

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

Annexes

Etude rédigée avec la collaboration de Carole Hentzgen,
rapporteuse


01/12/2025

Sommaire

Annexes.....	4
1. Lettre de mission	4
2. Textes juridiques en vigueur	6
3. Propositions de loi et amendements	17
4. Usages du RSN dans le cadre de la lutte contre le piratage	22
5. Comparaison des principaux indicateurs relatifs aux usages illicites	26
6. Indicateurs détaillés et données complémentaires - lutte contre le piratage	28
7. Compléments techniques	35

Annexes

1. Lettre de mission

 <p>ASSEMBLÉE NATIONALE</p>	<p>RÉPUBLIQUE FRANÇAISE LIBERTÉ - ÉGALITÉ - FRATERNITÉ</p>
<p>COMMISSION DES AFFAIRES CULTURELLES ET DE L'ÉDUCATION</p> <p>La Présidente</p>	<p>Monsieur Martin AJDARI Président de l'Autorité de régulation de la communication audiovisuelle et numérique 9, rue Brahms – CS 12603 71131 Paris cedex 12</p>
<p>Paris, le 2 juin 2025</p>	
<p>Réf : 20250602-R1</p>	
<p>Monsieur le Président,</p>	
<p>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 « <i>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</i> ».</p>	
<p>Cette demande, qui constitue, semble-t-il, la première application de cette disposition législative, viserait à :</p>	
<ul style="list-style-type: none">– 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 nationale¹ ;– 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 ;	
<p>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.</p>	
<p>126, rue de l'Université - 75355 PARIS 07 SP - Tél : 01 40 63 65 92</p>	

– 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 comparait 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.

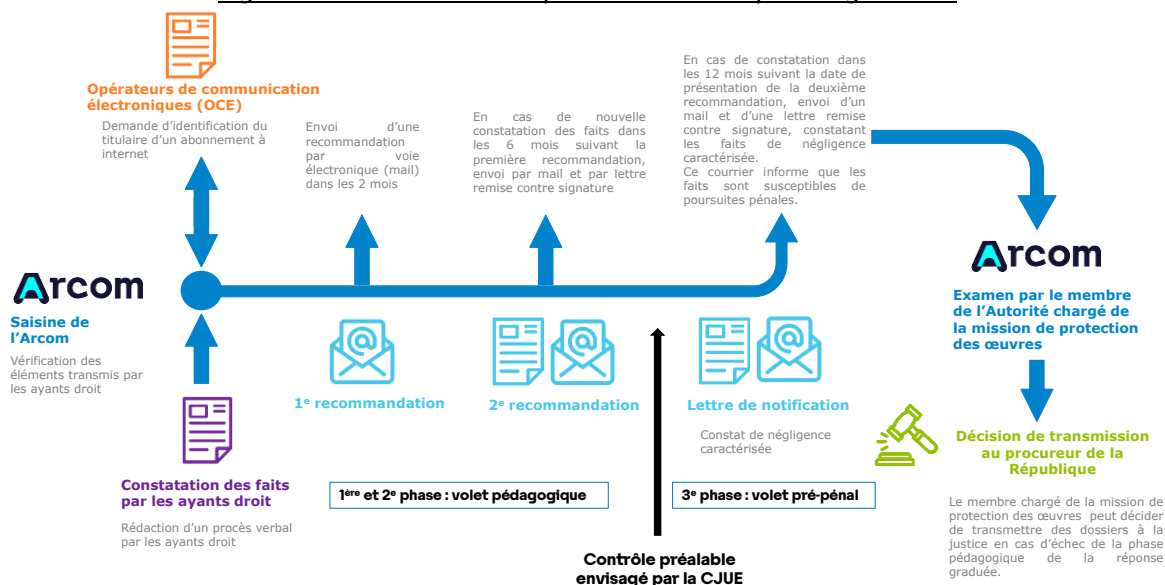
À tout moment, le service de communication au public en ligne peut demander à l'autorité d'être retiré de la liste mentionnée au I dès lors qu'il justifie du respect des droits d'auteur et des droits voisins. L'autorité statue sur cette demande par une décision motivée rendue après une séance publique 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 1 : 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)¹ 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 obligations² du texte.

a) Signalements et injonctions d'agir s'agissant de la diffusion de contenus culturels et de la retransmissions illicites d'événements 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* »³ 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 événement sportif.

Le traitement des signalements doit être réalisé « *en temps opportun de manière diligente, non arbitraire et objective* »⁴. 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

¹ 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).

² 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.

³ Article 16 du RSN, paragraphe 1.

⁴ 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 autres⁵. 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'événements sportifs, ni distinguer selon que l'événement est diffusé en direct ou qu'il s'agit d'une rediffusion.** A noter que les modèles harmonisés de rapport de transparence, qui deviendront obligatoires⁶ à compter de février 2026 pour les actions de modération entreprises à partir du 1^{er} 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 ;

⁵ 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).

⁶ 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 :
 - o dans certains rapports, la propriété intellectuelle n'est pas une catégorie identifiée amenant à des mesures de modération proactives (Tik Tok et Snapchat) ;
 - o 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) ;
 - o 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) ;
 - o 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 2^e 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'événements 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**⁷;
- 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 X⁸ 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'évènement), 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.

⁷ En réalité, les plateformes parlent de « Copyright ».

⁸ 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 boîtier 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 boîtiers ou des applications sur TV connectée, s'avère donc nécessaire pour mesurer dans leur globalité ces usages.

Tableau 1 : 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

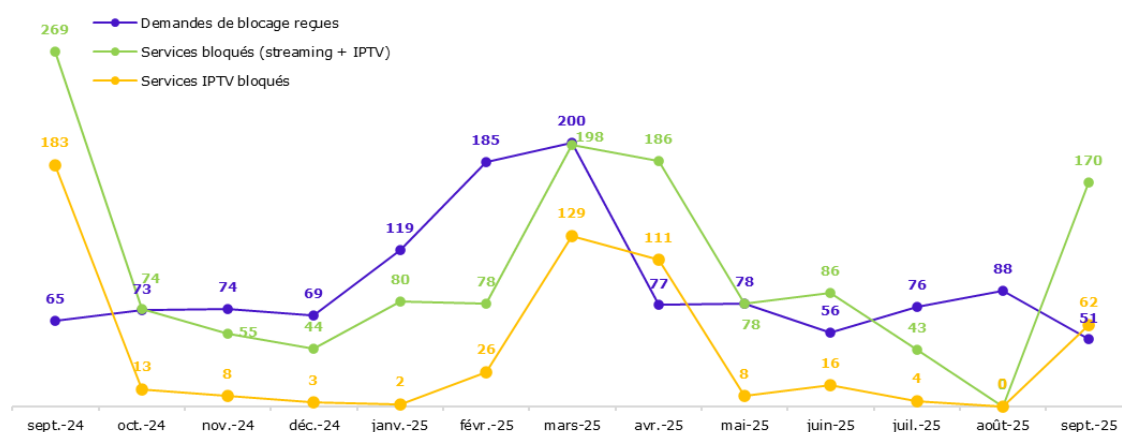
1. Données liées aux mesures prononcées

Tableau 2 : 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 2 : 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 3 : 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

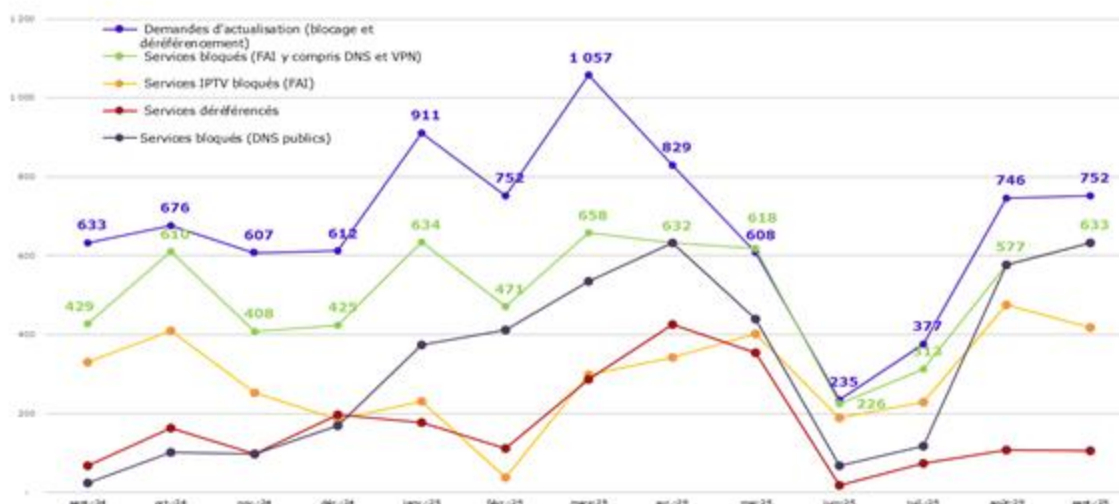
- *Données liées aux mesures prononcées*

Tableau 4 : 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
<i>Dont IPTV</i>	16	77	1 766	2 628	4 487
<i>Dont Live streaming</i>	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 3 : 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 5 : 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 ⁹ / 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)
				N° RG 25/05198	Cyberghost, Proton, Nord VPN (VPN)

⁹ 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 15/05/2025		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 alternatifs (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.

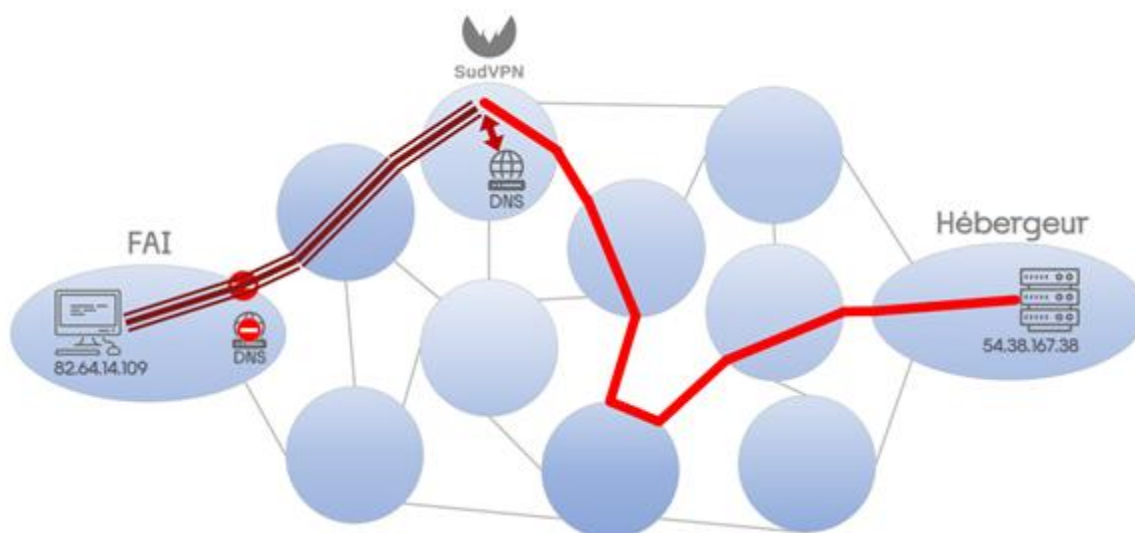
Mais il est également possible pour l'utilisateur d'installer sur son ordinateur ou sur son téléphone une application permettant d'activer ou de désactiver rapidement le VPN, de changer le point de sortie, etc. Les fournisseurs de VPN personnels proposent généralement leur propre application, simple 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 DNS¹⁰ et de blocage IP¹¹ 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 4 : Schéma simplifié du recours à un VPN personnel pour naviguer sur internet



Source : Arcom

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

¹⁰ 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)

¹¹ 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 dérivés ou détruits par le FAI, au lieu de suivre leur itinéraire normal sur internet.

Les VPN professionnels

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 dysfonctionnement (*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 6 : 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 FQDN en adresses IP. En revanche « www.versailles » (sans le .fr) ou « gov.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.

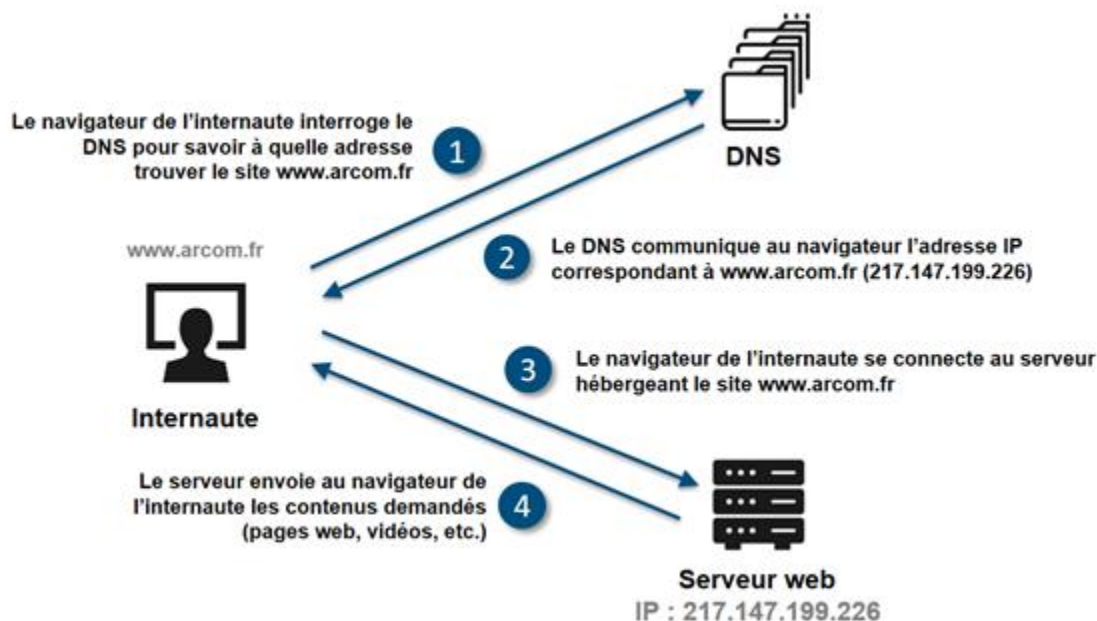
Par analogie, le DNS peut être comparé à une sorte d'annuaire téléphonique. Il associe le nom d'un abonné – *a priori* connu ou mémorisable par les usagers – à un numéro de téléphone. Dans cette analogie :

- 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 5 : 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 connaître 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.

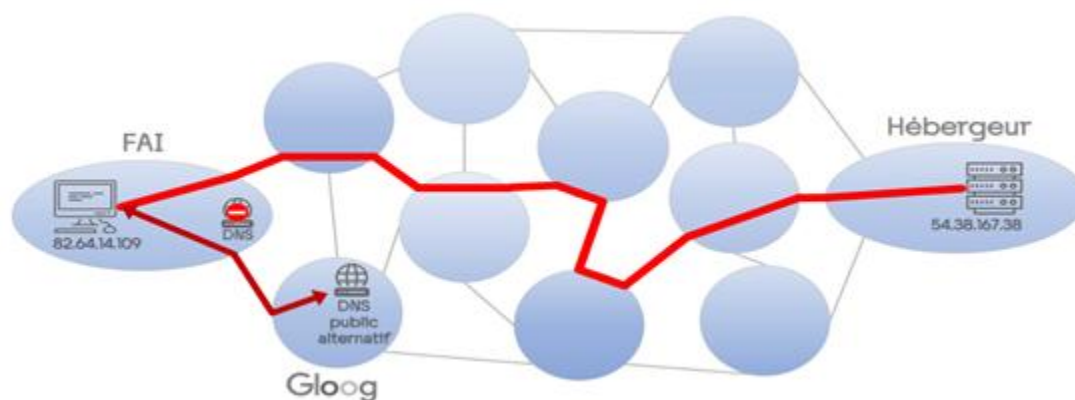
Enfin, en juin 2025, le service DNS4EU a été lancé. Ce projet co-financé par l’UE et supervisé par l’ENISA (agence européenne de cybersécurité) propose un service DNS européen souverain, qui ne collecte pas de données sur ses utilisateurs.

- *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 6 : 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 7 : 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 boîtiers 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.

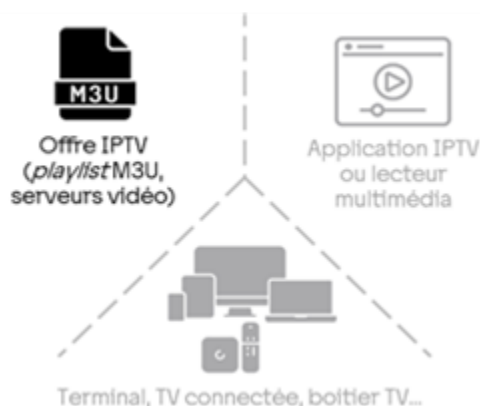
Au côté de ces offres légales, se sont développées depuis la fin des années 2010 des offres IPTV illégales, à l'échelle internationale. Ces offres sont constituées aujourd'hui de milliers voire de dizaines de milliers de chaînes TV du monde entier, rediffusées sans autorisation et accessibles en direct, ainsi que des dizaines de milliers de contenus à la demande¹² (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 chaînes 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* (boîtier TV relié à une télévision) ou une clé HDMI branchée sur TV...

¹² https://www.arcom.fr/sites/default/files/2024-11/Arcom-support-presentation-conference-bilan-antipiratage-sportif-2024_1.pdf

Figure 7 : 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 chaînes 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 chaînes et de contenus regroupés par pays d'origine ou par thématique. Une même chaîne 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 chaîne 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 chaînes 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 chaînes 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 chaînes 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 boîtiers 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 boîtiers 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 chaînes 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 chaînes proposées dans les offres IPTV incluent les programmes des chaînes TV contrôlées par des groupes terroristes, ou encore des chaînes 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 boîtiers 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 boîtiers connectés. Une plainte, déposée par Google en 2025 aux Etats-Unis, évoque par exemple l'existence de plusieurs millions de boîtiers potentiellement infectés à travers le monde par le programme malveillant surnommé BadBox.

