les données techniques mises à sa disposition pendant la durée nécessaire à l'exercice des compétences qui lui sont confiées au présent paragraphe.

La personne dont l'activité est d'offrir un accès à des services de communication au public en ligne est tenue d'informer l'autorité de la date à laquelle elle a débuté la

suspension ; l'autorité procède à l'effacement des données à caractère personnel relatives à l'abonné dès le terme de la période de suspension.

Article L. 331-23 du code de la propriété intellectuelle

Est autorisée la création, par l'Autorité de régulation de la communication audiovisuelle et numérique, d'un traitement automatisé de données à caractère personnel portant sur les personnes faisant l'objet d'une procédure dans le cadre du présent paragraphe.
Ce traitement a pour finalité la mise en œuvre, par l'autorité, des mesures prévues au présent paragraphe, de tous les actes de procédure afférents et des modalités de l'information des organismes de défense professionnelle et des organismes de gestion collective des éventuelles saisines de l'autorité judiciaire ainsi que des notifications prévues au cinquième alinéa de l'article L. 335-7.
Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les modalités d'application du présent article. Il précise notamment :
— les catégories de données enregistrées et leur durée de conservation ;
— les destinataires habilités à recevoir communication de ces données, notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne ;
— les conditions dans lesquelles les personnes intéressées peuvent exercer, auprès de l'autorité, leur droit d'accès aux données les concernant conformément à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Article L. 331-24 du code de la propriété intellectuelle

Un décret en Conseil d'Etat précise les conditions d'application du présent paragraphe.

Article L. 335-3 du code de la propriété intellectuelle

Est également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi.
Est également un délit de contrefaçon la violation de l'un des droits de l'auteur d'un logiciel définis à l'article L. 122-6.
Est également un délit de contrefaçon toute captation totale ou partielle d'une œuvre cinématographique ou audiovisuelle en salle de spectacle cinématographique.

Article L. 335-7-1 du code de la propriété intellectuelle

Pour les contraventions de la cinquième classe prévues par le présent code, lorsque le règlement le prévoit, la peine complémentaire définie à l'article L. 335-7 peut être prononcée selon les mêmes modalités, en cas de négligence caractérisée, à l'encontre du titulaire de l'accès à un service de communication au public en ligne auquel l'Autorité de régulation de la communication audiovisuelle et numérique, en application de l'article L. 331-19, a préalablement adressé, par voie d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date de présentation, une recommandation l'invitant à mettre en œuvre un moyen de sécurisation de son accès à internet.
La négligence caractérisée s'apprécie sur la base des faits commis au plus tard un an après la présentation de la recommandation mentionnée à l'alinéa précédent.
Dans ce cas, la durée maximale de la suspension est d'un mois.

Le fait pour la personne condamnée à la peine complémentaire prévue par le présent article de ne pas respecter l'interdiction de souscrire un autre contrat d'abonnement à

un service de communication au public en ligne pendant la durée de la suspension est puni d'une amende d'un montant maximal de 3 750 €.

Article R. 335-5 du code de la propriété intellectuelle

I.- Constitue une négligence caractérisée, punie de l'amende prévue pour les contraventions de la cinquième classe, le fait, sans motif légitime, pour la personne titulaire d'un accès à des services de communication au public en ligne, lorsque se trouvent réunies les conditions prévues au II :

1° Soit de ne pas avoir mis en place un moyen de sécurisation de cet accès ;

2° Soit d'avoir manqué de diligence dans la mise en œuvre de ce moyen.

II.- Les dispositions du I ne sont applicables que lorsque se trouvent réunies les deux conditions suivantes :

1° En application de l'article L. 331-20 et dans les formes prévues par cet article, le titulaire de l'accès s'est vu recommander par le membre de l'Autorité de régulation de la communication audiovisuelle et numérique désigné en application du IV de l'article 4 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication de mettre en œuvre un moyen de sécurisation de son accès permettant de prévenir le renouvellement d'une utilisation de celui-ci à des fins de reproduction, de représentation ou de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise ;

2° Dans l'année suivant la présentation de cette recommandation, cet accès est à nouveau utilisé aux fins mentionnées au 1° du présent II.

f) Encouragement au développement de l'offre légale

Article L. 331-17 du code de la propriété intellectuelle

Au titre de sa mission d'encouragement au développement de l'offre légale, qu'elle soit ou non commerciale, et d'observation de l'utilisation, qu'elle soit licite ou illicite, des œuvres et des objets protégés par un droit d'auteur ou par un droit voisin ou par des droits d'exploitation audiovisuelle mentionnés à l'article L. 333-10 du code du sport sur les réseaux de communications électroniques, l'Autorité de régulation de la communication audiovisuelle et numérique développe des outils visant à renforcer la visibilité et le référencement de l'offre légale auprès du public et publie chaque année des indicateurs dont la liste est fixée par décret. Elle rend compte du développement de l'offre légale dans le rapport mentionné à l'article 18 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

Elle identifie et étudie les modalités techniques permettant l'usage illicite des œuvres et des objets protégés par un droit d'auteur ou par un droit voisin ou par des droits d'exploitation audiovisuelle mentionnés à l'article L. 333-10 du code du sport sur les réseaux de communications électroniques. Dans le cadre du rapport prévu à l'article 18 de la loi n° 86-1067 du 30 septembre 1986 précitée, elle propose, le cas échéant, des solutions visant à y remédier.

g) Évaluation des mesures techniques d'identification (MTI) – mise en œuvre de l'article 17 de la directive 2019/790 du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique

Article L. 331-18 du code de la propriété intellectuelle

I.- L'Autorité de régulation de la communication audiovisuelle et numérique évalue le niveau d'efficacité des mesures de protection des œuvres et des objets protégés, prises par les fournisseurs de services de partage de contenus en ligne mentionnés à l'article L. 137-1, au regard de leur aptitude à assurer la protection des œuvres et des objets protégés, y compris leurs conditions de déploiement et de fonctionnement. Elle peut formuler des recommandations en vue de leur amélioration ainsi que sur le niveau de transparence requis.

Au titre de la mission d'évaluation mentionnée au premier alinéa du présent I, les agents habilités et assermentés de l'Autorité de régulation de la communication audiovisuelle et numérique peuvent mettre en œuvre des méthodes proportionnées de collecte automatisée des données publiquement accessibles.

L'Autorité de régulation de la communication audiovisuelle et numérique peut solliciter toutes informations utiles auprès des fournisseurs de service, des titulaires de droit et des concepteurs des mesures de protection.

II.- L'Autorité de régulation de la communication audiovisuelle et numérique encourage la coopération entre titulaires de droits et fournisseurs de services de partage de contenus en ligne en vue d'assurer la disponibilité sur le service des contenus téléversés par les utilisateurs qui ne portent pas atteinte au droit d'auteur et aux droits voisins. Elle peut, après consultation des parties prenantes, formuler des recommandations à l'attention des titulaires de droits et des fournisseurs de services, en particulier s'agissant des notifications ou des informations nécessaires et pertinentes fournies par les titulaires de droits.

III.- L'Autorité de régulation de la communication audiovisuelle et numérique rend compte de la mission prévue au présent article dans le rapport mentionné à l'article 18 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

3. Propositions de loi et amendements

a) *Proposition de loi visant à conforter la filière cinématographique en France (adoptée par le Sénat et déposée au bureau de l'Assemblée Nationale le 23 juillet 2024)*

Article 8

Le I de l'article L. 331-27 du code de la propriété intellectuelle est ainsi modifié :

1° Le premier alinéa est ainsi modifié :

a) À la première phrase, les mots : « passée en force de chose jugée » sont remplacés par le mot : « exécutoire » ;

b) À la même première phrase, les mots : « un titulaire de droits partie à la décision judiciaire » sont remplacés par les mots : « toute personne qualifiée pour agir sur le fondement du même article L. 336-2 » ;

c) Après la référence : « I, », la fin de la seconde phrase est ainsi rédigée : « le président de l'autorité ou, en cas d'empêchement, tout membre du collège désigné par lui, communique précisément les données d'identification du service en cause selon les modalités définies par l'autorité. » ;

2° Au deuxième alinéa, les mots : « l'autorité » sont remplacés par les mots : « le président de l'autorité ou, en cas d'empêchement, tout membre du collège de l'autorité désigné par lui » ;

3° Il est ajouté un alinéa ainsi rédigé :

« L'Autorité de régulation de la communication audiovisuelle et numérique tient à jour une liste des services de communication au public en ligne mentionnés au présent I qui ont fait l'objet de sa part d'une demande de blocage d'accès ou d'une demande de déréférencement ainsi que des données d'identification permettant l'accès à ces services et met cette liste à la disposition des signataires des accords mentionnés au troisième alinéa. Ces services sont inscrits sur cette liste pour la durée restant à courir des mesures ordonnées par l'autorité judiciaire. »

b) *Proposition de loi relative à l'organisation, à la gestion et au financement du sport professionnel (adoptée par le Sénat et déposée au bureau de l'Assemblée Nationale le 11 juin 2025)*

Article 10

La section 3 du chapitre III du titre III du livre III du code du sport est ainsi modifiée :

1° L'article L. 333-10 est ainsi modifié :

a) Au 1° du I, après le mot : « professionnelle », sont insérés les mots : « ou une société commerciale créée en application des articles L. 333-1 ou L. 333-2-1 » et, avant le mot : « compétitions », sont insérés les mots : « manifestations ou de » ;

b) Après le III, sont insérés des III bis et III ter ainsi rédigés :

« III bis. – Lorsque l'ordonnance prise sur le fondement du II le prévoit, les titulaires de droits communiquent à l'Autorité de régulation de la communication audiovisuelle et numérique, selon les modalités définies par une délibération de l'Autorité, les données d'identification permettant d'assurer la mise en œuvre sans délai des mesures propres à empêcher, pendant la diffusion en direct de la manifestation ou de la compétition sportive, l'accès aux services de communication au public en ligne non encore identifiés à la date de ladite ordonnance.

« La délibération mentionnée au premier alinéa du présent III bis prévoit également les conditions de validité des saisines des titulaires de droits, les modalités selon lesquelles les procédés de collecte des données d'identification choisis par les titulaires de droits sont soumis à l'accord de l'Autorité de régulation de la communication audiovisuelle et numérique avant leur mise en œuvre et la durée de conservation des éléments de preuve. L'Autorité ou un tiers mandaté par elle peut contrôler à tout moment les conditions dans lesquelles les données d'identification sont collectées par les titulaires de droits. À cette fin, elle peut recueillir auprès d'eux toutes les informations nécessaires à l'exercice de sa mission.

« Les données d'identification sont transmises aux personnes mentionnées par l'ordonnance prise sur le fondement du II par l'intermédiaire du système automatisé contrôlé par l'Autorité de régulation de la communication audiovisuelle et numérique afin qu'elles exécutent sans délai les mesures ordonnées à l'égard de ces services pendant toute la durée de la diffusion en direct de la manifestation ou de la compétition sportive. Les titulaires de droit attestent par tout moyen que les services dont il est demandé le blocage sans délai diffusent illicitement la compétition ou la manifestation sportive ou ont pour objectif principal ou parmi leurs objectifs principaux une telle diffusion. Ils en conservent la preuve et la tiennent à la disposition de l'Autorité selon des modalités qu'elle détermine.

« Pendant la diffusion en direct de la manifestation ou de la compétition sportive, le titulaire de droits concerné met à jour régulièrement les données d'identification transmises et sollicite sans délai, par l'intermédiaire du système automatisé, la levée de la mesure de blocage si ces données ne sont plus actives ou si leur objet a changé.

« Le titulaire de droits concerné informe par tout moyen les personnes dont le service de communication au public en ligne fait l'objet desdites mesures, le cas échéant par l'intermédiaire de son hébergeur.

« Les agents habilités et assermentés de l'Autorité peuvent, à tout moment et par tout moyen, s'assurer de la conformité des mesures prises sur la base des données d'identification transmises par l'intermédiaire du système automatisé au regard des conditions de validité définies conformément au deuxième alinéa du présent III bis. Lorsqu'ils constatent qu'une telle conformité n'est pas assurée, ils suspendent sans délai toute mesure avant la fin de la diffusion en direct de la manifestation ou de la compétition sportive.

« L'Autorité de régulation de la communication audiovisuelle et numérique peut solliciter des titulaires de droits tous les éléments nécessaires à la vérification de la conformité des saisines transmises par l'intermédiaire du système automatisé à la délibération susmentionnée.

« L'Autorité de régulation de la communication audiovisuelle et numérique peut adresser à tout moment, aux titulaires de droits, toute préconisation qu'elle juge nécessaire aux fins d'assurer ladite conformité. Elle est informée sans délai injustifié des suites données à ces préconisations.

« Lorsque le titulaire de droits ne donne pas suite à ces préconisations, de façon non justifiée, l'Autorité peut lui enjoindre, après mise en demeure, d'interrompre la transmission de données d'identification par le biais du système automatisé. Cette interruption est maintenue jusqu'à ce que le titulaire de droits est en mesure de se conformer à ces préconisations.

« Toute personne dont le service de communication au public en ligne a fait l'objet d'une mesure mentionnée au premier alinéa du présent III bis peut introduire devant le président de l'Autorité de régulation de la communication audiovisuelle et numérique ou tout membre du collège désigné par lui un recours contre ladite mesure, sous réserve de justifier de son identité et de l'irrégularité de la mesure, y compris pendant la diffusion en direct de la manifestation ou de la compétition sportive. Le président de l'Autorité ou tout membre du collège désigné par lui rend sa décision sur le recours après avoir sollicité, par tous moyens, les observations du titulaire de droits et de la personne qui a fait l'objet de la mesure de blocage.

« III ter. – Les litiges entre les titulaires de droits et les personnes mentionnées par l'ordonnance prévue au II relèvent de la compétence du président du tribunal judiciaire. » ;

c) Le IV est ainsi rédigé :

« IV. – L'Autorité de régulation de la communication audiovisuelle et numérique adopte des modèles d'accord que sont invités à conclure les titulaires de droits mentionnés au I, la ligue professionnelle ou la société commerciale créée en application des articles L. 333-1 ou L. 333-2-1 du présent code, l'entreprise de communication audiovisuelle ayant acquis un droit à titre exclusif et toute personne susceptible de contribuer à remédier aux atteintes mentionnées au I du présent article.

« L'accord conclu entre les parties précise les mesures qu'elles s'engagent à prendre pour prévenir et faire cesser d'éventuelles violations de l'exclusivité du droit d'exploitation audiovisuelle de la manifestation ou compétition sportive et la répartition du coût des mesures volontaires ou ordonnées sur le fondement du II.

« L'Autorité de régulation de la communication audiovisuelle et numérique tient à jour une liste des données d'identification permettant l'accès aux services de communication au public en ligne qui font l'objet des mesures mentionnées aux III et III bis. Ces services sont inscrits sur cette liste pendant toute la durée des mesures prévues conformément aux mêmes III et III bis.

« L'Autorité de régulation de la communication audiovisuelle et numérique met cette liste à disposition des signataires des accords volontaires. » ;

2° Sont ajoutés des articles L. 333-12 à L. 333-15 ainsi rédigés :

« Art. L. 333-12. – Les titulaires de droits rendent régulièrement compte à l'Autorité de régulation de la communication audiovisuelle et numérique des modalités de collecte des données d'identification et de transmission de celles-ci par l'intermédiaire du système automatisé.

« L'Autorité peut solliciter, auprès des personnes mentionnées par l'ordonnance prévue au II de l'article L. 333-10 et des signataires des accords volontaires, toute information utile relative à la mise en œuvre des mesures prises sur le fondement du III bis du même article L. 333-10.

« L'Autorité de régulation de la communication audiovisuelle et numérique rend compte de l'exercice de la mission prévue au présent article dans son rapport annuel d'activité.

« Art. L. 333-13. – I. – Est puni de trois ans d'emprisonnement et de 300 000 euros d'amende le fait de concevoir, d'éditer ou de mettre à la disposition du public, à titre onéreux ou à titre gratuit, un service de communication au public en ligne diffusant une compétition ou une manifestation sportive, sans l'autorisation :

« 1° Du titulaire du droit d'exploitation audiovisuelle au titre de l'article L. 333-1 ;

« 2° De l'entreprise de communication audiovisuelle, dans le cas où elle a acquis un droit à titre exclusif, par contrat ou accord d'exploitation audiovisuelle, sur une compétition ou manifestation sportive, que cette compétition ou manifestation sportive soit organisée sur le territoire français ou à l'étranger ;

« 3° De la ligue professionnelle, dans le cas où elle commercialise les droits d'exploitation audiovisuelle de manifestations ou de compétitions sportives professionnelles ;

« 4° Ou de la société commerciale créée par cette ligue professionnelle en application des articles L. 333-1 ou L. 333-2-1.

« II. – Est puni de trois ans d'emprisonnement et de 300 000 euros d'amende le fait de communiquer ou de mettre à la disposition du public, de façon habituelle, par l'intermédiaire d'une plateforme en ligne, à titre onéreux ou à titre gratuit, des retransmissions d'une compétition ou d'une manifestation sportive sans l'autorisation de l'une des personnes mentionnées aux 1° à 4° du I.

« III. – Est puni de trois ans d'emprisonnement et de 300 000 euros d'amende le fait, à des fins d'exploitation de droits exclusifs de compétitions ou de manifestations sportives sans titre ni propriété de ces droits, de fabriquer, importer, offrir à la vente, détenir en vue de la vente, vendre, louer, mettre à la disposition du public ou installer un dispositif ou un logiciel ayant manifestement pour objet de permettre l'accès illégal aux services mentionnés au I.

« IV. – Lorsque les délits prévus aux I à III ont été commis en bande organisée, les peines sont portées à sept ans d'emprisonnement et à 750 000 euros d'amende.

« V. – Est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait d'inciter par tout moyen, y compris par une annonce publicitaire, à l'usage d'un service de communication au public en ligne, d'un dispositif ou d'un logiciel permettant l'accès à une compétition ou une manifestation sportive sans l'autorisation de l'une des personnes mentionnées aux 1° à 4° du I.

« Art. L. 333-14 (nouveau). – Les personnes physiques coupables de l'une des infractions prévues à l'article L. 333-13 peuvent en outre être condamnées, à leurs frais, à retirer des circuits commerciaux tout dispositif ou logiciel mentionné au même article L. 333-13 ainsi que toute autre chose qui a servi ou était destinée à commettre l'infraction.

« La juridiction peut prononcer la confiscation de tout ou partie des recettes procurées par l'infraction ainsi que celle du matériel spécialement installé en vue de la réalisation du délit.

« Elle peut ordonner la destruction, aux frais du condamné, des dispositifs mentionnés audit article L. 333-13, ou de toute autre chose retirée des circuits commerciaux ou confisqués, sans préjudice de tous dommages et intérêts. Elle peut également ordonner, aux frais du condamné, l'affichage ou la diffusion du jugement prononçant la condamnation, dans les conditions prévues à l'article 131-35 du code pénal.

« Art. L. 333-15 (nouveau). – Les personnes morales déclarées responsables pénalement, dans les conditions prévues à l'article 121-2 du code pénal, des infractions définies à l'article L. 333-13 du présent code encourent, outre l'amende suivant les modalités prévues à l'article 131-38 du code pénal, les peines prévues à l'article 131-39 du même code. »

4. Usages du RSN dans le cadre de la lutte contre le piratage

Le règlement sur les services numériques (RSN)[80] contient des outils horizontaux de lutte contre les contenus illicites, y compris ceux portant atteinte au droit d'auteur ou aux droits voisins prévus par des textes spécifiques tels que la directive 2001/29/CE et la directive 2019/790/CE. Les retransmissions illicites de manifestations sportives, même si elles ne sont pas couvertes en tant que telles par le droit d'auteur et les droits voisins au sens du droit de l'UE, sont considérées comme des **contenus illicites au regard du droit français, et donc, au titre du RSN**.

Le règlement sur les services numériques fournit une palette d'outils mobilisables dans la lutte contre le piratage sur les fournisseurs de services en ligne. Depuis son entrée complète en application le 17 février 2024, tous les services d'hébergement sont désormais soumis aux obligations[81] du texte.

a) Signalements et injonctions d'agir s'agissant de la diffusion de contenus culturels et de la retransmissions illicites d'évènements sportifs dans le cadre du RSN

L'outil le plus immédiat, à portée de toutes les personnes faisant face à des atteintes à leurs droits de propriété intellectuelle, est le signalement. L'article 16 du RSN dispose que tous les fournisseurs de services d'hébergement, y compris les plateformes en ligne, doivent mettre à disposition des mécanismes de signalement des contenus illicites.

Ces outils doivent permettre aux utilisateurs de ces services de signaler la présence de contenus illicites directement depuis l'interface. Le RSN pose ensuite ce signalement comme le point de départ de la responsabilité de la plateforme : son inaction pour retirer le contenu ou le rendre inaccessible déclenche la possibilité d'engager sa responsabilité.

Le formulaire de signalement doit être « *facile d'accès et d'utilisation* »[82] pour les utilisateurs, le rendant actionnable par les titulaires de droits, qui peuvent ainsi porter à la connaissance du fournisseur de services la présence d'un contenu culturel protégé par le droit ou d'une retransmission illicite, y compris en direct, d'un évènement sportif.

Le traitement des signalements doit être réalisé « *en temps opportun de manière diligente, non arbitraire et objective* »[83]. Cette promptitude est particulièrement importante dans le cadre de la lutte contre les retransmissions illicites de manifestations sportives en direct, qui suppose une forte réactivité des fournisseurs (une inertie de traitement rendant les signalements sans objet).

En son article 22, le RSN crée un statut de signaleur de confiance dont les signalements de contenus illicites doivent être traités en priorité par les plateformes. Plusieurs ayants droit se sont manifestés pour obtenir le statut de signaleur de confiance, qui a été accordé par l'Autorité à l'ALPA (association de lutte contre la piraterie audiovisuelle, active dans le domaine de la culture).

Par ailleurs, l'article 9 du RSN permet aux autorités judiciaires ou administratives nationales d'émettre des **injonctions** d'actions contre des contenus illicites auprès des

[80] Règlement 2022/2065 du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).
[81] Les premières très grandes plateformes en ligne et les très grands moteurs de recherche (VLOPSEs en anglais) étaient déjà soumis à cette obligation depuis août 2023.
[82] Article 16 du RSN, paragraphe 1.
[83] Article 16 du RSN, paragraphe 6.

fournisseurs de services intermédiaires, y compris les plateformes en ligne. Ces injonctions peuvent être adressées par des autorités d'un État membre à des services qui sont établis dans d'autres États membres et doivent préciser « *leur champ d'application territorial, (…) sur la base des règles applicables du droit de l'Union et du droit national* ». Ces injonctions peuvent notamment avoir pour objet de mettre fin à la diffusion du contenu ou de la retransmission illicite de manifestations sportives ou autres[84]. Si le formalisme prévu à l'article 9 est respecté, les services qui en sont destinataires sont tenus d'y répondre en indiquant si elles ont agi (ou non).

b) Transparence sur les mesures adoptées par les plateformes à la suite de signalements ou d'injonctions

- *Rapports de transparence*

De manière complémentaire, le RSN impose aux fournisseurs de services d'hébergement, dont les plateformes en ligne, de **rendre compte de leurs activités de modération dans le cadre de rapports de transparence annuels** (semestriels pour les très grandes plateformes et très grands moteurs de recherche). Ces rapports doivent contenir **des données essentiellement quantitatives** à propos du traitement des injonctions, des signalements et des mesures proactives de modération. Ils doivent aussi inclure des informations sur les réclamations formulées par les utilisateurs pour contester les mesures de modération. On y retrouve parfois des **données chiffrées spécifiques relatives aux actions de modération** prises sur la base **d'atteintes à la propriété intellectuelle** (comprenant le droit d'auteur).

En outre, les rapports de transparence doivent mentionner le **délai médian de traitement des signalements et injonctions**. Ils constituent ainsi un outil de suivi permettant de documenter les activités de modération des plateformes sur des contenus illicites comme ceux portant atteinte à la propriété intellectuelle.

À date, **chaque rapport de transparence publié est construit selon sa propre méthodologie et les méthodes retenues sont très hétérogènes**. **Les rapports publiés à ce jour font uniquement référence à la catégorie des atteintes à la propriété intellectuelle, sans isoler plus spécifiquement celles relatives à la diffusion d'évènements sportifs, ni distinguer selon que l'évènement est diffusée en direct ou qu'il s'agit d'une rediffusion**. A noter que les modèles harmonisés de rapport de transparence, qui deviendront obligatoires[85] à compter de février 2026 pour les actions de modération entreprises à partir du 1er juillet 2025, comprennent une catégorie sur les atteintes à la propriété intellectuelle et une sous-catégorie sur les atteintes spécifiques au droit d'auteur (« *Copyright* »).

La propriété intellectuelle est un des types de contenus illicites les moins représentés dans l'ensemble des rapports de transparence, ce qui s'observe notamment, s'agissant des rapports publiés en avril 2025, à travers :

- la (quasi-totale) absence d'injonctions des autorités sur ce fondement, à l'exception de quelques-unes sur certaines places de marché ;

[84] Il semble que la loi française permettant à l'Arcom, sur la base d'une décision judiciaire initiale, de demander le blocage des sites diffusant sans autorisation des compétitions sportives identifiés *a posteriori* et ce jusqu'à la fin de la compétition, pourrait correspondre à une injonction d'agir au sens de l'article 9 du RSN, dès lors que celle-ci respecte le formalisme imposé par l'article 9 du règlement (v. art. L. 333-10 du code du sport).

[85] Règlement d'exécution 2024/2835 établissant des modèles en ce qui concerne les obligations en matière de rapports de transparence incombant aux fournisseurs de services intermédiaires et aux fournisseurs de plateformes en ligne en vertu du règlement (UE) 2022/2065 du Parlement européen et du Conseil.

- le très faible nombre de signalements, sauf sur certaines places de marché (ALiExpress, où il s'agit d'un des premiers motifs de signalements en nombre, ainsi qu'Amazon et Temu), quelques réseaux sociaux (Facebook et Instagram) et des plateformes de partages de vidéos (YouTube) ; si environ la moitié des signalements donne lieu à une action de modération de la part des places de marché, ceux sur les réseaux sociaux semblent moins suivis ;

- la part très faible de mesures pro actives adoptées sur le fondement d'une atteinte à la propriété intellectuelle :
    - dans certains rapports, la propriété intellectuelle n'est pas une catégorie identifiée amenant à des mesures de modération proactives (Tik Tok et Snapchat) ;
    - pour les plateformes de réseaux sociaux communiquant l'information, les mesures de modération proactives sur la base de la propriété intellectuelle sont résiduelles par rapport au nombre total de mesures prises (pour X, 870 mesures sur 55 millions ; pour Google Play, 33 sur 4,5 millions ; pour Instagram, 247 641 sur presque 40 millions) ;
    - sur certaines places de marché, la modération pro active de contenus portant atteinte à la propriété intellectuelle est parfois plus importante (atteignant presque 4 % du total des mesures prises pour Aliexpress et 37 % pour Shein) ;
    - à noter également que Google Search mentionne les atteintes à la propriété intellectuelle comme le premier fondement des mesures de modération pro active adoptées sur le moteur de recherche (ce qui était déjà le cas dans son précédent rapport sur le 2e semestre 2024).

À titre général, **les rapports ne permettent pas de savoir le temps médian de réaction** des plateformes pour traiter les signalements relatifs à des contenus portant atteinte à la propriété intellectuelle. Toutefois, on relèvera que les plateformes (hors boutiques d'applications) mettent dans la majorité moins de 24 heures pour traiter les signalements tous types de contenus confondus.

- *Rapports d'évaluation et d'atténuation des risques systémiques*

Les VLOPSEs sont soumis à des **obligations supplémentaires d'analyse et d'atténuation des risques systémiques** identifiés sur leur service. Dans ce cadre, ils doivent réaliser ou mettre en place (au moins une fois par an) :
- une évaluation des risques systémiques présents sur leurs services (art. 34 du RSN) ;
- des mesures d'atténuation adaptées aux risques identifiés lors de l'évaluation (art. 35 du RSN) ;
- un audit indépendant de conformité (art. 37 du RSN).

Les risques liés aux atteintes à la propriété intellectuelle sont bien identifiés par la plupart des VLOPSEs, cependant, le risque spécifique lié aux retransmissions en direct d'évènements sportifs n'est jamais explicitement détaillé.

Sur les réseaux sociaux (Tik Tok, Instagram, Youtube, X, Facebook, Pinterest, Snapchat) désignés VLOPs :

- le risque lié aux atteintes à la propriété intellectuelle est souvent classé comme **un des risques les moins importants** (tout particulièrement Instagram et TikTok par exemple, où il s'agit du risque identifié comme le moins élevé) ;
- les développements dans les rapports sur le sujet sont souvent relativement courts et très peu détaillés (atténuation des risques compris), allant jusqu'à moins d'une page, illustrant la **faible importance relative** de ce risque selon les plateformes.

Pour atténuer le risque plus général d'atteinte aux droits de PI, trois mesures sont communes à la majorité des rapports des ces réseaux sociaux :
- la mise en place d'un **canal ou formulaire dédié pour le respect du droit d'auteur**[86];
- la **coopération** avec les parties prenantes (spécialement les ayants-droits) ;
- la mise en place de **calendrier des évènements majeurs.**
(à titre d'exemple, le rapport d'évaluation des risques de X[87] indique que la plateforme considère que la gravité des atteintes à la propriété intellectuelle est généralement faible et qu'elle prend les mesures appropriées pour retirer le contenu si nécessaire après avoir reçu un signalement. Elle précise notamment « *se préparer aux évènements à risque en tenant un calendrier des futurs évènements sportifs et télévisuels populaires afin d'assurer une couverture et un soutien suffisants de la part des agents, le cas échéant (c'est-à-dire des agents supplémentaires pendant les heures de pointe de l'événement), en prévision d'éventuels pics dans la charge de travail liée aux infractions au droit d'auteur* ».).

Sur les **très grands moteurs de recherche (Bing, Google)**, le sujet de la propriété intellectuelle est très brièvement évoqué (au sein des contenus illicites), et les mesures d'atténuation mentionnées reposent essentiellement sur les mécanismes de signalement.

Sur les **places de marché en ligne désignées VLOPs (Aliexpress, Temu, Shein, Amazon, Google Shopping, Zalando)**, le sujet de la propriété intellectuelle est beaucoup plus prégnant, notamment du fait des potentiels atteintes aux droits de marque provenant des offres de produits. Le sujet très spécifique des produits pouvant permettre d'accéder à des canaux de rediffusion en direct de compétitions sportives n'est pas évoqué spécifiquement par ces places de marché. A noter par ailleurs que certaines comme Amazon ne mentionnent la propriété intellectuelle que sous l'angle de la protection des marques.

[86] En réalité, les plateformes parlent de « Copyright ».
[87] Report setting out the results of twitter international unlimited company risk assessment pursuant to article 34 EU digital services act – august 2024.

5. Comparaison des principaux indicateurs relatifs aux usages illicites

Pour rappel, une **étude quantitative** (ou étude sondagière) repose sur l'interrogation d'un échantillon limité d'un nombre d'individus (de l'ordre de quelques milliers de répondants, 1 000 au minimum, 3 000 à 4 000 pour les échantillons les plus importants), sa représentativité étant assurée par la méthode des quotas (principalement des quotas socio-démographiques : âge, sexe, profession et catégorie socio-professionnelle, région et/ou taille d'agglomération du lieu de résidence du répondant).

Les différentes études quantitatives réalisées par l'Arcom peuvent présenter des différences de résultat pour un même indicateur (par exemple : usage illicite, recours à un VPN, etc.). Ces différences peuvent avoir différentes origines, entre autres :

- la structure de l'échantillon : certaines études ont un échantillon représentatif de la population des internautes, d'autres de la population française ;
- la formulation de la question : pour un même indicateur, la façon d'interroger le répondant peut varier (question simple, croisement de réponses à différentes questions pour identifier un usage, etc.) ;
- les explications présentant un outil : la définition du VPN dans l'étude omnibus de 2025 précise par exemple la possibilité de « *de sécuriser leur connexion* », ce qui n'était pas mentionné dans l'étude « mesure de contournement » de 2023.

La **mesure d'audience** des sites et applications, mise en œuvre en France par Médiamétrie, repose sur l'analyse des comportements en ligne d'un panel de 25 000 internautes âgés de deux ans et plus, à partir d'un *meter* (ou balise) déposée sur les équipements utilisés traçant toute l'activité en ligne (mesure dite trois écrans : ordinateur fixe ou portable, tablette et smartphone). Il s'agit d'une mesure dite « passive », un internaute étant considéré comme utilisateur d'un service s'il a accédé au site ou application au moins une fois durant le mois écoulé, sur l'un des trois écrans suivis.

La mesure d'audience permet de mesurer assez précisément le taux d'utilisation des protocoles permettant d'accéder à des services illicites disponibles sur des sites internet ou, éventuellement, accessibles des applications, telles que le streaming, le live streaming ou le pair à pair ou le téléchargement direct.

A l'inverse, la mesure d'audience ne permet pas d'appréhender dans leur globalité le recours à l'IPTV illicite. Si celle-ci prend en compte le recours aux applications IPTV illicites sur ordinateur, smartphone et tablette (soit les trois écrans mesurés par Médiamétrie), les usages sur téléviseur, au moyen d'un boitier relié à celui-ci ou en ayant recours à une application IPTV téléchargé directement par l'OS (système d'exploitation) d'un téléviseur connecté (ou *smart* TV) ne sont pas comptabilisés.

L'enquête déclarative, permettant d'interroger les internautes sur l'ensemble de leurs modes d'accès à l'IPTV illicite, y compris le recours à des boitiers ou des applications sur TV connectée, s'avère donc nécessaire pour mesurer dans leur globalité ces usages.

Tableau 6 : Principaux indicateurs des usages illicites, selon les études de l'Arcom

En % d'internautes	Baromètre de la consommation (2025)	Omnibus DNS / VPN / IPTV (2025)	IPTV illicite (2024)	Mesure de contournement (2023)	Mesure audience juillet 2025
Sur base « ensemble internautes »					
Usages illicites en général	**25 %**	**n.d.**	**n.d.**	**24 %**	**14 %**
Streaming	12 %	n.d.	n.d.	n.d.	11 %
Téléchargement direct	11 %	n.d.	n.d.	n.d.	
Live streaming	2 %	n.d.	n.d.	n.d.	2 %
Pair à pair	6 %	n.d.	n.d.	n.d.	2 %
IPTV illicite	6 %	10 % (utilisent actuellement :5 % / déjà utilisé mais n'utilisent plus : 5 %)	11 %	n.d.	n.d.
Modification paramétrage DNS	n.d.	7 % (utilisent actuellement :5 % / déjà utilisé mais n'utilisent plus : 2 %)	n.d.	20 %	n.d.
Usage VPN	n.d.	23 % (utilisent actuellement :14 % / déjà utilisé mais n'utilisent plus : 9 %)	n.d.	29 % (régulier : 15 %)	n.d.
Sur base « internautes illicites »					
Streaming	48 %	n.d.	n.d.	n.d.	84 %
Téléchargement direct	44 %	n.d.	n.d.	n.d.	
Live streaming	7 %				14 %
Pair à pair	25 %	n.d.	n.d.	n.d.	13 %
IPTV illicite	23 %	n.d.	n.d.	n.d.	n.d.
Modification paramétrage DNS	n.d.	n.d.	n.d.	46 %	n.d.
Usage VPN	n.d.	n.d.	n.d.	57 % (régulier : 30 %)	n.d.
Détails méthodologiques					
Echantillon	4 500 internautes âgés de 15 ans et plus	1053 individus de 15 ans et plus (représentative pop. Français)	2 600 internautes âgés de 15 ans et plus	3 017 internautes âgés de 15 ans et plus	Panel de 25 000 internautes âgés de 2 ans et plus
Date terrain d'enquête	12 mai – 3 juin 2025	23-25 juillet 2025	3-14 juin 2024	21 juin – 23 juillet 2023	Mesure mensuelle

Notes de lecture :
25 % des déclarent avoir des usages illicites pour accéder à des ; 12 % y accèdent en streaming illicite.
48 % des internautes ayant des pratiques illicites ont recours au streaming pour accéder à des biens culturels dématérialisés ou des retransmissions sportives.

6. Indicateurs détaillés et données complémentaires - lutte contre le piratage

a) Lutte contre les sites miroirs

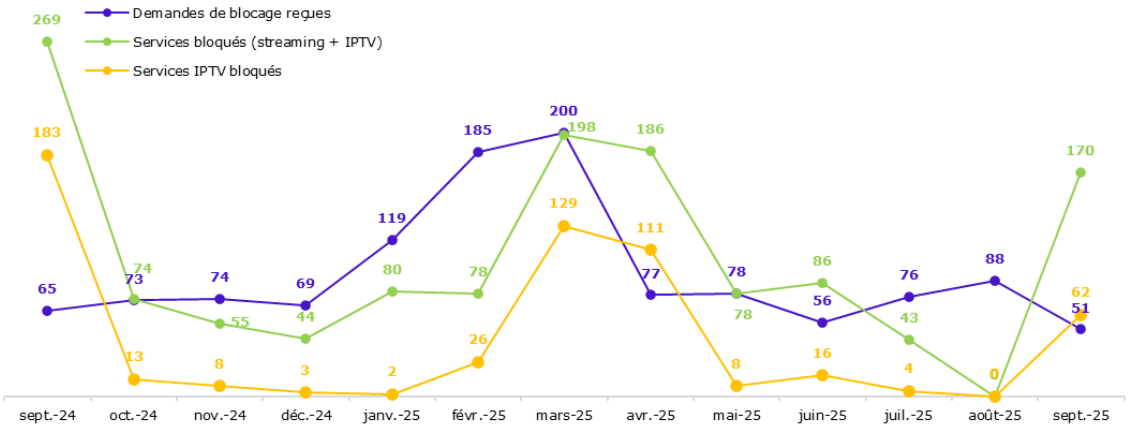
1. Données liées aux mesures prononcées

Tableau 7 : Statistiques blocage (culture)

	2022 (oct. – déc.)	2023	2024	2025 (MAJ : 30 sept.)	TOTAL
Noms de domaine bloqués (sur notification du juge)	408	520	511	688	2 127
Noms de domaine bloqués (sur notification de l'Arcom)	**45**	**549**	**838**	**919**	**2 351**
Dont IPTV	-	*34*	*236*	*358*	638
Dont Live streaming	*45*	*515*	*602*	*561*	1 713
Nombre de blocages mensuels moyen mis en œuvre par l'Arcom	15	46	70	97	
TOTAL blocage	**453**	**1 069**	**1 349**	**1 607**	**4 478**

Source : Arcom

Figure 11 : Evolution mensuelle du nombre de demandes de blocage reçues des titulaires de droits et des services bloqués par l'Arcom



Source : Arcom

2. Décisions judiciaires actualisées par l'Arcom

La durée des mesures pour l'ensemble des décisions ci-dessous est de 18 mois. Ces dernières sont toutes au bénéfice d'ayants droit de l'audiovisuel, l'auteur des transmissions auprès de l'Arcom fut donc systématiquement l'ALPA, pour le compte de ses mandants.

Tableau 8 : Récapitulatif des décisions judiciaires obtenues par Gaumont, Disney Entreprises et Paramount en vue de leur actualisation par l'Arcom (sept 2024-sept 2025)

Titulaire de droits	Date de la décision (TJ de Paris)	N° de décision
Gaumont Disney Entreprises	18/10/2024	RG 24/11901
Gaumont Paramount	15/11/2024	RG 24/13095
Gaumont Disney Entreprises	20/11/2024	RG 24/10914
Gaumont Disney Entreprises	20/11/2024	RG 24/10915
Gaumont Disney Entreprises	20/11/2024	RG 24/10917
Gaumont Paramount	20/11/2024	RG 24/10918
Gaumont Paramount	17/01/2025	RG 24/14587
Gaumont Disney Entreprises	29/01/2025	RG 24/14588
Gaumont Disney Entreprises	19/03/2025	RG 25/01144
Gaumont Paramount	10/04/2025	RG 25/02457
Gaumont Disney Entreprises	10/04/2025	RG 25/02459
Gaumont Disney Entreprises	21/05/2025	RG 25/04877
Gaumont Paramount	19/06/2025	RG 25/07283
Gaumont Disney Entreprises	19/06/2025	RG 25/07281
Gaumont Disney Entreprises	09/07/2025	RG 25/07285
Gaumont Paramount	09/07/2025	RG 25/07286

Source : Arcom

b) Lutte contre les retransmissions sportives illicites

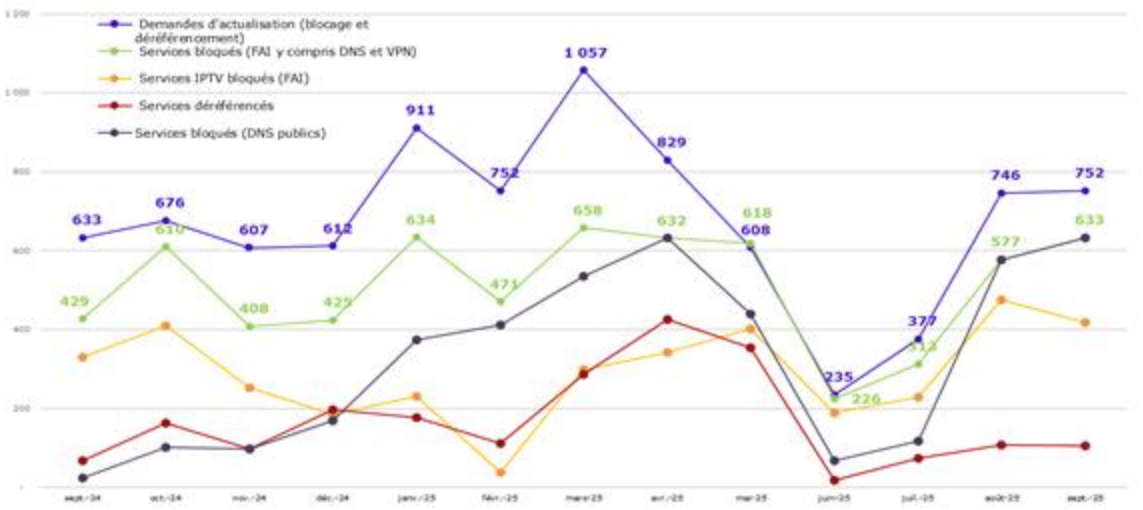
- *Données liées aux mesures prononcées*

Tableau 9 : Statistiques blocages (sport)

	2022	2023	2024	2025 (30 septembre 2025)	Total
Noms de domaine bloqués sur notification du juge	512	542	422	500	**1 976**
Noms de domaine bloqués sur notification de l'Arcom	**772**	**1 544**	**3 794**	**4 762**	**10 872**
Dont IPTV	*16*	*77*	*1 766*	*2 628*	4 487
Dont Live streaming	*756*	*1 467*	*2 028*	*2 134*	6 385
Dont demandes auprès des DNS alternatifs	-	-	439	3 792	4 231
Dont demandes auprès des VPN	-	-	-	494	494
Déréférencements	-	-	1 085	1 663	2 748
Nombre de blocages mensuels moyen mis en œuvre par l'Arcom	70	129	316	529	-
TOTAL blocage (juge + Arcom)	**1 284**	**2 086**	**4 216**	**5 262**	**12 848**

Source : Arcom

Figure 12 : Evolution mensuelle du nombre de demandes de blocage et déréférencement reçues des titulaires de droits et notifiées par l'Arcom (juillet 2024 – septembre 2025)



Source : Arcom

- *Les décisions judiciaires actualisées par l'Arcom*

Tableau 10 : Récapitulatif des décisions judiciaires visant à la protection des compétitions sportives (2024-2025) au 30 septembre 2025

Compétition	Titulaire de droits	Date de la décision	Date de fin de la compétition	N° de décision	Intermédiaires impliqués
F1	**CANAL**	TJ de Paris 18/06/2025	**07/12/2025**	N° RG 25/05133 (**art L. 333-10** + **L.336-2**)	FAI signataires[88] / non signataires (Outre-mer) / Google et Microsoft (moteur de recherche)
				N° RG 25/05129	Cloudflare (DNS alternatifs, CDN, Proxy inverse)
				N° RG 25/05130	Google et Quad 9 (DNS alternatifs)
		TJ de Paris 18/07/2025		N° RG 25/05198	Cyberghost, Proton, Nord VPN (VPN)

[88] FAI signataires de l'accord avec l'Association pour la protection des programmes sportifs (APPS) visant à renforcer la lutte contre la diffusion illicite de contenus sportifs en ligne en date du 18 janvier 2023.

Compétition	Titulaire de droits	Date de la décision	Date de fin de la compétition	N° de décision	Intermédiaires impliqués
MOTO GP	**CANAL**	TJ de Paris 07/05/2025	**16/11 /-25**	N° RG 25/03172 (**art L. 333-10** + **L.336-2**)	FAI signataires / non signataires (Outre-mer) / Google et Microsoft (moteur de recherche)
		TJ de Paris 28/03/2025		N° RG 25/01443	Cloudflare (DNS alternatifs, CDN, Proxy inverse)
		TJ de Paris 11/04/2025		N° RG 25/02092	Quad 9 (DNS alternatifs)
		TJ de Paris 07/05/2025		N° RG 25/03173	Google (DNS alternatifs)
		TJ de Paris 19/06/2025		N° RG 25/01464	Express, Expressco, Cyberghost, Proton, Nord VPN, Surfshark (VPN)
LIGUE 1 LIGUE 2	**LFP**	TJ de Paris 02/08/2024	***25/05/2025***	N° RG 24/55168	FAI signataires
		TJ de Paris 16/01/2025		N° RG 24/15307	Google (moteur de recherche)
				N° RG 25/00226	Microsoft (moteur de recherche)
				N° RG 24/13464	DNS alternatifs (Google, Cloudflare, Quad 9)
		TJ de Paris 15/05/2025		N° RG 24/15054	Cyberghost, Proton, Nord VPN (VPN)
		TJ de Paris 10/07/2025	**24/05/26**	N° RG 25/07645 et 25/08716 (rectificatif)	FAI signataires
		TJ de Paris 17/07/2025		N° RG 25/07644	Google, Cloudflare (DNS alternatifs)
WTA	**BEIN SPORTS**	TJ de Paris 24/01/2025	**10/11/ 2025**	N° RG 25/00148	FAI signataires et non signataires (Outre-mer)
		TJ de Paris 02/05/2025		N° RG 25/03179	Google, Cloudflare, Quad 9 (DNS alternatifs)
		TJ de Paris 18/07/2025		N° RG 25/05968	Cyberghost, Proton, Nord VPN (VPN)
EPL	**CANAL**	TJ de Paris 10/10/2024	**25/05/2025**	N° RG 24/11070	FAI signataires

Compétition	Titulaire de droits	Date de la décision	Date de fin de la compétition	N° de décision	Intermédiaires impliqués
				N° RG 24/11190 (**art L. 333-10**)	FAI non signataires (Outre-mer)
				N° RG 24/11191 (**art L.336-2**)	
				N° RG 24/11181	Microsoft (moteur de recherche)
				N° RG 24/11184	Google (moteur de recherche)
		TJ de Paris 24/10/2024		N° RG 24/11187	Google et Clouflare (DNS alternatifs)
		TJ de Paris 05/12/2024		N° RG 24/12413	Vercara et Quad 9 (DNS alternatifs)
		TJ de Paris 15/05/2025		N° RG 24/14722	Express, Expressco, Cyberghost, Proton, Nord VPN, Surfshark (VPN)
UCL	**CANAL**	TJ de Paris 10/10/2024	**31/05/2025**	N° RG 24/11213	FAI signataires
				N° RG 24/11196 (**art L. 333-10**)	FAI non signataires (Outre-mer)
				N° RG 24/11195 (**art L.336-2**)	
				N° RG 24/11183	Microsoft (moteur de recherche)
				N° RG 24/11185	Google (moteur de recherche)
		TJ de Paris 24/10/2024		N° RG 24/11188	Google et Clouflare (DNS alternatifs)
		TJ de Paris 05/12/2024		N° RG 24/12414	Vercara Quad 9 (DNS alternatifs)
		TJ de Paris 15/05/20s25		N° RG 24/14722	Express, Expressco, Cyberghost, Proton, Nord VPN, Surfshark (VPN)
TOP 14	**CANAL**	TJ de Paris 07/11/2024	**28/06/2025**	N° RG 24/11925	FAI signataires
				N° RG 24/11927 (**art L. 333-10**)	FAI non signataires (Outre-mer)
				N° RG 24/11928 (**art L.336-2**)	

Compétition	Titulaire de droits	Date de la décision	Date de fin de la compétition	N° de décision	Intermédiaires impliqués
				N° RG 24/11929	Microsoft (moteur de recherche)
				N° RG 24/11930	Google (moteur de recherche)
		TJ de Paris 05/12/2024		N° RG 24/12415	DNS alternatifs (Google, Cloudflare,Quad 9, Vercara)
		TJ de Paris 15/05/2025		N° RG 24/14722	Express, Expressco, Cyberghost, Proton, Nord VPN, Surfshark (VPN)
BUNDESLIGA	**BEIN SPORTS**	TJ de Paris 12/11/2024	***17/05/2025***	N° RG 24/57282	FAI signataires et non signataires (Outre-mer)
		TJ de Paris 02/05/2025		N° RG 25/03179	DNS alternatifs (Google, Cloudflare, Quad9)
LIGUE 1	**DAZN**	TJ de Paris 07/11/2024	**17/05/2025**	N° RG 24/12084	FAI signataires et non signataires
		TJ de Paris 05/12/2024		N° RG 24/12416	DNS alernatifs (Google et Cloudflare)
ROLAND-GARROS	**FFT**	TJ de Paris 15/05/2025	***08/06/2025***	N° RG 25/53140	FAI signataires
WIMBLEDON	**BEIN SPORTS**	TJ de Paris 25/06/2025	**13/07/2025**	N° RG 25/07393	FAI signataires et non signataires (Outre-mer)
		TJ de Paris 02/07/2025		N° RG 25/07687	

7. Compléments techniques

a) VPN (réseau privé virtuel)

- *Définition et principe fonctionnement*

Un réseau privé virtuel (VPN) peut être décrit comme un service de sécurité permettant à ses utilisateurs d'accéder à des ressources distantes en ligne, comme s'ils étaient connectés à ces ressources via un réseau local. Le principe du VPN consiste donc à créer une sorte de réseau virtuel qui vient s'intégrer au réseau internet standard, permettant d'isoler (et généralement de chiffrer) les communications entre deux points, par rapport au reste du trafic sur le réseau. Un outil VPN offre donc à ses utilisateurs un niveau de confidentialité accru en ce qui concerne leurs échanges sur internet.

On désigne par le terme « VPN personnel » un service, destiné notamment au grand public, qui crée une sorte de « tunnel » entre le véritable point d'accès à internet d'un utilisateur (son domicile par exemple) et un « point de sortie » (qui peut être situé dans différents pays – les utilisateurs de VPN personnels choisissent ce point de sortie parmi les options offertes par leur fournisseur). On parle de tunnel pour évoquer le fait que le trafic internet de l'utilisateur est chiffré et encapsulé sous forme de paquets de données, selon un protocole sécurisé spécifique, puis acheminé du terminal de l'utilisateur vers les infrastructures du VPN pour y être désencapsulé, et réciproquement. Le « tunneling » est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation du trafic pris en charge par un VPN.

Ce mode de fonctionnement assure un niveau de confidentialité plus élevé que le protocole de chiffrement HTTPS standard, communément utilisé aujourd'hui sur internet. Car si le protocole HTTPS chiffre bien le contenu des échanges sur le Web, il ne masque pas le fait que le terminal d'un internaute est en train de communiquer avec tel ou tel serveur. Grâce au « tunneling » opéré par un VPN, le fournisseur d'accès à internet de l'utilisateur (ou d'autres tiers) ne peut voir cette fois ni quelles données sont envoyées et reçues, ni quels sites ou services en ligne sont consultés par les utilisateurs. En revanche, s'il procédait à une analyse plus ou moins avancée du trafic ou des protocoles utilisés par ses abonnés, le FAI pourrait encore techniquement constater – sans en savoir davantage – que des abonnés utilisent manifestement un VPN.

Vu de l'extérieur, l'utilisateur d'un VPN personnel est perçu comme navigant sur internet depuis le « point de sortie » choisi (et non depuis sa véritable localisation géographique). Sa véritable adresse IP est donc masquée par le VPN. De nombreux services de VPN personnels prétendent ne pas conserver de logs de connexions de leurs utilisateurs, ce qui complique toute attribution ultérieure d'éventuelles activités criminelles à un utilisateur en particulier, y compris en cas de demande des autorités compétentes auprès du fournisseur de VPN.

Le recours à un VPN peut parfois être configuré directement dans les paramètres d'un navigateur à internet, mais aussi au niveau du système d'exploitation du terminal de l'utilisateur ou au niveau du routeur / de la *box* d'un abonné à internet.

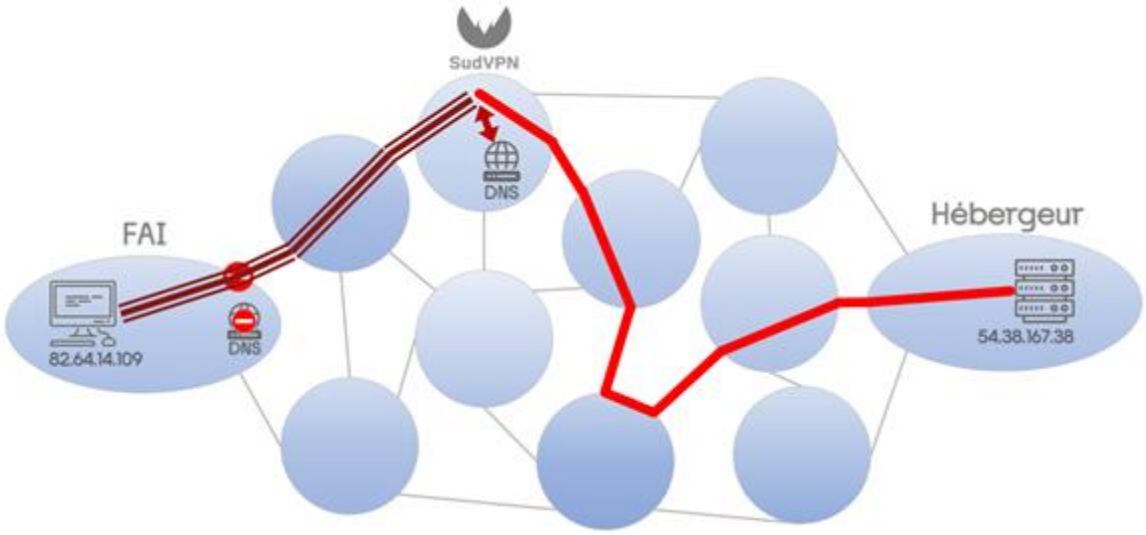
Mais il est également possible pour l'utilisateur d'installer sur son ordinateur ou sur son téléphone une application permettant d'activer ou de désactiver rapidement le VPN, de changer le point de sortie, etc. Les fournisseurs de VPN personnels proposent généralement leur propre application, simple d'utilisation.

L'un des usages possibles des VPN personnels est la consultation de contenus soumis à des restrictions d'accès géographiques : les internautes peuvent donner l'impression d'être connectés à internet depuis un autre pays, pour accéder aux contenus bloqués localement.

Le schéma ci-après illustre le fonctionnement d'un VPN personnel (appelé SudVPN dans cet exemple). Le fait de passer par le tunnel chiffré (entre le lieu de connexion de l'internaute et les installations du VPN) peut permettre de contourner à la fois les mesures de blocage DNS[89] et de blocage IP[90] éventuellement mises en œuvre par le FAI national de l'utilisateur, car ce FAI perd toute visibilité sur ce qui circule dans le tunnel créé par le VPN :

- le VPN personnel utilise en effet généralement son propre service DNS (ou celui d'un tiers), qui n'applique pas forcément de mesures de blocage DNS ;
- le FAI d'origine de l'utilisateur ignore que le trafic chiffré a pour véritable destination une adresse IP censée être bloquée – il n'est donc pas en mesure de stopper le flux en question.

Figure 13 : Schéma simplifié du recours à un VPN personnel pour naviguer sur internet



Source : Arcom

- *Les différents types de VPN (professionnels, personnels payants, personnels gratuits*

Les VPN professionnels

[89] Le blocage DNS consiste à demander aux fournisseurs de service de résolution de nom de domaine (DNS) de refuser d'établir la correspondance entre un nom de domaine (ex : arcom.fr) et l'adresse IP du serveur à contacter sur internet pour accéder au service désiré (ex : l'adresse 217.147.204.82 en ce qui concerne le domaine arcom.fr)

[90] Le blocage IP consiste à demander aux fournisseurs d'accès à internet de bloquer les échanges de données entre leurs abonnés et une adresse IP particulière. En pratique, les paquets de données à destination / provenant de l'adresse IP en question sont déroutés ou détruits par le FAI, au lieu de suivre leur itinéraire normal sur internet.

Les VPN professionnels servent généralement à se connecter à distance au réseau local d'une organisation, afin d'accéder aux ressources internes de cette organisation. Le but premier de ces outils est de sécuriser l'accès aux données et aux services, par exemple pour les employés en télétravail ou en déplacement, ou pour les partenaires d'une entreprise.

Les VPN communautaires

Les individus soucieux de protéger au maximum la confidentialité de leurs échanges en ligne ont aujourd'hui tendance à utiliser des VPN dédiés ou auto-gérés, c'est-à-dire des VPN qu'ils installent et administrent eux-mêmes. Ces systèmes sont plus discrets et moins facilement détectables que les VPN grand public.

Les VPN personnels payants

Les principaux services, tels que NordVPN, ExpressVPN, Surfshark, CyberGhost ou ProtonVPN, offrent comme « point de sortie » sur internet une grande variété de serveurs, situés dans de nombreux pays, et acheminent le trafic internet des utilisateurs vers ces points de sortie sous forme chiffrée. Ces services permettent de contourner les restrictions géographiques et les blocages imposés par les FAI nationaux. Ces fournisseurs proposent presque tous des périodes d'essai gratuites ainsi que des promotions et des tarifs dégressifs.

Les principales caractéristiques des VPN personnels sont généralement les suivantes :

- Implantation dans un pays très protecteur en matière de confidentialité ou peu coopératif sur le plan judiciaire au niveau international ;
- Chiffrement puissant des communications ;
- Absence de « *log* » (registre) des connexions des utilisateurs ;
- Existence de serveurs optimisés pour le téléchargement en pair à pair ou pour le streaming ;
- Dispositifs de sécurité évitant les fuites de données en cas de disfonctionnement (*kill switch*).

Les VPN personnels peuvent être installés et configurés manuellement au niveau des paramètres des navigateurs web ou du système d'exploitation sur les ordinateurs et les appareils mobiles. Mais plus fréquemment, l'installation et l'utilisation de ces services se fait par l'intermédiaire d'applications dédiées, de logiciels ou d'extensions pour navigateurs.

Les VPN personnels gratuits

Sur un plan fonctionnel, les VPN personnels gratuits ont tendance à être moins performants que leurs équivalents payants, et proposent globalement moins de fonctionnalités. Certains logiciels tels que des navigateurs web intègrent par ailleurs des fonctionnalités de VPN (exemple : Opera).

Quelques idées reçues concernant les VPN personnels

Les VPN renforcent la sécurité des connexions et protègent la vie privée des utilisateurs

Dans leurs argumentaires commerciaux, les services de VPN personnels affirment que leurs services assurent la sécurité des connexions et protègent la vie privée des internautes, en évitant que des tiers soient en mesure d'observer leurs activités en ligne. En réalité, l'usage d'un VPN déporte simplement (généralement vers des tiers situés à l'étranger) la question de la confidentialité des échanges. Ainsi, le fournisseur

d'accès à internet national (Bouygues Telecom, Free, Orange, SFR…) d'un utilisateur français de VPN n'a plus de visibilité précise sur ce que font leurs abonnés en ligne, mais d'autres acteurs (les opérateurs de VPN personnels et leurs partenaires) héritent de cette capacité. Or tous les services ne se valent pas, en termes de fiabilité et de sécurité. Les infrastructures d'un VPN, notamment gratuit, peuvent en effet être moins bien protégées que celles d'un FAI français, exposant les utilisateurs à davantage de risques de fuites de données, de piratage, etc. En France, l'ANSSI prévient d'ailleurs l'utilisation d'un VPN gratuit à titre professionnel peut s'avérer moins fiable et moins sûr que d'autres offres proposées par des éditeurs de confiance.

Les VPN n'appliquent pas de filtrage des communications

Les VPN personnels ont longtemps mis en avant le fait de proposer un accès à internet non bridé, non censuré, sans limites. Au cours des dernières années, ces opérateurs ont toutefois complété leur offre d'accès à internet par des fonctionnalités de cybersécurité, protégeant par exemple les utilisateurs face aux sites internet considérés comme dangereux. Le service fourni prend parfois un aspect dual, voire contradictoire. Certains services de VPN personnels garantissent ainsi de pouvoir utiliser en toute discrétion des réseaux pair à pair (P2P) souvent associés au téléchargement illégal de contenus soumis au droit d'auteur, et offrent dans le même temps à leurs utilisateurs des outils de blocage de sites malveillants ou illicites. Autre exemple dual : certains VPN personnels peuvent permettre de contourner le blocage de sites internet pornographiques, mais ils proposent par ailleurs des options permettant le blocage de contenus pour adultes.

- *Les effets sur les outils de régulation nationaux*

Les VPN personnels « brouillent » une partie significative du trafic web aux yeux des FAI nationaux (aujourd'hui impliqués dans la lutte contre les activités illicites en ligne grâce notamment aux mesures de blocage) et aux yeux des autorités nationales.

Le recours aux VPN personnels peut donc servir à contourner effectivement les mesures de blocage et de lutte contre les activités illicites en ligne liées aux missions de l'Arcom.

Tableau 11 : Effets du recours à un VPN personnel sur les mesures de blocage et de lutte contre les activités illicites en ligne

Type de mesure	Effet en cas de recours à un VPN non coopératif
Blocage de type DNS (services portant atteinte au droit d'auteur, streaming sportif, sites pornographiques, etc.)	Contournement du blocage mis en œuvre par les FAI nationaux
Blocage de type IP (streaming sportif)	Contournement du blocage mis en œuvre par les FAI nationaux
Réponse graduée (piratage sur les réseaux pair à pair)	Le FAI national de l'abonné n'est plus directement identifiable
Blocage des médias sous sanctions européennes	Contournement du blocage mis en œuvre par les FAI nationaux
Blocages « Ofac » (propagande terroriste, pédopornographie, actes de barbarie, narcotrafic)	Contournement du blocage mis en œuvre par les FAI nationaux
Vérification de l'âge des visiteurs	Contournement de la mesure si celle-ci ne s'applique que dans certains pays

Source : Arcom

b) DNS (système de nom de domaine)

- *Définition et principe fonctionnement*

Le DNS (*Domain Name System*, ou système de nom de domaine) est un système clé sur internet, en particulier sur le « web ». Il est chargé d'établir la correspondance entre un nom de domaine pleinement qualifié (ex : arcom.fr) et une adresse IP (ex : 217.147.204.82).

Le terme de nom de domaine pleinement qualifié (ou FQDN, *Fully Qualified Domain Name*) désigne techniquement un nom de domaine complet et valide, qui correspond à un « hôte » précis – c'est-à-dire à une machine ou à un serveur bien identifié sur internet.

Par exemple, « www.versailles.fr » ou « achats.versailles.fr » sont bien des FQDN car ils correspondent chacun à un serveur spécifique hébergeant des contenus précis. Le DNS sait traduire ces FDQN en adresses IP. En revanche « www.versailles » (sans le .fr) ou « gouv.fr » ne sont pas des FQDN, car ces expressions sont incomplètes. De même que « abc.versailles.fr » n'est pas non plus un FQDN car, au niveau du DNS, aucune adresse IP n'est spécifiquement associée au sous-domaine « abc » du domaine « versailles.fr ».

Le grand public parle en général de « nom de domaine » pour désigner indistinctement un domaine, un sous-domaine ou un FQDN, alors que les fournisseurs d'accès à internet (FAI) et les gestionnaires de DNS utilisent le terme FQDN. Cette notion de noms de domaines ou de sous-domaines pleinement qualifiés est importante car, du point de vue technique, toute adresse web non valide – c'est-à-dire, ne renvoyant pas à l'adresse IP d'un serveur – est inexploitable.

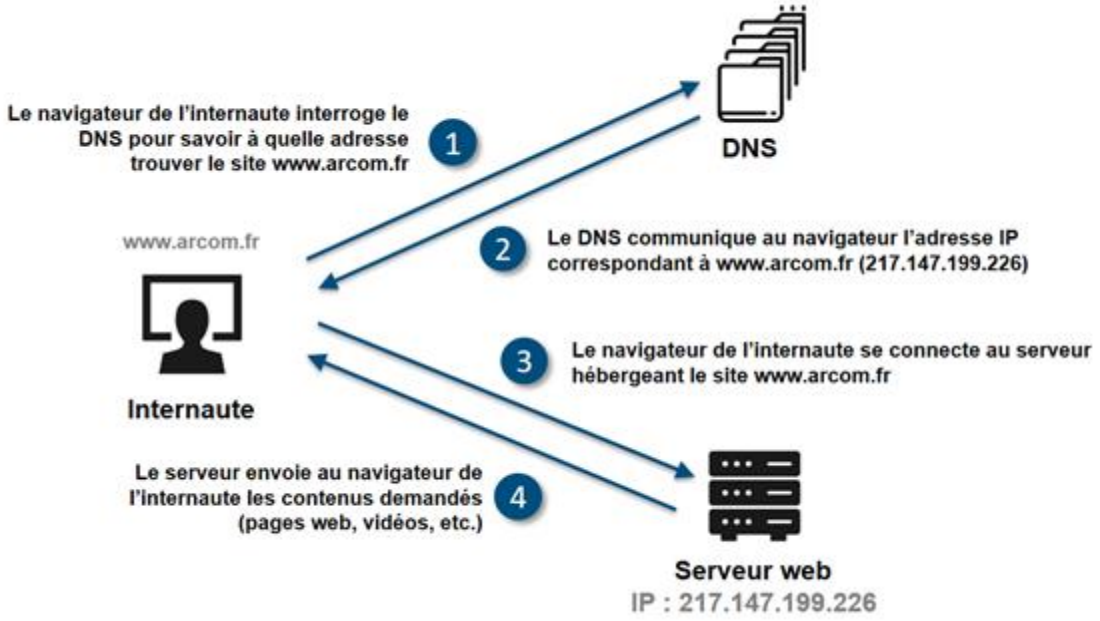
Par analogie, le DNS peut être comparé à une sorte d'annuaire téléphonique. Il associe le nom d'un abonné – *a priori* connu ou mémorisable par les usagers – à un numéro de téléphone. Dans cette analogie :

- le nom de l'abonné correspond au FQDN / nom de domaine du site web ;
- le numéro de téléphone correspond à l'adresse IP du serveur qui héberge le site web.

Un nom de domaine doit idéalement être explicite et facile à mémoriser pour les internautes. Les internautes n'ont en revanche pas besoin de mémoriser l'adresse IP correspondant dans l'annuaire à ce nom de domaine. Cette adresse IP peut d'ailleurs changer au fil du temps, pour des raisons techniques (si l'opérateur du site change de prestataire d'hébergement par exemple). De tels changements sont simplement renseignés par l'opérateur du site dans le DNS (c'est-à-dire dans l'annuaire) et ils restent donc transparents pour les internautes, qui ont juste besoin de retenir le nom de domaine d'un site pour y accéder.

Voici comment fonctionne – de façon simplifiée – le DNS, lorsqu'un internaute cherche à accéder à un site internet :

Figure 14 : Fonctionnement schématique et simplifié du DNS



Source : Arcom

Dans cet exemple, l'internaute souhaite charger la page d'accueil du site de l'Arcom. Il entre donc « www.arcom.fr » dans son navigateur internet. Le navigateur sollicite le DNS pour connaitre l'adresse IP du serveur qui héberge le site www.arcom.fr (1). Le serveur DNS interrogé renvoie l'adresse IP correspondant au nom de domaine www.arcom.fr, telle que connue au moment de la requête (2). Le navigateur de l'internaute se connecte ensuite au serveur web à l'adresse IP indiquée, pour demander un accès à la page d'accueil du site de l'Arcom (3). Le serveur web envoie au navigateur de l'internaute les informations et les contenus demandés (4).

Le DNS repose en réalité sur un ensemble de serveurs interconnectés qui communiquent entre eux pour trouver l'information demandée, à jour : résolveurs récursifs, serveurs racines de noms de domaine, serveurs de noms TLD et enfin de très nombreux serveurs de noms « faisant autorité » (c'est-à-dire qui détiennent en temps réel, et pour un nom de domaine précis, tous ses détails de configuration).

La technique du blocage DNS, souvent utilisée sur internet pour limiter l'accès des internautes à certains sites internet, consiste à contraindre les serveurs DNS d'un fournisseur d'accès à internet à ne pas répondre lorsqu'un utilisateur effectue une demande de résolution pour un nom de domaine interdit. En l'absence de réponse, ou en étant volontairement réorienté vers une mauvaise adresse IP, l'internaute se voit dans l'incapacité de joindre le service demandé.

- *Les DNS publics alternatifs*

Au lieu d'utiliser par défaut le DNS de leur FAI, les internautes peuvent aussi choisir de modifier les paramètres de leur navigateur internet ou de leur système d'exploitation afin de sélectionner un résolveur DNS tiers (ou alternatif). Ces DNS publics alternatifs proposent généralement une fonctionnalité de « DNS sécurisé », ou DoH (pour *DNS over HTTPS*) : ce mode permet de chiffrer les requêtes DNS de l'internaute, qui à l'origine ne sont pas forcément protégées.

La plupart des navigateurs web proposent aujourd'hui une présélection de services alternatifs de DNS sécurisés et publics. Aucune inscription n'est requise pour utiliser ces services et il n'est pas non plus nécessaire de valider des conditions générales d'utilisation ou des dispositions relatives aux données personnelles. Il suffit de choisir un fournisseur de services DNS dans la liste prédéfinie ou d'entrer les coordonnées d'un autre fournisseur que l'internaute souhaite utiliser. L'activation du service est quasi immédiate.

L'opération revient donc pour un internaute à consulter un autre « annuaire » que celui proposé par défaut par son FAI. L'usage des DNS alternatifs est le plus souvent gratuit pour les utilisateurs, bien que certains services optionnels ou personnalisés puissent être payants. Pour l'utilisateur, le recours à un DNS alternatif sécurisé peut être perçu comme un moyen de renforcer la protection de sa vie privée et la confidentialité de ses activités en ligne. Certains DNS alternatifs affirment également être plus performants et rapides que ceux des FAI.

Plusieurs grands acteurs dominent le marché des DNS publics alternatifs, parmi lesquels Google Public DNS (8.8.8.8), Cloudflare (1.1.1.1), Quad9 (9.9.9.9).

Cisco proposait jusqu'en 2024 en France son service OpenDNS, avant d'annoncer son retrait du marché français, en réaction à des demandes de blocage de sites illicites. En 2025, le fournisseur de service de VPN personnel Surfshark a annoncé le lancement de son propre service de DNS public gratuit. D'autres acteurs proposent aussi des DNS publics alternatifs, tel que l'association French Data Network (FDN) qui sont « non censurés » mais dont les performances restent limitées.

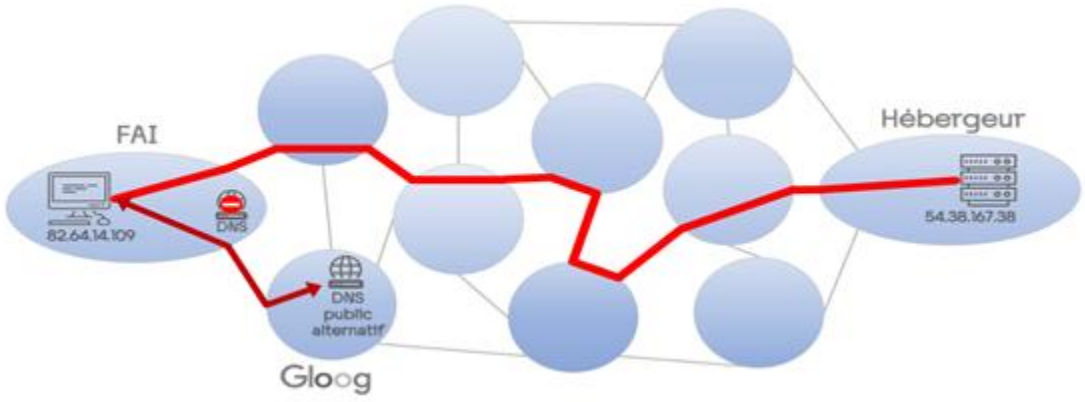
Enfin, en juin 2025, le service DNS4EU a été lancé. Ce projet co-financé par l'UE et supervisé par l'ENISA (agence européenne de cybersécurité) propose un service DNS européen souverain, qui ne collecte pas de données sur ses utilisateurs.

- *Les effets sur les outils de régulation nationaux*

Jusqu'en 2024, les DNS publics alternatifs n'étaient pas concernés par les demandes judiciaires et administratives de blocage : quiconque optait pour ces services pouvait échapper aux mesures de blocage.

Le schéma ci-après illustre le contournement d'une mesure de blocage implémentée au niveau du DNS du FAI, par le recours au DNS alternatif (ici nommé « Gloog »).

Figure 15 : Schéma simplifié du recours à un DNS public alternatif pour naviguer sur internet



Source : Arcom

En revanche, le recours à un DNS public alternatif ne permet pas de contourner le blocage IP.

Le tableau ci-dessous détaille l'impact du recours à un DNS public alternatif (n'appliquant pas les mesures de blocage) sur différents types de mesure.

Tableau 12 : Effets du recours à un DNS public alternatif sur les mesures de blocage et de lutte contre les activités illicites en ligne

Type de mesure	Effet en cas de recours à un DNS non coopératif
Blocage de type DNS (services portant atteinte au droit d'auteur, streaming sportif, sites pornographiques, etc.)	Contournement du blocage mis en œuvre par les FAI nationaux
Blocage de type IP (streaming sportif)	Le blocage mis en œuvre par les FAI nationaux reste efficace
Réponse graduée (piratage sur les réseaux pair à pair)	L'abonné à internet reste identifiable lorsqu'il partage des contenus en P2P
Blocage des médias sous sanctions européennes	Contournement du blocage mis en œuvre par les FAI nationaux
Blocages « Ofac » (propagande terroriste, pédopornographie, actes de barbarie, narcotrafic)	Contournement du blocage mis en œuvre par les FAI nationaux
Vérification de l'âge des visiteurs	Le système de contrôle reste actif car la géolocalisation de l'internaute ne change pas

Source : Arcom

c) IPTV illicite

- Définition et principe fonctionnement

L'IPTV (*Internet Protocol Television*) est une technologie qui permet la diffusion de contenus audiovisuels par le biais d'internet. Ce standard a d'abord été exploité par les fournisseurs d'accès à internet (FAI) qui ont alloué à ce service une partie de leur bande passante afin de garantir à leurs abonnés une diffusion de qualité des flux télévisuels, *via* leurs boitiers TV. On parle dans ce cas d'IPTV « gérée » car ce service est mis en œuvre et contrôlé par les FAI, sur leurs propres infrastructures (le service n'est ainsi accessible que par leurs abonnés).

Depuis plusieurs années, grâce au développement du très haut débit, de nombreux services audiovisuels en direct ou à la demande ont vu jour et ont également recours à la technologie IPTV pour acheminer leurs signaux directement jusqu'aux consommateurs. On parle d'auto-distribution ou encore de services « OTT » (*over-the-top*) c'est-à-dire accessibles cette fois par tout internaute en utilisant sa connexion à internet classique. Les entreprises offrant de tels services (groupes de télévision traditionnels, Molotov, Roku…) proposent généralement des applications dédiées pour accéder aux programmes. Ces applications proposent d'ailleurs souvent un accès aux flux TV en direct, en différé, ainsi que des programmes à la demande.

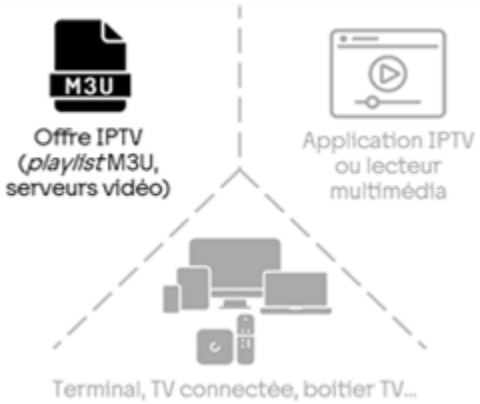
Au côté de ces offres légales, se sont développées depuis la fin des années 2010 des offres IPTV illégales, à l'échelle internationale. Ces offres sont constituées aujourd'hui de milliers voire de dizaines de milliers de chaines TV du monde entier, rediffusées sans autorisation et accessibles en direct, ainsi que des dizaines de milliers de contenus à la demande[91] (films, séries TV, contenus exclusifs Netflix / Amazon Prime Video / Disney+ / Canal+, etc.). Par glissement sémantique, le grand public évoque souvent ces services illicites sous le simple nom d'IPTV.

Les « IPTV illicites » s'apprécient à travers trois composantes qui sont chacune indispensable pour faire fonctionner le service :

- une offre IPTV : cette offre prend généralement la forme d'une liste de lecture (*playlist*) pointant vers des serveurs de streaming qui rediffusent les chaines TV en direct ou hébergent les contenus à la demande ;
- un logiciel : il s'agit généralement d'une application IPTV conçue pour afficher les menus des programmes et lire les flux vidéo, ou d'un lecteur multimédia capable de lire les playlists IPTV ;
- un terminal : ce support peut être un ordinateur, un *smartphone* ou tablette, une télévision connectée, une *box* (boitier TV relié à une télévision) ou une clé HDMI branchée sur TV…

[91] https://www.arcom.fr/sites/default/files/2024-11/Arcom-support-presentation-conference-bilan-antipiratage-sportif-2024_1.pdf

Figure 16 : représentation simplifiée des trois composantes de l'IPTV illicite



La plupart des offres IPTV illicites sont compatibles avec de nombreuses applications et peuvent être visionnées sur une multitude d'appareils. L'accès au service illicite se fait à partir d'identifiants personnels envoyés aux utilisateurs dès qu'ils ont payé leur abonnement. Pour accéder aux flux IPTV, il suffit généralement de trois éléments : un nom d'utilisateur, un mot de passe et le nom d'un serveur d'authentification auquel se connecter avec ces identifiants.

Les fournisseurs envoient également parfois à leurs abonnés un lien « M3U » d'accès direct à la *playlist*. Concrètement, cette liste de lecture standardisée référence l'ensemble des chaines et contenus disponibles, ainsi que des URL correspondant à chacun des contenus proposés. Ce lien M3U intègre lui-même les identifiants personnels de l'abonné, de sorte que la connexion au service peut se faire directement, à partir de ce seul lien hypertexte. La *playlist* est le plus souvent constituée d'ensembles de chaines et de contenus regroupés par pays d'origine ou par thématique. Une même chaine TV peut figurer dans plusieurs bouquets au sein d'une offre IPTV. Les utilisateurs naviguent ainsi à travers les menus en sélectionnant un bouquet (ou une catégorie), puis une chaine TV (ou un programme à la demande). Les contenus s'affichent ensuite à l'écran et l'abonné peut alors contrôler à sa guise le mode de lecture et de visionnage au moyen d'une télécommande virtuelle ou physique.

- *Un écosystème complexe*

Pour l'utilisateur, l'offre IPTV est relativement simple à utiliser. Cette offre peut d'ailleurs être qualifiée de service pirate « tout-en-un » : pour un abonnement unique, l'utilisateur a accès à l'ensemble des contenus en direct ou à la demande du marché. Pour autant, l'infrastructure de ces services repose sur un écosystème composé de multiples couches, faisant intervenir différentes activités et de nombreux acteurs.

Les différents acteurs

A l'origine, les contenus rediffusés par les offres IPTV illicites doivent être captés – en temps réel pour ce qui concerne les chaines TV. Certains opérateurs se spécialisent donc dans la récupération des flux légitimes (à travers des accès légaux aux contenus vidéo, ou au moyen de comptes d'utilisateurs piratés afin d'éviter d'être identifiés). Ces flux sont alors réencodés puis envoyés, éventuellement par lots, à des serveurs de streaming qui rediffuseront eux-mêmes ces flux à des abonnés ou à d'autres serveurs de streaming – relayant ainsi les programmes de manière arborescente, vers différents réseaux de

distribution. Un nombre assez limité de « têtes de réseau » peuvent ainsi alimenter une grande quantité d'offres IPTV sous-jacentes, mises sur le marché.

Les offres IPTV proposant des dizaines de milliers de chaines sont en général constituées d'une agrégation de multiples sources de flux provenant de différents prestataires spécialisés dans la captation des contenus. Certains opérateurs se concentrent donc sur la constitution des offres agrégées. Ils s'assurent de la disponibilité continue des programmes captés puis rediffusés illégalement. Leur objectif est de disposer d'un catalogue de flux et de contenus en permanence à jour. Ils gèrent également l'infrastructure nécessaire à la rediffusion de ces contenus.

Cette infrastructure peut se constituer de parcs (ou de fermes) de serveurs de streaming, rediffusant chacun un nombre limité de chaines ou de contenus, et dont l'organisation peut être ajustée en fonction de la demande ou de contraintes techniques. On peut même parler de réseaux dédiés de diffusion de contenus (ou CDN, *content delivery network*) lorsque ces infrastructures sont particulièrement sophistiquées, afin d'optimiser dynamiquement l'accès aux flux vidéo en fonction par exemple de la localisation des utilisateurs, de la charge des serveurs, pour contourner d'éventuelles mesures de blocage, etc.

Viennent ensuite les fournisseurs, qui peuvent commercialiser des offres en gros auprès de revendeurs et de détaillants. En pratique, ces derniers achètent auprès des grossistes un volume de « crédits » (un crédit correspondant généralement à un abonnement actif à un instant t) qu'ils vont ensuite revendre sous forme d'abonnements aux utilisateurs finaux – pour une semaine, 3 mois, 6 mois, un an…

Les fournisseurs exploitent des serveurs d'authentification afin de gérer les accès aux offres illicites. Ces serveurs d'authentification sont au cœur du système puisqu'ils sont connectés à la fois aux serveurs de streaming (qui rediffusent les contenus et programmes piratés), aux revendeurs et détaillants (qui gèrent leurs quotas de crédits, les offres souscrites et leur base d'abonnés) et aux utilisateurs finaux (qui accèdent aux programmes auxquels ils se sont abonnés, après s'être dûment identifiés *via* le serveur d'authentification).

Gravitent enfin autour de ces acteurs les développeurs d'applications IPTV ainsi que des producteurs de boitiers et de clés électroniques bon marché, à connecter à des téléviseurs afin de profiter de l'offre IPTV sur grand écran (ces *box* TV ou sticks HDMI peuvent d'ailleurs être plus ou moins « préconfigurés », c'est-à-dire livrés avec certaines applications préinstallées).

Un même acteur peut en réalité assurer un ou plusieurs des rôles ci-dessus : certains fournisseurs proposent par exemple à la fois des abonnements à l'unité (à des utilisateurs finaux) ou en gros (à des revendeurs) et ils peuvent coupler leur offre avec la vente en option de *box* TV ou de clé HDMI prêtes à l'emploi.

Les types d'offres

Les offres IPTV illicites sont commercialisées avec ou sans équipement (*box* TV, stick HDMI). Le prix de l'équipement est généralement fixe et doit être payé intégralement à l'achat. Le prix de l'abonnement dépend quant à lui de la durée de l'abonnement choisi. Il est dégressif : plus on s'engage sur un nombre important de mois, moins le coût par mois est élevé. Mais le prix correspondant à l'intégralité de l'abonnement doit le plus souvent être prépayé au moment de la souscription. A la fin de la période d'abonnement

prépayé, il est possible de prolonger l'abonnement en rachetant un forfait de la durée de son choix.

Ces offres sont proposées sur différents points de vente :

- site internet dédié : les vendeurs d'abonnements IPTV disposent ici de leur propre site vitrine sur le web. Les offres sont commercialisées sans intermédiaire. Les abonnés choisissent l'offre de leur choix (et éventuellement un appareil électronique complémentaire) et paient en ligne. Ils reçoivent aussitôt leurs identifiants de connexion (et leur équipement par voie postale) ;
- plateformes de commerce électronique : bien que la vente d'offres IPTV illicites soit interdite sur la plupart des plateformes de e-commerce, il n'est pas rare d'en trouver. Les vendeurs utilisent différents subterfuges pour camoufler la nature illicite de leur offre. Ils proposent par exemple des boitiers électroniques et précisent discrètement que l'appareil est fourni avec un « service » valable pour un an. D'autres proposent de fausses options associées à la *box* (par exemple 1, 3, 6 ou 12 Go de « RAM » complémentaire, mais on comprend en lisant entre les lignes que l'option correspond en fait au nombre de mois d'abonnements IPTV inclus) ;
- une fois leur base de clients constituée, les vendeurs d'abonnement passent souvent par les réseaux sociaux et les messageries instantanées pour assurer le service après-vente et pour proposer à leurs clients le renouvellement de leurs abonnements (évitant ainsi d'avoir à s'appuyer sur une plateforme intermédiaire qui se rémunère en prélevant un pourcentage du montant des ventes). Ce mode de communication est d'ailleurs plus discret que les sites web vitrines ou que les annonces postées sur les plateformes de e-commerce. Les services chargés de lutter contre le piratage ont donc plus de mal à découvrir et à limiter ce genre de transactions ;
- on observe enfin dans certaines villes des « revendeurs de quartier » qui s'appuient sur le bouche-à-oreille pour commercialiser les offres IPTV dans leur entourage en proposant un service d'installation à domicile. L'abonné a ainsi la garantie que le service sera fonctionnel, même s'il n'est pas familier avec l'installation d'*apps* IPTV, avec la configuration de clés HDMI ou encore avec la manipulation de *playlists* M3U.

- *Les problématiques annexes et les risques pour les utilisateurs*

Certaines offres IPTV illicites proposent des contenus inappropriés pour le jeune public, ainsi que des chaines TV interdites. Certains services incluent en effet des contenus pornographiques accessibles sans contraintes – les fonctionnalités de contrôle parental parfois évoquées dans les argumentaires publicitaires semblent en réalité inexistantes ou ne sont pas activées par défaut.

Certains bouquets de chaines proposées dans les offres IPTV incluent les programmes des chaines TV contrôlées par des groupes terroristes, ou encore des chaines de télévision russes actuellement sous sanctions européennes (la diffusion ou la rediffusion de leurs contenus est interdite en Europe tant que les sanctions s'appliquent). Si ces programmes restent minoritaires par rapport à l'ensemble des contenus proposés dans les offres IPTV illicites, ils n'en demeurent pas moins problématiques au regard du droit (mais sans lien en l'occurrence avec les questions de propriété intellectuelle).

Les internautes s'exposent par ailleurs à différents risques numériques ou informatiques, lorsqu'ils s'abonnent à des services IPTV illicites. Parmi ces risques :

- La compromission de données personnelles et bancaires : les utilisateurs achetant directement un abonnement IPTV, auprès d'un revendeur ou sur un site vitrine, doivent fournir leur coordonnées personnelles et leurs données bancaires. Des vendeurs malintentionnés pourraient être tentés de réutiliser ces informations. Ces données, souvent peu protégées, peuvent également fuiter ou être piratées par des tiers. De même, les utilisateurs de *box* IPTV ou d'applications non officielles risquent de voir les identifiants personnels de leurs comptes Netflix, Amazon, Apple+, etc. interceptés et piratés ;

- Les failles de sécurité sur les équipements et applications : les équipements bon marché prétendent souvent disposer d'un système d'exploitation à jour. En réalité, ils fonctionnent fréquemment avec un système d'exploitation non officiel, dépassé, non sécurisé et ne bénéficiant pas de mises à jour régulières. Ces appareils peuvent par conséquent être victimes d'attaques informatiques et leur utilisation sur un réseau domestique comporte des risques importants en matière de cybersécurité ;

  Les non-conformités aux normes (notamment électriques) : l'origine des appareils électroniques vendus sous marque blanche, pour quelques euros, est bien souvent incertaine. Leur compatibilité avec les normes européennes n'est pas garantie (y compris en termes de normes électriques) et les mentions légales ainsi que la désignation des producteurs et importateurs sont souvent fantaisistes ou imprécises ;

- La présence de programmes potentiellement malveillants : des analyses techniques, portant depuis 2023 sur les systèmes d'exploitation et sur les applications généralement utilisées sur les boitiers IPTV, ont mis en lumière la présence de programmes malveillants voire nuisibles sur ces équipements, agissant à l'insu des utilisateurs. Des tiers peuvent en effet, à travers des systèmes de « *command and control* » utiliser les appareils et les connexions internet des utilisateurs pour commettre des fraudes en ligne voire pour mener des attaques informatiques, ou pour permettre à des tiers de naviguer anonymement sur internet par l'entremise des boitiers connectés. Une plainte, déposée par Google en 2025 aux Etats-Unis, évoque par exemple l'existence de plusieurs millions de boitiers potentiellement infectés à travers le monde par le programme malveillant surnommé BadBox.

@Arcom