

Stratégies de lutte **contre** le piratage

DES CONTENUS CULTURELS ET SPORTIFS
EN FRANCE ET À L'INTERNATIONAL

ANALYSE • RAPPORT DE VEILLE INTERNATIONALE 2019 - 2020



Hadopi

Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet

SOMMAIRE

Page 5

LA MÉTHODOLOGIE

Page 6

1^{RE} PARTIE ANALYSE

I - LES MESURES DE BLOCAGE VISANT LES SITES ILLICITES ET LEURS DIFFÉRENTS CHEMINS D'ACCÈS

Page 7

● 1.1 Une offre illicite de contenus culturels et sportifs diverse et évolutive

Page 12

● 1.2 La consolidation des injonctions judiciaires ou administratives de blocage

Page 13

● 1.3 La lutte contre les contournements des mesures de blocage

II - LA NÉCESSAIRE MOBILISATION DE L'ENSEMBLE DES ACTEURS DU NUMÉRIQUE

Page 22

● 2.1 L'implication des différents intermédiaires dans la lutte contre le piratage

Page 32

● 2.2 L'implication des plateformes de partage de contenus en ligne

III - LA RESPONSABILISATION DES INTERNAUTES

Page 38

● 3.1 Les dispositifs visant les internautes qui partagent des œuvres sur les réseaux pair à pair

Page 40

● 3.2 La sensibilisation du public

Page 44

2^E PARTIE FICHES DESCRIPTIVES PAR PAYS

Page 45
Page 46
Page 52
Page 53
Page 58
Page 61
Page 63
Page 67
Page 69
Page 73
Page 78
Page 79
Page 84
Page 94
Page 103
Page 107

● Afrique du Sud
● Allemagne
● Argentine
● Australie
● Belgique
● Brésil
● Canada
● Chine
● Corée du Sud
● Danemark
● Égypte
● Espagne
● États-Unis
● France
● Grèce
● Inde

Page 111
Page 114
Page 120
Page 123
Page 126
Page 128
Page 130
Page 134
Page 137
Page 140
Page 149
Page 152
Page 154
Page 157
Page 159
Page 161

● Irlande
● Italie
● Japon
● Lituanie
● Mexique
● Nouvelle-Zélande
● Pays-Bas
● Pérou
● Portugal
● Royaume-Uni
● Russie
● Singapour
● Suède
● Suisse
● Taïwan
● Vietnam

LA MÉTHODOLOGIE

La veille internationale est réalisée de manière continue par la Direction des affaires juridiques, européennes et internationales de l'Hadopi depuis 2011 et fait l'objet pour la troisième fois d'une publication dédiée.

Elle a pour objectif d'interroger les différents modèles de lutte contre le piratage mis en place à l'étranger, de partager les meilleures pratiques et d'éclairer les pouvoirs publics français, notamment en vue d'un renforcement de l'action publique en faveur de la protection des droits sur internet.

Dans l'objectif d'offrir davantage de visibilité aux différentes régions du monde, pour la première fois, 32 pays ont été analysés (au lieu de 23 pour la précédente édition), y compris la France, qui fait l'objet d'une fiche créée à l'attention de notre lectorat à l'international. Chacune des fiches intègre des données chiffrées, obtenues auprès de la société britannique MUSO, relatives aux visites sur les services illicites proposant des contenus culturels (musique/films/séries/logiciels (jeux inclus)/édition) pour les trois principaux modes d'accès (*streaming*, téléchargement direct, pair à pair). MUSO fournit des indicateurs globaux concernant les pratiques contrefaisantes, dans différents pays du monde, à partir de données de trafic fournies par SimilarWeb. Ces chiffres sont utilisés dans le présent rapport de façon à disposer de données comparables entre les différents pays étudiés, y compris la France.

Le rapport de veille internationale comporte d'une part une analyse des points saillants et des enjeux actuels de la lutte contre le piratage dans le monde, qui évoque les dispositifs nationaux les plus emblématiques et, d'autre part, des annexes comportant des fiches descriptives détaillées pour chacun des pays étudiés, lesquelles présentent les dispositifs juridiques qui y sont en vigueur ou les projets de réformes qui y sont discutés.

L'analyse est essentiellement réalisée à partir des éléments mis en évidence dans les fiches, lesquelles font l'objet d'une actualisation périodique, couvrant ici la période de janvier 2019 à janvier 2021, grâce à une veille sur internet et à des échanges avec le réseau de contacts locaux de l'Hadopi.

Les informations obtenues résultent ainsi tant de documents publics (articles de presse, jurisprudence, textes de loi, etc.) que de documents qui nous ont été transmis par un réseau d'interlocuteurs mêlant acteurs publics institutionnels et acteurs du secteur privé. Ce réseau de contacts a pu être noué et renforcé au fil des ans à partir des travaux de veille de l'Hadopi concernant les actualités en matière de lutte contre le piratage (rapports chiffrés, analyses juridiques, prises de positions publiques, etc.), et dans certains cas avec l'appui des ambassades ou consulats français.

Les informations collectées dans le cadre de notre veille ont été vérifiées et complétées, chaque fois que cela a été possible, par un nombre important d'entretiens avec des interlocuteurs locaux qualifiés. Il n'a cependant pas toujours été possible d'obtenir des informations aussi précises qu'attendu pour chacun des pays étudiés.

Il est à noter que, compte tenu de la barrière de la langue et des différences de systèmes juridiques, les fiches sont susceptibles de comporter des approximations ou des erreurs de compréhension.

1^{RE} PARTIE

ANALYSE

La complexification de l'écosystème du piratage sur internet, qui s'accompagne d'une facilité de contournement des décisions de justice et d'une prolifération des acteurs impliqués, mobilise l'ensemble des pouvoirs publics en Europe et à l'international dans la recherche de dispositifs de lutte diversifiés et modernisés.

Consciente du caractère essentiel de la dimension internationale des solutions de lutte contre le piratage et de l'importance d'une approche comparatiste pour se nourrir des expériences étrangères, l'Hadopi s'est rapidement saisie de cette mission de veille et de collaboration internationale et a, dans ce cadre, multiplié les collaborations fructueuses tant avec ses homologues étrangers qu'avec les organisations en charge du piratage à l'étranger.

Cet exercice de veille des initiatives engagées à l'étranger, initié il y a désormais dix ans, se révèle être fondamental en raison tant du caractère transnational du phénomène de piratage et de certains acteurs de l'écosystème, que de la similarité des défis à relever sur le plan mondial pour les combattre.

La lutte contre le piratage semble désormais se concentrer autour de trois axes majeurs : la lutte directe contre la contrefaçon commerciale *via* des procédures pénales à l'encontre des sites illicites et, à défaut, des injonctions de blocage, administratives ou judiciaires (I) ; l'implication des intermédiaires d'internet (II) ; les mesures visant à responsabiliser les internautes (III).

Les enjeux qui ressortent de ce travail de veille sont multiples : instaurer un travail de caractérisation des services afin d'appréhender l'offre évolutive et protéiforme de services se livrant au piratage ; prévoir des dispositifs souples et agiles de lutte contre les stratégies de contournement des mesures de blocage mises en œuvre par les opérateurs de services illicites ; associer à la lutte contre le piratage tous les acteurs d'internet, tels que les services de système de noms de domaine dits « DNS alternatifs » ; créer un dispositif spécifique de lutte contre le piratage de retransmissions de rencontres sportives.

I LES MESURES DE BLOCAGE VISANT LES SITES ILLICITES ET LEURS DIFFÉRENTS CHEMINS D'ACCÈS

Un premier constat s'impose : la typologie des services se livrant au piratage de contenus protégés est de plus en plus variée, et s'attaquer à cette offre évolutive et protéiforme implique nécessairement en amont un travail de caractérisation au regard des caractéristiques techniques et juridiques de ces services.

Parmi les mesures susceptibles d'être obtenues à l'encontre de ces services, leur fermeture est la plus impactante. Il s'agit d'une mesure coercitive prise à l'issue d'actions en justice en contrefaçon introduites par les ayants droit et qui portent sur la responsabilité et la mise en cause directe du site et de ses administrateurs. Ces procédures pénales visant des administrateurs de sites illicites, impliquant généralement la saisie des serveurs web hébergeant les sites, conduisent ainsi à la disparition des services illicites visés et sanctionnés par la procédure.

Il n'est cependant pas toujours possible d'agir à la source pour obtenir la fermeture de services, du fait de l'impossibilité d'identifier leurs administrateurs ou de leur localisation à l'étranger. À défaut de pouvoir engager de telles actions, les ayants droit disposent aujourd'hui dans de nombreux pays de la faculté d'introduire des actions en cessation à l'encontre des intermédiaires techniques sans avoir à mettre en cause le service illicite lui-même. Il s'agit de dispositifs alternatifs ou subsidiaires qui visent principalement à enjoindre les fournisseurs d'accès à internet de mettre en œuvre des mesures de blocage des services illicites.

Le service illicite continue ainsi d'exister mais n'est plus accessible sur le territoire *via* les principaux fournisseurs d'accès à internet. Les injonctions de blocage à l'encontre des intermédiaires techniques peuvent être prononcées par le juge ou par l'autorité publique sans que leur responsabilité ne soit recherchée.

Toutefois, ces mesures, dès lors qu'elles n'affectent pas directement l'administrateur, ni les ressources ou infrastructures du service, peuvent être contournées. On constate alors que les sites bloqués sont de nouveau accessibles assez rapidement après le prononcé d'une mesure de blocage, soit *via* une redirection ou un autre moyen d'accès vers un nouveau site à l'identique (on parle alors communément de « sites miroirs »), soit sous une forme légèrement différente.

Cette question du contournement des mesures de blocage est encore plus cruciale pour les ayants droit de l'écosystème des retransmissions de rencontres sportives, le piratage des diffusions en direct de ces

contenus nécessitant ainsi d'innover encore pour trouver des outils à même de répondre au besoin de pouvoir bloquer en temps réel les diffusions en direct illicites de ces contenus.

1.1 | UNE OFFRE ILLICITE DE CONTENUS CULTURELS ET SPORTIFS DIVERSE ET ÉVOLUTIVE

L'évolution constante de l'écosystème de l'offre illicite de contenus sur internet fait qu'aujourd'hui des contenus tant culturels que sportifs sont disponibles *via* différents services, chacun jouant un rôle distinct dans cet écosystème complexe. Une analyse des actions engagées par les ayants droit à l'encontre de ces services permet ainsi de dresser un panorama de leur diversité.

1.1.A | LES SITES DE LIENS PROPOSANT DES CONTENUS CULTURELS

Jusqu'à récemment, les ayants droit concentraient leurs actions contre les sites de liens, soit les sites centralisant des liens renvoyant vers des fichiers disponibles sur les réseaux pair à pair ou hébergés sur des sites tiers, dits services d'hébergement de contenus ou de fichiers. Les différents liens présents sur ces sites sont organisés et catégorisés à la manière de ce que font les services de l'offre légale. De nombreuses actions dans le monde ont été et sont toujours engagées à l'encontre de ces services, qu'il s'agisse de procédures judiciaires visant directement leurs administrateurs ou de procédures visant à obtenir le blocage de ces services.

En France, on peut relever que les actions judiciaires destinées à l'obtention de mesures de blocage ne se limitent plus – comme cela était le cas pour les premières procédures – aux noms de domaine des sites d'une seule et même galaxie, c'est-à-dire des sites pour lesquels on pouvait supposer qu'ils ont des administrateurs communs, mais embrassent une pluralité de sites de liens, regroupés pour les besoins de la procédure. Cette évolution traduit deux phénomènes : d'une part, le morcellement de l'offre illégale au travers d'une myriade de petits sites de moindre capacité et audience, comme conséquence des mesures de blocage, l'audience des sites illégaux ne se concentrant plus désormais sur quelques grands sites à très forte notoriété, et, d'autre part, la très forte dynamique des sites illicites consistant à chercher à contourner les mesures de blocage par la multiplication des avatars.

En Europe, la Cour de justice de l'Union européenne a construit sa jurisprudence en matière de liens hypertextes, essentiellement depuis l'arrêt dit Svensson^[1] en 2014. La jurisprudence GS Media^[2] fin 2016 a posé le principe d'une présomption d'illégalité des sites de liens (professionnels) pointant vers des sites illicites, ce qui facilite l'éventuelle caractérisation de sites massivement contrefaisants ainsi que le travail probatoire devant les tribunaux. La condamnation d'un site de contenus contrefaisants entraînerait plus facilement le constat de l'illégalité des sites de liens pointant vers les contenus de ce site. Deux autres arrêts font application de ces critères et relèvent notamment le rôle spécifique joué par le lecteur multimédia ou la plateforme « *The Pirate Bay* » pour donner accès aux œuvres aux internautes.

1.1.B | LES SERVICES D'HÉBERGEMENT DE FICHIERS

Les plateformes d'hébergement de fichiers d'œuvres contrefaisantes sont des acteurs phares de l'écosystème du téléchargement direct et du *streaming*. Ceux-ci hébergent des contenus, référencés sur des services tiers, qui peuvent être consommés selon un ou plusieurs modes : téléchargement direct et/ou *streaming*. Il peut également s'agir de serveurs rediffusant ponctuellement ou continuellement des flux en *live streaming* ou des programmes TV, sportifs ou autres. De manière générale, ce sont les sites de liens ou des services d'agrégation spécialisés qui redirigent les internautes vers ces hébergeurs spécialisés.

Dans la mesure où ces services ne sont pas éditorialisés, il est souvent considéré comme délicat d'agir à leur encontre, notamment du fait du régime de responsabilité limitée des hébergeurs.

Dernièrement, plusieurs actions ont cependant été engagées avec succès à l'encontre de services d'hébergement de fichiers, tant par l'industrie musicale que par les acteurs de l'audiovisuel.

En 2019, des actions diligentées par les ayants droit de la musique en France, en Italie et en Russie ont notamment abouti au blocage de sites d'hébergement de fichiers.

Au cours du mois d'octobre 2019, l'action de l'*Alliance For Creativity and Entertainment* (ACE)^[3]

a ainsi conduit, à la suite d'un accord, à la fermeture de l'un des plus importants sites d'hébergement de fichiers *Openload* et de sites connexes tels que *Streamango*.

Fin 2019, à la suite de l'action en justice diligentée par Netflix et Warner Bros, un accord a été conclu avec l'un des plus grands services d'hébergement de fichiers, *Rapidvideo*, entraînant sa fermeture, mais également le versement de sommes importantes à titre de dommages et intérêts ainsi que le transfert des noms de domaine concernés à la *Motion Picture Association*.

Par ailleurs, l'administration américaine, via l'*United States Trade Representative* (USTR), une agence gouvernementale qui coordonne la politique commerciale des États-Unis, inscrit régulièrement sur sa liste annuelle de services illicites des services d'hébergement de fichiers, dont le service *1Fichier*, localisé en France, qui est listé depuis plusieurs années par l'USTR.

En janvier 2019, l'autorité publique italienne ayant le pouvoir d'enjoindre des mesures de blocage, l'AGCOM, a également ordonné le blocage du service d'hébergement de fichiers *1Fichier*.

1.1.C | LES SERVICES ILLICITES DE STREAM RIPPING

Le *stream ripping* est une pratique qui consiste à réaliser une copie pérenne (*ripping*) de contenus diffusés en *streaming* sur internet. L'acte de *stream ripping* peut être réalisé par un logiciel, installé directement sur le poste de l'utilisateur, lors de la réception des données en *streaming*. Mais cet acte peut également être délégué à un tiers, notamment à des services en ligne distants qui vont lire et enregistrer un flux en direct souhaité pour le compte de l'utilisateur, puis le stocker pour le distribuer à d'autres utilisateurs à l'avenir, ou qui vont aller consulter le contenu désiré sur une plateforme de *streaming* à la demande et en réaliser une copie.

Les actions engagées par l'industrie musicale, notamment représentée à l'international par la Fédération internationale de l'industrie phonographique (IFPI), présente dans 59 pays, se sont récemment concentrées sur les services de *stream ripping* illicites, des décisions visant ces services ayant récemment été prononcées pour la première fois dans nombre de pays.

[1] CJUE, 13 février 2014, C-466/12, Svensson e.a. Cet arrêt a posé que lorsque le contenu a été diffusé initialement avec l'accord du titulaire des droits il faut, pour déterminer si le lien pointant vers ce contenu était aussi soumis à autorisation ou non, vérifier si ce contenu était déjà accessible librement ou s'il était réservé à des abonnés. Si le contenu était déjà accessible, le lien est libre et ne constitue pas une communication au public qui nécessiterait une autorisation. En revanche, si le contenu était réservé à des abonnés, il faut vérifier si ce lien n'est pas de nature à mettre ce contenu à disposition d'un « public nouveau » auquel cas il faudrait recueillir une nouvelle autorisation.

[2] CJUE, 8 septembre 2016, C-160/15, GS Media.

[3] L'*Alliance For Creativity and Entertainment* (ACE), créée en juin 2017 sous l'égide de la *Motion Picture Association*, réunit des ayants droit de l'audiovisuel de différents pays dans le cadre d'une coalition destinée à lutter contre le piratage au niveau international. À ce jour, celle-ci compte 35 membres dont Apple TV+, Disney, Amazon, Netflix, Warner Bros, NBCUniversal, Canal+ Group, Sky, la BBC...

Depuis 2018, les actions à l'encontre de ce type de service se multiplient, notamment en Allemagne, en Australie, au Danemark, en Espagne, en Italie^[4] et en Russie^[5].

1.1.D | LES SERVICES DIFFUSANT DES CONTENUS PROTÉGÉS EN DIRECT

Le piratage des contenus diffusés en direct, et notamment de contenus sportifs sur internet, a pris une ampleur considérable ces dernières années dans de nombreux pays.

Les offres de contenus diffusés en direct prennent notamment la forme de sites dédiés au piratage de contenus sportifs, dits services de « *live streaming* », et de bouquets illicites de chaînes de télévision, dits services IPTV illicites.

Les services dits de « *live streaming* » sont principalement utilisés pour visionner des manifestations sportives en direct. Ces services présentent leurs contenus sous forme de liens organisés par événement ou par type de sport, indépendamment des chaînes de télévision à l'origine de leur diffusion. Ces liens pointent vers des plateformes d'hébergement de contenus qui peuvent être exclusivement dédiées au piratage et s'appuyer dans certains cas sur des sites intermédiaires.

Les services IPTV illicites donnent accès à un grand nombre de chaînes de télévision et, notamment, à des chaînes payantes thématiques consacrées au sport ou diffusant régulièrement des contenus sportifs. Les services qui alimentent l'offre de bouquets de chaînes n'ont pas nécessairement de site internet et se contentent d'avoir des serveurs qui diffusent les chaînes en flux.

Une étude publiée en novembre 2019 par l'Observatoire européen des atteintes aux droits de propriété intellectuelle rattachée à l'Office de l'Union européenne pour la propriété intellectuelle (EUIPO) – à laquelle l'Hadopi a contribué – estime que 941,7 millions d'euros de revenus illégaux ont été générés par des fournisseurs de services IPTV illicites dans l'Union européenne en 2018 et que ces services ont été utilisés par 13,7 millions de personnes (soit 3,6 % de la population de l'Union)^[6].

Il faut également signaler que les services IPTV illicites ont fait leur apparition sur la liste des marchés facilitant la contrefaçon et le piratage publiée par la Commission européenne fin 2020 (voir ci-après). Une catégorie dédiée à ces services a ainsi été créée, face aux nombreuses réponses des diffuseurs ou des organisateurs d'événements sportifs à la consultation publique préalable à l'établissement de la liste, témoignant d'une inquiétude croissante concernant la prolifération de ces services.

En Europe, sous la coordination d'Europol, plusieurs services IPTV importants ont été fermés récemment grâce à une coopération entre les services de police de différents pays. L'intervention de l'ACE a notamment conduit à la fermeture du service IPTV populaire *Utlango TV*, qui donnait notamment accès gratuitement à des milliers de flux télévisés sans licence. Le nom de domaine a été transféré à l'ACE au début de l'année 2020. En 2019, la lutte menée à l'encontre des services IPTV illicites par l'ACE a par ailleurs entraîné la fermeture d'un bon nombre d'entre eux.

Enfin, les acteurs de la diffusion des contenus sportifs ont obtenu diverses mesures de blocage dans le monde entier, plus ou moins adaptées aux spécificités de la lutte contre le piratage de ce type de contenus (voir ci-après).

1.1.E | LE PARTAGE DE MOTS DE PASSE SUR LES SITES DE L'OFFRE LÉGALE

La pratique du partage de mots passe facilite l'accès à des contenus non autorisés et constitue à ce titre l'une des préoccupations actuelles de l'ACE. Selon une étude publiée par Magid^[7], le partage de mots de passe pourrait entraîner pour Netflix une perte d'environ 135 millions de dollars d'abonnements. L'ACE a annoncé récemment qu'un nouveau groupe de travail s'intéresserait à la question afin de définir de « meilleures pratiques » et de faire face à l'accès non autorisé de contenus.

[4] En Italie, l'AGCOM a ainsi prononcé des injonctions de blocage visant 16 sites de stream ripping. Dans une décision du 2 août 2019, le tribunal de Latium a confirmé l'injonction de blocage du site de stream ripping Yout prononcée par l'AGCOM.

[5] <https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2019/2019fca0751>, la première décision de blocage de sites de stream ripping a été obtenue en avril 2019. Tribunal de commerce de Madrid, AGEDI v Telefonica 29 avril 2019, 201910269787429.

[6] « IPTV illégale dans l'Union européenne, Étude sur les modèles d'entreprises en ligne portant atteinte aux droits de propriété intellectuelle -phase 3 », EUIPO, novembre 2019, https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Illegal_IPTV_in_the_European_Union/2019_Illegal_IPTV_in_the_European_Union_Full_en.pdf

[7] <https://magid.com/mentions/the-netflix-sharing-problem/>

1.1.F | UN ENJEU DE CARACTÉRISATION DES SERVICES ILLICITES

La lutte contre les services illicites implique, pour éviter l'obsolescence ou l'inefficacité (voire l'inapplicabilité) des mesures projetées, de laisser assez ouvertes les hypothèses et critères de caractérisation d'un site ou service illicite.

Dans certains pays, des critères pour caractériser les sites illicites sont prédéfinis par la loi, la jurisprudence ou l'administration. Il s'agit le plus souvent d'un faisceau d'indices fondés sur une logique de seuils (nombre d'œuvres ou de liens concernés) ou de pourcentages de contenus illicites à identifier.

Cette caractérisation est d'abord cruciale au niveau national afin de faciliter et de fluidifier le recours aux mesures de blocage, mais c'est également un enjeu au niveau international dans l'optique de faciliter les actions des ayants droit pour obtenir des mesures de blocage à l'encontre du même site dans un autre pays. Dès lors, la question se pose aujourd'hui, en particulier au niveau européen, de la prise en compte par l'autorité judiciaire ou publique d'un pays donné, des précédentes décisions judiciaires ou administratives rendues dans un pays tiers concernant le même site.



En Australie, la loi prévoyant les mesures de blocage sur injonction judiciaire a été modifiée fin 2018 pour élargir son champ d'application – jusqu'alors restreint aux seuls sites qui ont pour objet de porter atteinte ou de faciliter les atteintes à la propriété intellectuelle – à tous les sites qui ont simplement pour effet de porter atteinte au droit d'auteur ou de faciliter leur violation.

Au Canada, pour qualifier les services illicites, le juge peut prendre en compte les éléments suivants, prévus par la loi : le fait que le responsable du service fasse valoir comme argument de promotion que ledit service permet de commettre des actes de contrefaçon ; la connaissance par le responsable du site du fait que son service était utilisé pour faciliter la contrefaçon ; le fait que le service soit significativement utilisé ou non à d'autres fins que pour commettre des actes de contrefaçon ; les mesures prises pour limiter la contrefaçon ; les avantages retirés des actes de contrefaçon et/ou la viabilité économique de la fourniture du service dans les cas où celui-ci n'aurait pas été utilisé pour commettre de tels actes.

En Corée du Sud, le critère anciennement retenu, selon lequel 70 % des contenus des sites devaient avoir été mis illicitement à disposition pour que le régulateur des communications, la *Korea Communications Standards Commission*, enjoigne au blocage de ces sites, n'est plus en vigueur depuis 2019.

En France, le projet de réforme du dispositif anti-piratage actuellement envisagé prévoit de charger le régulateur d'établir une liste noire de services illicites visant à objectiver et sécuriser les accords du type « *Follow the money* », signés entre les ayants droit et les acteurs économiques, comme notamment les acteurs de la publicité et du paiement en ligne. Une autre utilisation possible de cette nouvelle mission de caractérisation des services illicites est qu'elle soit un facteur de clarification sur la manière d'appréhender un site illicite qui puisse être utile au grand public, aux acteurs économiques et au juge.

Au Danemark comme au **Royaume-Uni**, les ayants droit doivent démontrer que le contenu disponible sur le site leur appartient et qu'ils n'ont pas directement ou indirectement consenti à sa mise à disposition. Il n'y a pas de seuil prédéfini pour déterminer le caractère contrefaisant d'un site internet. En principe, une infraction est suffisante, mais les ayants droit concentrent leurs actions sur les sites qui fournissent un nombre substantiel d'œuvres contrefaisantes.

En Lituanie, les critères pris en considération pour déterminer si un site est illégal sont les suivants : le ratio des contenus illicites présents sur le site ; le site a été créé et est utilisé pour diffuser des contenus illicites ; si le site diffuse uniquement des contenus protégés par le droit d'auteur ou s'il met également à disposition d'autres types de contenus ; si les utilisateurs sont directement ou indirectement incités à promouvoir, télécharger, reproduire ou à utiliser de toute autre manière les contenus illicites ; des mesures spécifiques sont mises en œuvre pour supprimer les contenus illicites ; l'audience du site ; si le site a une activité lucrative ; le contenu protégé par le droit d'auteur dont le demandeur demande le retrait est accessible sur des sites de l'offre légale.

Au Portugal, deux critères sont utilisés par l'inspection générale des affaires culturelles (IGAC), rattachée au ministère de la Culture, pour déterminer le caractère contrefaisant d'un site et ordonner son blocage : soit le nombre de liens contrefaisants notifiés par les ayants droit doit être supérieur à 500, soit le pourcentage de contenus contrefaisants sur le site est au moins de 66 %.

À Singapour, la loi prévoit un faisceau de critères pour déterminer si un site porte effectivement atteinte aux droits d'auteur et doit en conséquence être bloqué : si l'objectif principal du site est de commettre ou de faciliter la violation du droit d'auteur ; si le site met à disposition des contenus ou des répertoires, des index ou des catégories de liens vers des contenus pour faciliter la violation des droits d'auteur ; si l'opérateur du site démontre un mépris général du droit d'auteur ; si le site a déjà fait l'objet de mesures de blocage dans un autre pays pour cause de violation du droit d'auteur ou en lien avec une telle violation ; si le site contient des guides ou des instructions pour contourner des mesures, ou des décisions de justice visant à empêcher l'accès à des sites illégaux ; l'audience du site.

1.2 | LA CONSOLIDATION DES INJONCTIONS JUDICIAIRES OU ADMINISTRATIVES DE BLOCAGE

Dans de nombreux pays, les ayants droit peuvent saisir le juge ou l'autorité publique afin de voir

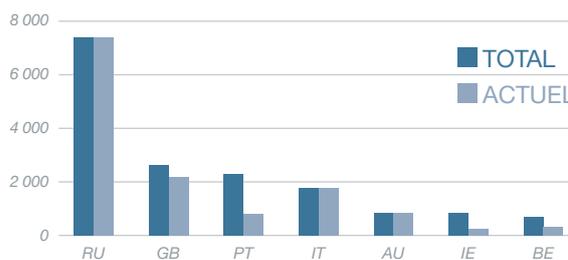
prononcées des mesures de blocage enjoignant les fournisseurs d'accès à internet de prévenir ou faire cesser des atteintes en matière de protection des droits d'auteur, indépendamment de toute recherche de mise en cause de la responsabilité du fournisseur d'accès.

CARTOGRAPHIE DES MESURES DE BLOCAGE – MESURES DE BLOCAGE DE SITES DANS LE MONDE



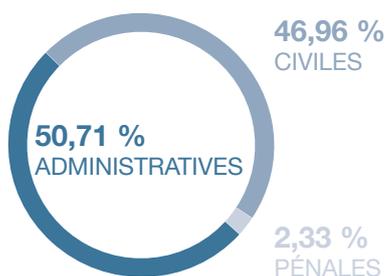
Au niveau mondial, on constate que le recours aux injonctions judiciaires est presque aussi fréquent que le recours aux injonctions administratives. Sur les sept pays ayant le plus de noms de domaine bloqués, trois ont instauré un système de blocage administratif (Russie, Portugal, Italie). Les quatre autres pays ont mis en place un dispositif de blocage judiciaire, trois de ces pays étant régis par la *common law* (Australie, Irlande, Royaume-Uni) – le Royaume-Uni ayant mis en œuvre la procédure de blocage judiciaire la plus ancienne et la plus éprouvée.

NOMS DE DOMAINE BLOQUÉS PAR PAYS



Source : Motion Picture Association - chiffres 2020

TYPES DE PROCÉDURES : ADMINISTRATIVES, PÉNALES, CIVILES



Source : Motion Picture Association

Pour les pays de l'Union européenne, c'est l'article 11 de la directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle, dite directive « IPRED », qui ouvre la possibilité pour les titulaires de droits de demander une injonction à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit de propriété intellectuelle. Une disposition similaire à l'article 11 figurait déjà dans la directive 2001/29/CE sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, dite « DADVSI » (article 8.3)^[8].

En Italie, en Grèce, en Espagne et au Portugal, s'ajoutent parallèlement aux procédures administratives fondées sur la transposition de la directive dite « commerce électronique »^[9], des procédures judiciaires en cessation.

[8] « Les États membres veillent à ce que les titulaires de droits puissent demander qu'une ordonnance sur requête soit rendue à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit d'auteur ou à un droit voisin. »

[9] « Article 12 [...] 3. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation. »

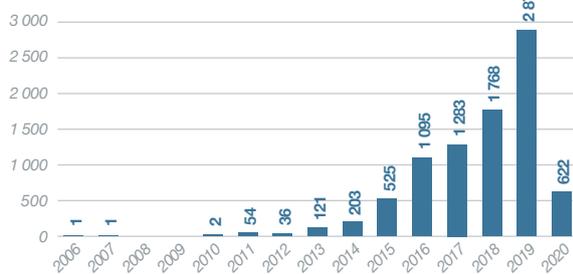
Dans chacun des quatre pays précités, la procédure administrative devient caduque si les ayants droit saisissent la justice *via* des actions en cessation pour les mêmes sites litigieux.

1.3 | LA LUTTE CONTRE LES CONTOURNEMENTS DES MESURES DE BLOCAGE

À travers le monde est apparu l'expression générique de « site miroir » qui englobe de manière très hétérogène les phénomènes de réapparition et de réplification de sites bloqués ainsi que la création d'accès détournés à ces sites. Ces pratiques de contournement des mesures mises en place à leur encontre par les administrateurs des sites illicites mettent en lumière l'ampleur du piratage et la nécessité de trouver une solution agile afin de permettre la conservation dans le temps des effets des mesures de blocage.

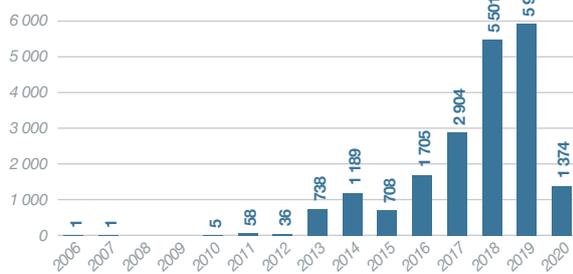
Les graphiques ci-dessous illustrent le fait qu'aujourd'hui, en moyenne, pour chaque service illicite bloqué, il faudra bloquer au moins deux noms de domaine afférents à ce service. Les phénomènes de réapparition concerneraient, selon certains interlocuteurs interrogés, 30 % à 40 % des sites bloqués.

NOMBRE TOTAL DE SITES BLOQUÉS PAR AN



Source : Motion Picture Association - chiffres 2020

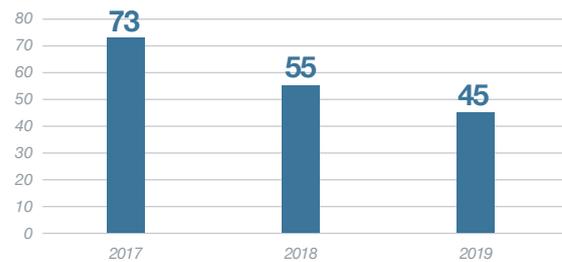
NOMBRE TOTAL DE NOMS DE DOMAINE BLOQUÉS PAR AN



Source : Motion Picture Association - chiffres 2020

Les effets collatéraux des mesures de blocage relevés en France sont d'une part le morcellement de l'offre illégale au travers d'une myriade de petits sites de moindre capacité et audience, l'audience des sites illégaux ne se concentrant plus désormais sur quelques grands sites à très forte notoriété, et d'autre part, la très forte dynamique des sites illicites qui cherchent à contourner les mesures de blocage par la multiplication d'avatars.

PART D'AUDIENCE EN % DU TOP 10 DES SITES ILLICITES



Source : Alpa-CNC-Médiamétrie

1.3.A | LES ENJEUX JURIDIQUES LIÉS AU PRONONCÉ DE MESURES PRÉVENTIVES EN EUROPE

Les actes de contournement sont par nature peu prévisibles dans leurs manifestations concrètes et évolutifs sur le plan technologique. Ces phénomènes sont difficiles à appréhender et à qualifier juridiquement, si bien que les États se heurtent à deux interrogations récurrentes :

- Quelles sont les facultés dont disposerait déjà le pouvoir judiciaire ou les autorités publiques en charge de la lutte contre le piratage pour y faire face de manière préventive, notamment par le biais d'injonctions cadres ou dynamiques à l'égard des parties prenantes ?
- Faut-il consacrer par la loi ou un autre vecteur juridique ces nouvelles formes de procédures ou d'injonctions et avec quel degré de précision ou de généralité acceptable pour agir plus efficacement et rapidement contre ces phénomènes ?

En Europe, l'article 8.3 de la directive 2001/29 du 22 mai 2001 dite DADVSI, et le dernier alinéa de l'article 11 de la directive 2004/48 du 29 avril 2004 dite IPRED, prévoient la possibilité pour les titulaires de droits de demander une injonction préventive à l'encontre des intermédiaires associés aux mesures initiales de blocage.

La jurisprudence européenne a fait une interprétation de ces textes en considérant qu'ils permettent d'obtenir des mesures préventives de la part du juge ou des autorités publiques^[10].

Dans ses lignes directrices relatives aux modalités d'application de la directive dite IPRED^[11], la Commission encourage le recours aux injonctions préventives et précise que l'objectif de lutte contre la réapparition des sites miroirs peut également être atteint grâce à l'intervention d'une autorité publique ou de la police^[12].

1.3.B | LA RECHERCHE DE SOLUTIONS EFFICACES POUR LUTTER CONTRE LES SITES MIROIRS

L'essor des accords volontaires sur la base d'injonctions dynamiques de blocage

La difficulté majeure dans le cadre de mesures judiciaires de blocage réside dans l'obligation de revenir devant le juge aux fins d'actualisation des décisions pour ajouter les adresses du site (et les nouveaux noms de domaine utilisés ou adresses IP supplémentaires) opposables aux fournisseurs d'accès à internet.

Une des solutions déjà explorées dans certains pays consiste à admettre ou à introduire plus de flexibilité dans le prononcé des injonctions judiciaires, alors dites « dynamiques », et d'y adjoindre des mécanismes de droit souple afin d'actualiser plus rapidement les mesures de blocage des sites illicites au fur et à mesure de leurs migrations ou mutations. Une telle solution permet également d'économiser du temps et de réduire les coûts pour les parties et les tribunaux.

Cela implique concrètement pour le tribunal d'ordonner – outre le blocage de sites illicites spécifiques initialement visés par la décision – le blocage, dans le cadre d'un dialogue entre les parties faisant suite à la décision, des noms de domaine et, le cas échéant, des adresses IP, identifiés par les ayants droit et notifiés aux fournisseurs d'accès à internet (et/ou aux moteurs de recherche) aux fins d'actualisation.

En Australie, une nouvelle loi adoptée en novembre 2018 permet le prononcé d'injonctions judiciaires dynamiques et incite au dialogue et au conventionnement entre les ayants droit et les intermédiaires attirés dans la procédure (fournisseurs d'accès à internet et moteurs de recherche).

Au Canada, en juillet 2019, la première décision judiciaire de blocage rendue en matière de contrefaçon a prévu que, face à l'apparition de sites dits miroirs, les parties pourront revenir devant le juge avec une nouvelle liste de noms de domaine et/ou d'adresses IP. Les fournisseurs d'accès à internet pourront alors s'opposer à l'actualisation de la mesure de blocage mais, en l'absence de contestation dans les dix jours, la cour pourra ordonner l'actualisation des mesures de blocage.

Au Danemark, le code de conduite entre les fournisseurs d'accès et les ayants droit organisant le blocage des sites miroirs à la suite d'une injonction judiciaire a été amendé en 2020 pour faciliter et accélérer encore le blocage de ces sites. De plus, la jurisprudence récente permet aux ayants droit de demander aux fournisseurs d'accès à internet le blocage non plus seulement de sites identifiés par leur nom de domaine mais également de sites identifiés par leur contenu, leur interface, quel que soit leur nom de domaine.

En Inde, en avril 2019, la haute cour de Delhi a ordonné le blocage de certains des plus importants sites de pair à pair et de *streaming*, ainsi que les noms de domaine alternatifs et proxys utilisés. La décision prévoit que les ayants droit pourront transmettre les informations relatives à l'apparition de sites miroirs aux fournisseurs d'accès à internet afin que ceux-ci soient immédiatement bloqués.

[10] CJUE, 12 juillet 2011, C-324/09 L'Oréal SA et autres contre eBay International AG et autres, décision relative à l'article 11 de la directive IPRED; CJUE, 24 novembre 2011, C-70/10 Scarlet Extended SA contre Sabam, sur le fondement de l'article 8.3 de la directive dite DADVSI.

[11] ec.europa.eu/docsroom/documents/26582

[12] « Furthermore, injunctions may in certain cases lose some effectiveness because of changes in the subject matter in respect of which the injunction was ordered. This may be, for example, the case of website blocking injunctions, where a competent judicial authority grants the injunction with reference to certain specific domain names, whilst mirror websites can appear easily under other domain names and thus remain unaffected by the injunction. Dynamic injunctions are a possible means to address this. These are injunctions which can be issued for instance in cases in which materially the same website becomes available immediately after issuing the injunction with a different IP address or URL and which is drafted in a way that allows to also cover the new IP address or URL without the need for a new judicial procedure to obtain a new injunction. The possibility of issuing such injunctions exists, inter alia, in the United Kingdom and Ireland. This objective could also be pursued through intervention of a public authority or the police, as it occurred in a specific case in Belgium. »

En Irlande, depuis 2013, les décisions prévoient expressément que les fournisseurs d'accès à internet bloqueront par la suite les sites permettant d'accéder aux sites bloqués, dans le respect d'un protocole d'accord désormais annexé à l'ordonnance judiciaire.

Au Royaume-Uni, les décisions de blocage permettent l'actualisation des sites et des adresses IP. Cette actualisation est mise en œuvre par les fournisseurs d'accès à internet, en collaboration avec les ayants droit qui leur transmettent les listes actualisées d'adresses à bloquer, sans repasser devant le juge. Les fournisseurs d'accès à internet supportent les coûts de mise en œuvre de ces mesures.

À Singapour, fin 2018, la haute cour de Singapour a ordonné pour la première fois le blocage dynamique de 153 noms de domaine considérés comme manifestement illicites. Les fournisseurs d'accès à internet doivent ainsi sur simple notification des ayants droit visant à démontrer que le nom de domaine initial a par exemple été redirigé, bloquer les sites dits miroirs des sites visés dans le jugement.

En Suède, suite au prononcé en décembre 2019 par la cour des brevets et du marché de Stockholm d'une injonction dynamique de blocage, les ayants droit peuvent demander l'actualisation des mesures de blocage des noms de domaine et adresses IP sans passer devant le juge.

Les exemples de suivi administratif des mesures de blocage

Les enjeux et les apports de l'intervention d'une autorité publique en matière de sites de contournement consistent selon les cas de figure à :

- établir une méthodologie ou définir un cadre de référence pour l'identification et la caractérisation des services de contournement concourant ou contribuant à rendre accessible des sites massivement contrefaisants ayant fait l'objet de mesures préalables de blocage ;
- limiter ou à défaut simplifier et raccourcir les procédures visant à ordonner le blocage des sites et services de contournement ;

- faciliter et sécuriser la mise en œuvre de ces décisions par les fournisseurs d'accès à internet et les étendre à d'autres acteurs volontaires (autres fournisseurs d'accès à internet, moteurs de recherche, etc.) ;
- obtenir de manière plus systématique la mise en œuvre de redirections vers une page d'information institutionnelle indiquant les motifs de la mesure de blocage et renvoyant vers l'offre légale.

En France, le projet de réforme prévoit de créer un dispositif qui permettrait à l'autorité publique, sur saisine des ayants droit, de pouvoir demander l'actualisation des mesures de blocage prononcées par le juge, pour la durée de l'injonction restant à courir.

En Espagne, les injonctions administratives de blocage doivent être validées par le juge mais il n'est cependant pas nécessaire de repasser devant lui pour que les ayants droit obtiennent le blocage des sites miroirs, ceux-ci peuvent se contenter d'indiquer aux fournisseurs d'accès à internet en quoi le nouveau site est un site miroir.

En Grèce, depuis une loi de juillet 2020, l'autorité publique peut ordonner toute mesure visant à prévenir ou à faire cesser une atteinte à un droit d'auteur ou un droit voisin. Désormais, si à la suite de l'adoption et de l'exécution d'une ou de plusieurs décisions, l'atteinte persiste, le titulaire de droits lésé peut déposer une demande afin de solliciter l'adoption d'une nouvelle décision, ce sans payer de frais supplémentaires.

En Italie, le règlement entré en vigueur le 16 octobre 2018 a introduit une nouvelle disposition dédiée aux hypothèses de réitération des violations constatées ayant déjà fait l'objet d'une injonction administrative, lequel prévoit une procédure accélérée.

En Lituanie, la commission chargée de mettre en œuvre la procédure de blocage effectue un suivi quant à la réapparition de sites dits miroirs. Elle a ainsi procédé en 2019 au blocage de cinq sites miroirs.

En Russie, le régulateur est également chargé de maintenir à jour la liste des sites bloqués. Une loi, adoptée le 1^{er} juillet 2017, a introduit un dispositif de blocage simplifié des sites de contournement *via* une procédure administrative accélérée qui ne nécessite pas de repasser devant le juge.

1.3.C | LES ACTIONS À L'ÉGARD DE CERTAINS SERVICES DE SYSTÈME DE NOMS DE DOMAINE (DNS DITS ALTERNATIFS)

Le *Domain Name System* en anglais, ou DNS, est un système clé du web qui fournit la correspondance entre le nom de domaine d'un site et l'adresse du serveur où ce site est hébergé. Les abonnés d'un fournisseur d'accès à internet utilisent par défaut le service DNS que celui-ci met à leur disposition. Lorsque ce fournisseur d'accès à internet met en œuvre une mesure de blocage de noms de domaine (dit blocage DNS), il configure généralement son service DNS de façon à fournir aux utilisateurs une adresse d'hébergement invalide pour le site à bloquer ou de façon à rediriger les connexions vers un serveur de substitution (qui affiche par exemple un message d'alerte ou d'information).

Il est toutefois possible pour les internautes – plutôt que d'utiliser le système DNS de leur fournisseur d'accès à internet – de configurer leur navigateur web, le système d'exploitation de leur terminal (ordinateur, équipement mobile, etc.) ou même leur *box* internet (routeur domestique) dans le but d'utiliser un système DNS dit alternatif car proposé par un tiers tel que Google, Cloudflare, etc. Étant donné que ces services alternatifs ne sont pas à ce jour attirés dans les procédures de blocage ciblant les services illicites, leur utilisation permet aux internautes de contourner les mesures de blocage mises en œuvre par les fournisseurs d'accès à internet nationaux. C'est pourquoi des réflexions sont aujourd'hui à l'étude afin d'impliquer davantage ces services dans la mise en œuvre des mesures de blocage.

Ces réflexions sont d'autant plus importantes que l'effectivité des mesures de blocage est de nature à être diminuée par le récent développement du *DNS over HTTPS* (DoH) – une évolution technique du système DNS qui a pour objectif d'améliorer la sécurité et le niveau de protection de la vie privée des utilisateurs, en chiffrant les échanges entre les applications ou équipements des internautes et les serveurs DNS. En effet, l'usage du DoH implique le plus souvent – en l'état – le recours à un service DNS alternatif. Or, son usage pourrait rapidement devenir massif car son utilisation peut être proposée par défaut, ou *via* une configuration simple, par les navigateurs, systèmes d'exploitation ou *box* internet.

Une piste pour éviter les contournements des mesures de blocage DNS, sous réserve de la proportionnalité de ces mesures au regard du niveau d'utilisation de ces services, pourrait être de requérir le blocage DNS des sites illicites non plus seulement aux fournisseurs d'accès à internet mais également aux opérateurs proposant des services DNS alternatifs.

La proposition de règlement *Digital Services Act*^[13] (DSA) présenté par la Commission européenne en décembre 2020, laquelle a vocation à actualiser les dispositions de la directive dite « commerce électronique » qui détermine le régime de responsabilité des intermédiaires techniques, pourrait faciliter de telles démarches. En effet, le considérant 27 de ce texte liste les intermédiaires d'internet qui existent aujourd'hui mais n'étaient pas expressément visés par le texte de la directive « commerce électronique » – parmi lesquels figurent les systèmes de noms de domaine, pour indiquer que ceux-ci devraient pouvoir bénéficier du régime de responsabilité des intermédiaires techniques dès lors qu'il est possible de les rattacher à une des catégories prévues par la directive et confortée par la proposition de règlement, à savoir les services offrant une infrastructure de réseau, les services de cache et les hébergeurs. Dès lors, s'il apparaît que le DSA confirme la possibilité d'obtenir en Europe des mesures de cessation à l'encontre des services de système de noms de domaine, il serait cependant précieux que le statut des DNS alternatifs soit précisé expressément.

En Italie, l'autorité publique locale a conclu un accord volontaire concernant le service DNS de CISCO en 2019. Aux termes de celui-ci, CISCO s'est engagé à bloquer, pour les internautes utilisant son service depuis l'Italie, les sites visés par une ordonnance de blocage prononcée par l'AGCOM et destinée aux seuls fournisseurs d'accès internet locaux.

En Lituanie, des échanges ont eu lieu entre des représentants de l'autorité publique locale et Google en 2019 afin de discuter de la suppression des sites bloqués et de leurs miroirs des résultats du moteur de recherche d'une part et du service de DNS alternatif de Google d'autre part. Les représentants de Google ont répondu positivement à la première requête de la commission.

En Russie, une loi adoptée le 29 juillet 2017 permet de sanctionner les services d'anonymisation, qui peuvent faire l'objet de mesures de blocage s'ils ne respectent pas les nouvelles obligations qui leur incombent.

[13] <https://eur-lex.europa.eu/legal-content/fr/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN>

1.3.D | LES PARTICULARITÉS DE LA LUTTE CONTRE LE PIRATAGE DE RETRANSMISSIONS DE CONTENUS SPORTIFS EN DIRECT : L'ÉMERGENCE D'UN DISPOSITIF DE BLOCAGE DYNAMIQUE DIT DE « LIVE BLOCKING »

S'agissant du piratage sur internet de retransmissions de rencontres sportives diffusées en direct, il est encore plus essentiel de pouvoir actualiser les mesures de blocage rapidement, voire en temps réel, compte tenu du fait que la valeur de ces contenus se concentre sur le temps de cette diffusion en direct.

Des propositions en ce sens sont d'ailleurs actuellement discutées au Parlement européen, qui s'était engagé à travailler sur la lutte contre le piratage de contenus sportifs, alors que la création d'un droit voisin en faveur des organisateurs de manifestations sportives n'a pas été retenue dans la directive 2019/790 du Parlement européen et du Conseil du 17 avril 2019, dite « droit d'auteur ».

La commission Culture et Éducation du Parlement européen a ainsi adopté le 26 janvier 2021 un rapport sur les défis des organisateurs d'événements sportifs dans l'environnement numérique^[14]. Ce texte doit maintenant être renvoyé à la commission Affaires Juridiques, laquelle devra voter, sur la base du rapport d'un ses membres^[15], une résolution parlementaire qui a ensuite vocation à être discutée par le Parlement. *In fine*, il s'agira pour le Parlement européen de décider s'il demande à la Commission de déposer une proposition législative, au cœur de laquelle pourrait figurer l'obtention de mesures de retrait dans un délai adapté à la diffusion en direct (en temps réel ou en 30 minutes). La conclusion d'accords privés entre les parties prenantes est également un des axes envisagés.

En France, les titulaires de droits d'exploitation audiovisuelle sur les manifestations et compétitions sportives ne disposent pas, en l'état du droit positif, d'une procédure judiciaire *sui generis* leur permettant d'obtenir des mesures de blocage susceptibles de pouvoir intervenir en direct (à l'occasion de la retransmission d'un match) afin de lutter efficacement contre le piratage de leurs contenus.

Le projet de réforme devait permettre :

- d'obtenir, dans le cadre d'une procédure unique, le prononcé d'une décision dynamique permettant d'étendre l'efficacité des mesures de blocage ou de déréférencement des sites ou services illicites identifiés au jour de la décision à d'autres sites ou services susceptibles d'apparaître pendant la durée de la compétition, étant précisé que les mesures peuvent être mises en œuvre selon un calendrier prévisionnel calqué sur le calendrier officiel de la compétition ;
- de s'appuyer sur un régulateur jouant un rôle de tiers de confiance pour faciliter l'identification des sites ou services diffusant illicitement la rencontre sportive en cause et notamment des services miroirs.

Dans le monde, plusieurs dispositifs de blocage adaptés à la lutte contre le piratage sportif ont été mis en œuvre récemment dans différents pays. On peut catégoriser ces différents dispositifs selon le mode de blocage utilisé (soit un blocage de noms de domaine dit « *Domain Name System* ou DNS », soit un blocage dit « *internet Protocol* ou IP » de l'adresse du serveur utilisé par le service illicite) et l'autorité ayant prononcé la mesure de blocage.

Du fait du mode de diffusion des flux retransmettant les rencontres sportives illicitement et de l'écosystème du piratage sportif, la question se pose en effet dans différents pays du type de mesure de blocage à mettre en œuvre. La plupart des législations en vigueur en matière de blocage de contenus – et notamment culturels – ne précisent pas le type de mesures techniques devant être mises en œuvre par les fournisseurs d'accès à internet et laissent ce soin au juge.

En Europe, la Cour de justice de l'Union européenne veille sur ce point à ce que ne soit pas imposée aux intermédiaires la mise en œuvre de mécanismes de filtrage trop larges et coûteux.

Dans certains pays, pour la plupart anglo-saxons (Australie, Irlande, Royaume-Uni), les deux mesures de blocage de types « DNS » ou « IP » peuvent être mises en œuvre alternativement selon les circonstances d'espèce. Lorsque des mesures de blocage dites « IP » sont mises en œuvre, des contrôles sont réalisés en amont pour pallier les risques de surblocage afin de s'assurer que l'adresse IP devant être bloquée n'est pas partagée (une même adresse IP pouvant héberger différents services, licites comme illicites). Une notification à l'hébergeur est un des moyens permettant de s'assurer de l'absence de partage de l'adresse à bloquer.

[14] https://www.europarl.europa.eu/doceo/document/CULT-PA-658792_FR.pdf

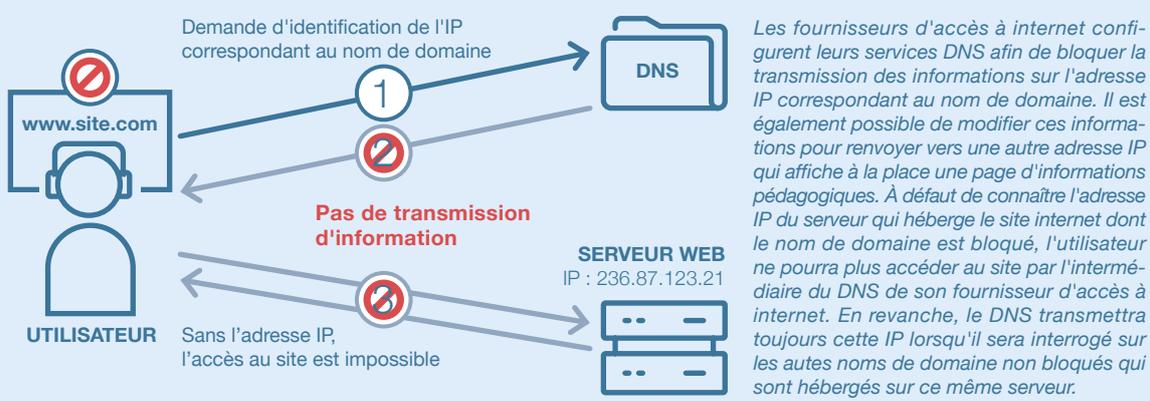
[15] https://www.europarl.europa.eu/doceo/document/JURI-PR-657490_EN.pdf

LES INJONCTIONS DE BLOCAGE DNS

Le blocage de type « DNS » consiste à priver l'internaute de l'accès à un site *via* son fournisseur d'accès à internet en bloquant le nom de domaine de ce dernier, si bien que lorsque l'internaute cherche à y accéder, soit en tapant directement le nom de domaine, soit *via* un lien (le cas échéant référencé par un moteur de recherche), la connexion n'aboutit pas. Cette mesure de blocage est mise en œuvre sur les serveurs DNS des fournisseurs d'accès à internet. Elle permet de bloquer l'accès à tout service ayant un nom de domaine, c'est-à-dire une adresse du type : nomdusite.com.

En cas de blocage DNS, il faut environ 24 heures pour créer un nouveau nom de domaine et faire connaître son adresse aux internautes (moteurs de recherche, réseaux sociaux, etc.). La stratégie de contournement des mesures de blocage de type « DNS » à laquelle recourent les administrateurs de sites illicites consiste, bien souvent, en cours d'actions judiciaires et avant même que la décision de blocage ne soit prononcée, à réserver plusieurs noms de domaine (similaires ou non) afin de rendre le site bloqué, ou une copie de celui-ci, accessible sous ce ou ces nouveaux noms de domaine. Les noms de domaine alternatifs peuvent être connectés aux serveurs originaux du site bloqué qui sont toujours en ligne et restent accessibles *via* leur adresse IP, puisque seuls les noms de domaine sont bloqués.

BLOCAGE DIT "DNS" : BLOCAGE DE NOMS DE DOMAINE



Les mesures de blocage DNS peuvent concerner le blocage, pérenne ou provisoire, de noms de domaine de sites de liens dédiés au *streaming* en direct de rencontres sportives comme de noms de domaine de plateformes d'hébergement de contenus dédiés au « *live streaming* » illicites ou de leurs sites intermédiaires.

Les injonctions judiciaires de blocage DNS

Au Danemark, en avril 2019, la ligue de football espagnole *La Liga*, en coopération avec *RettighedsAlliancen*, l'association de lutte contre le piratage, a obtenu en justice une injonction dynamique de blocage DNS à l'encontre de neuf services illicites de diffusion de rencontres sportives.

En Inde, en juin 2019, la haute cour de Delhi^[16] a rendu une ordonnance en référé, dans le cadre d'une procédure initiée par un groupe détenant les droits exclusifs des retransmissions radio des matchs de la coupe du monde du cricket – laquelle devait s'achever début

juillet 2019. Dans le cadre de l'ordonnance, les moteurs de recherche sont également tenus de supprimer de leurs résultats les site web/URL qui donnent accès à ces sites sur notification du défendeur.

À Singapour, dans le cadre d'une procédure intentée fin 2018 par Singtel, opérateur de télécommunications et fournisseur de services de télévision payants du groupe Fox, qui distribue plusieurs chaînes payantes, et la *Football Association Premier League* anglaise, la haute cour de Singapour a prononcé une injonction dynamique de blocage à l'encontre des noms de domaine de serveurs qui sont utilisés par les services diffusant les bouquets de chaînes illégalement

[16] High Court of Delhi, 03 juin 2019, CS (COMM) 326/2019 & I.A. 8510/2019 & 8508/2019 : <https://torrentfreak.com/images/Channel2-blocking-order-Delhi-High-Court.pdf>

(ces serveurs d'authentification permettent aux services illicites de vérifier que l'utilisateur qui veut accéder à l'offre est bien titulaire d'un abonnement valide).

En Espagne, le 11 février 2020, dans le cadre d'une procédure initiée par le diffuseur Telefónica Audiovisual Digital, le tribunal de commerce de Madrid^[17] a rendu une décision ordonnant le blocage dynamique de 44 services permettant la diffusion illicite des matchs de football en direct, et en particulier de serveurs d'authentification et d'aiguillage. Les ayants droit ont la possibilité de notifier les nouvelles adresses à bloquer aux fournisseurs d'accès à internet toutes les semaines sans avoir à repasser devant le juge. Les mesures de blocage devront être mises en œuvre dans les trois heures à partir de la notification des adresses à bloquer.

La décision court jusqu'au 25 mai 2022, soit pour trois saisons de football.

Les injonctions administratives de blocage DNS

En Italie, l'AGCOM peut ordonner des mesures de blocage à l'égard des sites proposant du *live streaming*. Ces injonctions ne sont cependant pas actualisées en temps réel.

Au Pérou, en 2018, l'Institut national de défense de la concurrence et de la protection de la propriété intellectuelle (Indecopi) a enjoint les fournisseurs d'accès à internet de bloquer le site de retransmission en direct de contenus sportifs *Rojadirecta* à la suite d'une demande de Fox Sports Latin America.

FOCUS SUR LE PORTUGAL : DU MODÈLE HISTORIQUE DE BLOCAGE DNS ADMINISTRATIF ET CONVENTIONNEL...

Au Portugal, un dispositif administratif de blocage (DNS) des sites illicites (sportifs et culturels) est mis en œuvre dans le cadre de deux *memorandum* (MoU) conclus principalement entre l'inspection générale des affaires culturelles (IGAC, entité rattachée au ministère de la Culture), l'association portugaise des opérateurs de télécommunications (APRITEL) et les ayants droit regroupés au sein du MAPINET (association anti-piratage plurisectorielle).

Le MoU, dédié à la mise en œuvre des mesures de blocage ponctuelles en direct, intitulé « Procédure technique pour les événements diffusés en direct », a été signé fin 2018. Il permet chaque semaine pendant les compétitions de football de bloquer de manière temporaire pour la durée du match au maximum 50 sites illicites par jour. Les sites qui peuvent être bloqués sont les services qui proposent des liens vers des contenus sportifs diffusés de manière non autorisée par des plateformes dites de « *live streaming* »^[18]. Ces mesures de blocage en direct interviennent dans un délai de 15 minutes et s'appliquent pour la durée du match. Les demandes de blocage ne peuvent intervenir qu'aux heures suivantes : du lundi au vendredi, de 17h30 à 22h45 et les samedis, dimanches et jours fériés, de 11h15 à 13h30 et de 15h30 à 22h.

En complément de ce dispositif, chaque mois, la MAPINET demande le blocage administratif pérenne, dans le cadre du premier MoU, des sites bloqués qui ont été ciblés par les mesures temporaires les semaines précédentes. Ainsi les mesures de « *live blocking* » sont moins nombreuses au fil du temps et ne visent que les nouveaux services illicites non encore identifiés.

... AUX INJONCTIONS JUDICIAIRES DYNAMIQUES DE BLOCAGE IP

L'écosystème a toutefois déjà évolué au Portugal depuis 2019 avec une croissance des offres IPTV illicites et un important contournement des mesures de blocage DNS par les internautes. Dans ce contexte, Nos Telecom, un des principaux opérateurs de télécommunications portugais et copropriétaire de la chaîne sportive Sport TV, a obtenu en justice à la suite de procédures initiées en mars et en octobre 2019, deux injonctions de blocage IP temporaire en temps réel : la première injonction prévoit que les mesures de blocage ne visent que les retransmissions des rencontres impliquant les quatre principales équipes de football portugaises diffusées par Sport TV ; la seconde injonction a permis que l'extension de ces mesures pour la saison 2019/2020 soit prononcée.

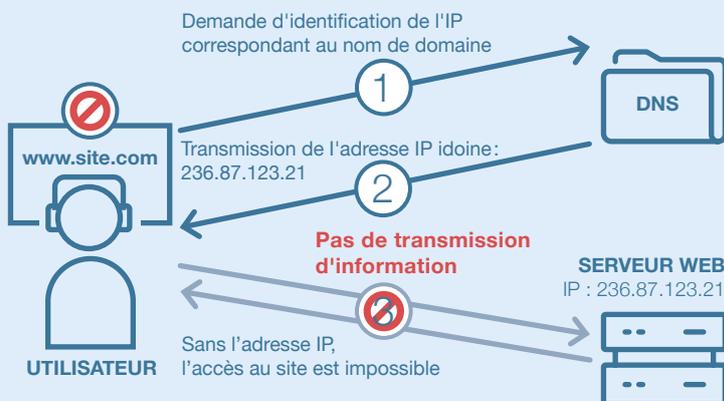
[17] Tribunal de commerce de Madrid, 11 février 2020, 28079470072020100001 : <https://www.poderjudicial.es/search/AN/openDocument/d1ecc270d29d6605/20200219>

[18] Une plateforme dédiée a été créée afin de permettre le fonctionnement du dispositif prévu par la procédure technique. Le prestataire des ayants droit (ou ces derniers) rentre dans la plateforme l'URL de la page d'un site de liens via lequel est accessible la rencontre sportive et joint des captures d'écran de cette page attestant de la diffusion. Ces preuves sont revues par l'association de lutte contre le piratage puis par l'autorité publique, qui ordonne le blocage en direct pour la durée du match.

LES INJONCTIONS JUDICIAIRES DYNAMIQUES DE BLOCAGE IP

Les mesures de blocage dites IP (*Internet Protocol*, Protocole Internet) consistent à empêcher le trafic en provenance ou à destination d'une adresse IP définie, qui est celle du serveur diffusant les contenus illicites.

BLOCAGE DIT "IP" : BLOCAGE DU TRAFIC AVEC LE SERVEUR



Le blocage IP consiste pour le fournisseur d'accès à internet à Interdire ou détourner les échanges entre les utilisateurs de son réseau et l'adresse IP d'un serveur web. En amont des mesures de blocage IP, certaines vérifications s'imposent pour s'assurer que le serveur en question est uniquement utilisé par le service illicite visé. Si d'autres services légitimes sont également hébergés sur le serveur (et utilisent donc la même adresse IP), ils seront en effet également bloqués, par effet collatéral.

Le blocage IP fonctionne quels que soient les noms de domaine et les liens utilisés pour accéder à l'adresse IP ciblée.

Seule une observation en conditions réelles sur une période significative est de nature à permettre de quantifier le nombre d'adresses IP à bloquer et à éviter les risques de surblocage. Par ailleurs, le blocage IP et les phénomènes de contournement qu'il suscite, plus rapides, peuvent impliquer un suivi et un besoin d'actualisation plus important, notamment pendant la diffusion de retransmissions sportives pour la mise en œuvre de mesures de blocage conservatoires.

Le recours à ce type de blocage est plus pertinent pour bloquer l'accès aux serveurs diffusant des bouquets de chaînes illicites IPTV qui n'ont pas de nom de domaine et dont l'accès à un serveur se fait directement à partir de l'adresse IP.

Le modèle historique du Royaume-Uni

La *Football Association Premier League* (FAPL), qui est l'entité qui administre la *Premier League*, le principal championnat de football professionnel pour les clubs anglais, a obtenu en 2017 la première décision requérant des principaux fournisseurs d'accès à internet britanniques qu'ils bloquent en direct de manière ponctuelle les serveurs des services retransmettant illégalement des enregistrements de matchs de football. L'injonction est limitée à la durée des matchs et est susceptible de se répéter sur une période correspondant à une saison.

En vertu de l'injonction cadre ordonnée par le juge, la FAPL (*via* ses prestataires) détecte chaque semaine les serveurs qui diffusent les contenus sportifs. Elle dresse la liste des adresses à bloquer qui est transmise aux fournisseurs d'accès à internet. En accord avec les parties, le protocole confidentiel de détection et sélection des adresses à bloquer est présenté au juge et actualisé dès que nécessaire.

Les fournisseurs d'accès à internet bloquent les serveurs de la liste au moment du match, sachant que la liste des adresses des serveurs à bloquer peut en outre être actualisée en temps réel et tout au long du match, de façon manuelle si nécessaire. En pratique, la communication des serveurs à bloquer s'effectue *via* une plateforme sécurisée avec au moins deux actualisations par date de match. La décision précise que les fournisseurs d'accès à internet ne peuvent qu'être tenus de faire leurs meilleurs efforts pour bloquer les services notifiés, selon la configuration de leur réseau et leurs ressources.

Dans les dix jours ouvrables à la suite de la mise en œuvre de la décision de justice, les fournisseurs d'accès à internet doivent informer par voie électronique leurs abonnés que l'accès à un nombre de serveurs associés à la diffusion illicite de matchs a été bloqué par décision de justice et que des mesures similaires vont intervenir pour la saison en cours.

Les internautes sont également informés de l'identité de la partie qui a obtenu la décision et du fait qu'ils peuvent saisir le juge.

L'Irlande

La haute cour d'Irlande, en se fondant sur la jurisprudence développée au Royaume-Uni, a rendu le 15 juillet 2019^[19] une injonction de blocage IP dynamique en temps réel, limitée à la durée des matchs, pour bloquer l'accès aux contenus sportifs de la *Premier League*. L'injonction s'applique jusqu'au 30 juin 2020, afin de couvrir la saison 2019/2020 de football. La *Premier League* peut demander le renouvellement de cette injonction devant le juge. En septembre 2020, l'UEFA a obtenu une injonction similaire pour la saison 2020/2021^[20].



[19] High Court Commercial, 15 juillet 2019, *the Football Association Premier League Limited v eircom limited trading as eir, sky ireland limited, sky subscribers services limited, virgin media ireland limited, vodafone ireland limited* : <http://www.courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/65ee8c8d1c26c939802584580041e0a7?OpenDocument>

[20] High Court Commercial, 29 septembre 2020, *Union des associations européennes de Football v eircom limited t/a eir, sky ireland limited, sky subscribers services limited, virgin media ireland limited and vodafone ireland limited* [https://www.baillii.org/cgi-bin/format.cgi?doc=/ie/cases/IEHC/2020/2020IEHC488.html&query=\(uefa\)](https://www.baillii.org/cgi-bin/format.cgi?doc=/ie/cases/IEHC/2020/2020IEHC488.html&query=(uefa))

II LA NÉCESSAIRE MOBILISATION DE L'ENSEMBLE DES ACTEURS DU NUMÉRIQUE

Le caractère tentaculaire et protéiforme du piratage implique nécessairement une pluralité d'outils et de stratégies de lutte, ainsi que la participation de tous les acteurs du numérique qui ne sauraient, par stricte neutralité ou simplement par inertie, continuer à éluder les difficultés liées à la profusion de contenus illicites sur internet. Certains acteurs, notamment dans le secteur de la publicité ou encore et dans une certaine mesure les moteurs de recherche, se sont engagés dans une démarche active consistant à améliorer le traitement des notifications qui leur sont transmises par les ayants droit.

Au-delà de l'implication de ces différents intermédiaires du piratage, une autre approche – actée en Europe par la directive du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique – consiste à associer à cette démarche participative les plateformes de partage de contenus générés par les utilisateurs, en vue de permettre soit le retrait d'œuvres dont la diffusion n'aurait pas été autorisée, soit leur monétisation en recourant à des technologies de reconnaissance de contenus.

2.1 | L'IMPLICATION DES DIFFÉRENTS INTERMÉDIAIRES DANS LA LUTTE CONTRE LE PIRATAGE

2.1.A | LES ACTEURS DE LA PUBLICITÉ EN LIGNE

Si les dispositifs d'assèchement ou d'identification des sources de revenus des sites illicites relevant de la mise en œuvre de la démarche dite « *Follow the money* » (« Suivez l'argent ») font consensus sur leur utilité, des questions se posent aujourd'hui sur les modalités de leur mise en œuvre, les effets de ces mesures et le bilan de leur efficacité. Se pose également la question de savoir comment sécuriser et accroître la portée de ces dispositifs pour permettre, au-delà de l'assèchement, la disparition de ces sites. Il s'agirait de construire des « ponts » entre les constats opérés dans le cadre des mesures d'assèchement et les actions judiciaires à mener contre les sites listés pour permettre ensuite la multiplication des décisions de blocage.

En France, le projet de réforme prévoit ainsi la possibilité pour le régulateur d'encourager la conclusion d'accords volontaires susceptibles de contribuer à remédier aux atteintes au droit d'auteur, aux droits voisins et aux droits des organisateurs de manifestations sportives. Il est en outre prévu que le régulateur ait une mission de carac-

térisation des services illicites *via* l'établissement d'une liste, laquelle pourrait être utilisée par les signataires des accords volontaires afin de sécuriser leurs actions.

Les dispositifs relevant d'une démarche volontaire des acteurs du secteur

Dans plusieurs pays, ces dispositifs relèvent aujourd'hui de la liberté contractuelle des acteurs signataires dans le cadre d'une autorégulation volontaire strictement privée sans réelle intervention publique (Australie, États-Unis, Japon, Pays-Bas, Suède, France). Les signataires de ces chartes de bonnes pratiques s'engagent ainsi, à titre principal, à consentir à prendre des mesures d'assèchement à l'égard des services ayant été considérés comme portant atteinte à la propriété intellectuelle. Concrètement, ils introduisent dans leurs contrats commerciaux des clauses de garantie excluant la diffusion de publicités sur les sites contrevenants.

Ce type de dispositif, outre l'assèchement des ressources des sites illicites, a un bénéfice en ce qu'il dégrade aussi la qualité de service et l'image de marque du site, dont le caractère illégal apparaît désormais plus facile à identifier pour le consommateur de bonne foi.

Toutefois, on constate, en France et à l'étranger, après quelques années d'application, que les sites massivement contrefaisants qui perdurent sont ceux qui s'adaptent aux mesures d'assèchement en se tournant vers des régies proposant des publicités dégradées (pornographie et jeux en ligne), d'autres moyens de paiement (monnaie virtuelle) ou encore d'autres sources de financement.

L'essor des dispositifs impliquant une intervention publique

L'intervention d'une autorité publique est prévue dans un nombre croissant de pays afin d'apporter de manière plus effective ces garanties en termes de fiabilité et de contrôle des sites objets des mesures, ainsi qu'une meilleure évaluation de l'impact et de l'efficacité de ces actions d'assèchement. Généralement, ces dispositifs s'inscrivent dans un système global beaucoup plus large prévoyant un ensemble de prérogatives plus vastes confiées aux pouvoirs publics en matière de blocage administratif de sites (Espagne) ou à la police dans le cadre d'une éventuelle procédure pénale (Royaume-Uni).

Au Brésil, en décembre 2019, le Conseil national de lutte contre le piratage et les crimes contre la propriété intellectuelle, organisme public-privé rattaché au ministère de la Justice, a signé un protocole d'accord avec les principaux acteurs de la publicité pour mettre en place un mécanisme de conformité afin d'empêcher la publicité sur les sites illicites. Dans la suite de ces accords, le Brésil a également signé un accord avec le Royaume-Uni et les États-Unis.

Au Danemark, notamment afin de garantir la compatibilité de la liste noire aux enjeux liés à la protection des données personnelles, il a été convenu de confier au ministère de la Culture la gestion de la liste des sites. Un accord en ce sens a été approuvé en janvier 2020.

En Inde, le nouveau projet de réglementation sur le commerce électronique publié début 2019 prévoit la mise en œuvre de mesures de type « *Follow the money* ».

En Espagne, un dispositif « *Follow the money* » a été imposé par la loi aux acteurs de la publicité. L'autorité publique en charge des mesures de blocage peut également identifier les organismes de paiement et de publicité partenaires du site en infraction pour leur demander de cesser de collaborer avec ce site sous la menace d'une sanction administrative allant jusqu'à 600 000 euros.

Au Royaume-Uni, à l'appui de signalements par les ayants droit de sites massivement contrefaisants, la PIPCU (unité spécialisée de la police de Londres) tient une liste des sites illicites dite « *Infringing Website List* » susceptibles de faire l'objet de poursuites pénales. Cette liste est disponible sur une interface automatisée, accessible à près de 250 partenaires volontaires du dispositif.

Cette démarche d'établissement d'une liste de services illicites ne doit pas être confondue avec celle dite de « *Name and Shame* » (ci-après) consistant à publier des listes d'acteurs peu vertueux pour stigmatiser leur irrespect des droits de propriété intellectuelle (incluant propriété industrielle et propriété littéraire et artistique), qui poursuit plusieurs objectifs.

De la même manière, dans les pays pratiquant le blocage administratif (Italie, Portugal), les listes de sites qui peuvent être rendues publiques n'ont pas cette finalité d'assèchement des ressources du site dès lors qu'elles portent sur les sites bloqués.

Les initiatives internationales

En Europe, la Commission met en exergue les difficultés juridiques du recours à de tels mécanismes d'auto-régulation au regard du droit de la concurrence, des libertés d'entreprendre et de communication sur internet ainsi que le besoin d'évaluation de leur efficacité et d'un meilleur suivi des plaintes sous la responsabilité d'un tiers indépendant. Afin de contourner ces obstacles, les analyses juridiques de la Commission (développées lors de l'élaboration du « *Memorandum of Understanding on online advertising and IPR* » (MoU) signé au niveau européen le 25 juin 2018) invitent à prévoir désormais des restrictions et des garde-fous pour éviter que des acteurs privés puissent être regardés comme étant juges du caractère contrevenant des sites.

En août 2020, la Commission européenne a publié un rapport sur la première année de mise en œuvre du MoU sur la publicité en ligne et les droits de propriété intellectuelle. Il ressort de ce rapport que les signataires estiment en général que le dispositif du MoU a bien fonctionné et que celui-ci a eu un impact sur la volonté des marques d'éviter de voir leurs publicités sur des services illicites^[21].

Parmi les pistes d'évolution et projets évoqués dans ce bilan, certains signataires souhaiteraient s'attaquer aux acteurs de la publicité qui n'ont pas adhéré aux initiatives volontaires du secteur et qui manquent de diligence quant au placement des publicités. Ces actions pourraient être conduites en coopération avec les autorités nationales ou internationales chargées d'établir des listes de services illicites.

Enfin, la proposition de règlement DSA prévoit d'instaurer une obligation de transparence sur les publicités diffusées par les plateformes sur internet, laquelle va dans le sens des mesures prises au titre de l'approche dite « *Follow the money* ».

Il faut également relever l'initiative, de portée plus large, de l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) qui a créé le dispositif « *WIPO ALERT*^[22] » proposant aux organismes autorisés des États membres, au premier rang duquel figurent les autorités publiques locales, de contribuer à une base de données centralisée listant les sites internet contrefaisants recensés à travers

[21] https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-of-understanding-online-advertising-ipr_en

[22] <https://www.wipo.int/wipo-alert/en/>

le monde, laquelle sera mise à disposition des acteurs de la publicité en ligne.

Après signature d'un accord avec l'OMPI, les utilisateurs autorisés reçoivent un sceau d'adhésion qu'ils peuvent utiliser pour montrer publiquement leur engagement contre le piratage en ligne, prévenir le détournement de la publicité dans l'écosystème numérique et protéger les intérêts et la réputation des marques.

Fin 2020, les premiers pays ayant adhéré au dispositif « *WIPO ALERT* » étaient les suivants : le Brésil, la Corée du Sud, l'Espagne, l'Équateur, l'Italie, le Japon, le Pérou, la Russie, l'Ukraine. Logiquement, compte tenu de l'organisation du dispositif, nombre de ces pays sont dotés d'une autorité publique ayant des missions de lutte contre le piratage.

2.1.B | LES INITIATIVES DE STIGMATISATION DITES « *NAME AND SHAME* »

Les initiatives de stigmatisation dites « *Name and Shame* » engagées par les États-Unis et par l'Union européenne consistent à dresser des listes publiques de services illicites dans l'objectif de stigmatiser les acteurs ou les marchés économiques peu vertueux. Si un des objectifs est de conduire des actions de plaidoyer à l'égard des pays dans lesquels des services listés sont domiciliés, l'objectif est également d'impliquer l'ensemble des acteurs du numérique, services illicites visés par les listes ainsi que leurs partenaires commerciaux, et de sensibiliser les internautes aux risques inhérents à la fréquentation des services listés.

L'administration américaine, via l'*United States Trade Representative* (USTR), une agence gouvernementale qui coordonne la politique commerciale des États-Unis, publie chaque année deux listes distinctes qui n'ont pas d'autres effets que de stigmatiser les acteurs les moins vertueux :

- une liste dite « *Special 301 List* », rédigée en vertu d'une loi, qui répertorie les pays qui ne fournissent pas une protection effective des droits de propriété intellectuelle^[23] ;
- la « *Notorious Markets List* », réalisée en-dehors de tout texte législatif, identifiant les marchés physiques et numériques dans le monde qui commettent ou incitent manifestement à la commission d'actes de contrefaçon de droits de propriété in-

dustrielle ou de droits d'auteur. Il faut relever que si jusqu'à présent, la liste visait seulement les marchés hors États-Unis, l'édition 2020 vise des antennes locales d'Amazon, compagnie pourtant basée aux États-Unis. La volonté première de l'agence gouvernementale est de faire réagir les opérateurs de ces marchés, mais également de mobiliser les gouvernements locaux. Il s'agit également d'alerter les consommateurs sur la nécessité de prendre leurs distances vis-à-vis de ces services illicites et des risques qu'ils peuvent encourir en les utilisant. La liste est publiée et actualisée chaque année. L'impact le plus important de la liste concerne les services légitimes qui tolèrent ce type d'agissement, et avec lesquels l'administration américaine travaille afin qu'ils concluent des accords. La liste est également utilisée pour engager des discussions avec les intermédiaires de l'écosystème de la contrefaçon tels que les services de paiement.

Le rapport met chaque année en lumière une problématique spécifique, laquelle peut être un défi particulier dans la lutte contre la contrefaçon ou un nouveau mode de piratage tel que le *stream ripping* illicite, qui a ainsi fait l'objet d'un focus dédié dans le rapport de 2018.

L'édition 2019 met ainsi en exergue la complexité de l'écosystème du piratage et le rôle déterminant joué par chacun de ces acteurs (les bureaux d'enregistrement de noms de domaine, les fournisseurs de services d'hébergement, les annonceurs et les réseaux de placement publicitaire, les acteurs du paiement, les réseaux sociaux et les moteurs de recherche), lesquels peuvent grandement contribuer à faciliter ou réduire le piratage. Ainsi, pour la première fois cette année, une régie publicitaire, Propeller Ads, est identifiée comme un marché notoire pour son rôle dans le financement des sites de piratage.

L'Union européenne, à l'image de ce que font les États-Unis, a publié pour la première fois en décembre 2018 une liste des marchés physiques et numériques (« *Counterfeit and Piracy markets watch list* »)^[24] – hors Union européenne – qui ont été signalés à la Commission comme portant atteinte aux droits de propriété intellectuelle ou facilitant ces atteintes^[25]. La seconde édition de la liste a été publiée le 14 décembre 2020^[26]. Les objectifs de cette liste sont d'intensifier les efforts à l'encontre de la contrefaçon commerciale pour protéger les intérêts européens et d'inciter tant les autorités locales que les opérateurs privés à prendre des mesures

[23] https://ustr.gov/sites/default/files/2020_Special_301_Report.pdf

[24] <http://trade.ec.europa.eu/doclib/press/index.cfm?id=1952>

[25] Aux fins d'établissement de la liste, la Commission a initié une consultation publique. Les informations ont ensuite été vérifiées par la direction « DG Trade » en lien avec l'EUIPO et Europol. Les marchés à inscrire sur la liste ont ensuite été sélectionnés.

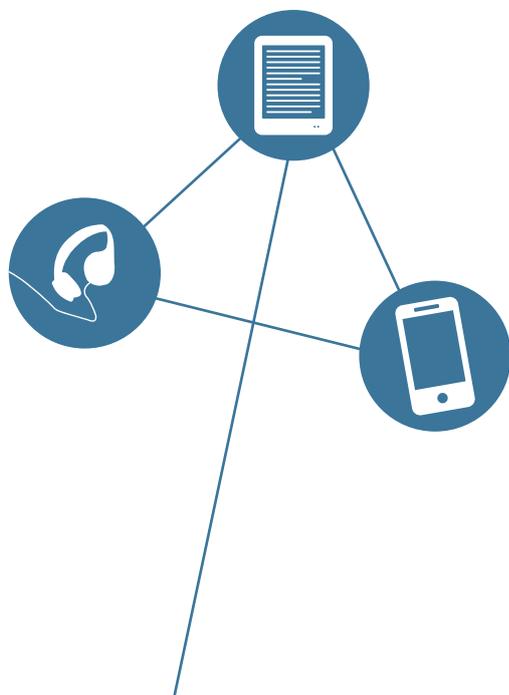
[26] https://trade.ec.europa.eu/doclib/docs/2020/december/tradoc_159183.pdf

pour lutter contre la contrefaçon. La liste est établie à partir des contributions reçues à la consultation publique organisée par la Commission et des investigations réalisées par les services avec l'assistance de l'Office de l'Union européenne pour la propriété intellectuelle (EUIPO) et d'Europol. Des recherches de titres ou de marques populaires ont été effectuées sur les services listés. Les mesures volontaires prises par les plateformes pour lutter contre la présence de contenus illicites ont enfin été signalées par les parties prenantes et il en a été tenu compte. Surtout, la Commission a cherché à entrer en contact avec tous les services listés.

Lorsqu'elle le peut, la Commission précise, pour chaque acteur, le rôle joué dans l'écosystème, le pays dans lequel il est hébergé, le pays où réside son opérateur, ses moyens de financement, le nombre de visites en juin 2020, son classement au sein des sites internet les plus populaires, le(s) pays où le service est particulièrement populaire et s'il a fait l'objet d'une décision judiciaire dans certains États.

Pour le droit d'auteur, les acteurs visés sont très divers et recouvrent l'ensemble de l'écosystème : *cyberlockers*, services de *stream ripping* illicites, sites de liens, sites de liens pair à pair, sites dédiés à des applications, sites payants de téléchargement illicite, prestataires de services d'hébergement. Pour cette seconde édition, la Commission a créé deux nouvelles catégories : les services IPTV illicites et les réseaux sociaux.

En France, le projet de réforme prévoit d'attribuer à l'autorité publique la charge de dresser une liste de services illicites, laquelle aura un effet de stigmatisation (« *Name and shame* ») et d'information du public. Pour autant, elle ne sera pas susceptible d'interdire ni de limiter, par elle-même, l'activité du site ou du service en cause. Son intérêt résidera alors dans son utilisation par les acteurs économiques dans le cadre d'initiatives volontaires de lutte contre le piratage, voire par le juge dans le cadre d'instances judiciaires initiées par les ayants droit.



2.1.C | LES FOURNISSEURS DE SERVICES D'HÉBERGEMENT

Les fournisseurs de services d'hébergement sont des maillons essentiels de l'écosystème dont le régime de responsabilité est prévu dans la plupart des pays, souvent sur le modèle du *Digital Millennium Copyright Act* (DMCA) américain, datant de 1998 ou de la directive 2000/31/CE du 8 juin 2000 dite « commerce électronique ». Ces textes prévoient en substance que la responsabilité de ces acteurs ne peut être engagée dès lors qu'ils assurent le retrait ou l'inaccessibilité à bref délai des contenus illicites qui leur sont notifiés.

L'actualisation du cadre législatif à la lumière des défis actuels semble aujourd'hui faire consensus en Europe, la directive dite « commerce électronique », n'ayant pas atteint tous ses objectifs et se révélant insuffisante face aux nouveaux enjeux liés à la transformation numérique, la Commission européenne a présenté le 15 décembre 2020 la proposition de règlement DSA précitée.

Il ressort de la proposition de règlement que les grands principes de la directive « commerce électronique » ne sont pas véritablement bouleversés, seulement aménagés et précisés, en particulier à l'égard des hébergeurs.

Concernant le dispositif de notification et de retrait, est prévu un mécanisme normalisé, accessible et convivial, sans pour autant qu'un délai de traitement soit imposé. Le délai de retrait des contenus illicites par les services d'hébergement est pourtant un des axes de la lutte contre le piratage de contenus sportifs.

Des propositions en ce sens sont d'ailleurs actuellement discutées au Parlement européen, dans l'optique de demander à la Commission de déposer une proposition législative, au cœur de laquelle pourrait figurer l'instauration de mesures de retrait dans un délai adapté à la diffusion en direct (en temps réel ou en 30 minutes). La conclusion d'accords privés entre les parties prenantes est également un des axes envisagés.

Enfin, en l'état, la proposition de DSA n'a pas donné suite à la demande des ayants droit dite « *Know your customer* » ou « connais ton client », notamment promue par la *Motion Picture Association*, consistant à imposer aux intermédiaires techniques, et notamment aux fournisseurs de services d'hébergement, de mettre en œuvre un protocole proportionné et efficace pour vérifier l'identité de leurs clients sur la base de documents, données ou informations validés (comme l'enregistrement de la société ou toute autre preuve d'identité suffisante). Une obligation en ce sens figure en effet dans la proposition de DSA mais elle ne concerne que les places de marché – et donc surtout les titulaires de marques.

Aux Pays-Bas, l'association anti-piratage, la BREIN, promeut la nécessité pour les intermédiaires techniques néerlandais de vérifier l'identité de leurs clients et d'exiger contractuellement la même chose de leurs clients qui revendent leurs services. En 2020, la BREIN a intenté, en collaboration avec la *Motion Picture Association*, des actions contre trois intermédiaires techniques pour qu'ils mettent en œuvre des mesures leur permettant de disposer d'informations fiables sur l'identité de leurs clients, qu'ils pourraient transmettre aux ayants droit en cas de violation de la propriété intellectuelle, et exigent la même chose de leurs revendeurs.

2.1.D | LES MOTEURS DE RECHERCHE

En droit américain, les moteurs de recherche disposent également d'un régime de responsabilité allégée dit « *safe harbor* » reposant sur le principe dit de notification et de retrait (en anglais « *Notice and Take down* »).

En Europe, la directive dite « commerce électronique » n'aborde pas expressément le rôle des moteurs de recherche. Lors de l'adoption de ce texte, les moteurs de recherche n'étaient en effet pas encore aussi développés^[27]. Aujourd'hui, les moteurs de recherche peuvent être assimilés dans les communications de la Commission européenne aux acteurs plus génériquement connus sous le terme de « plateformes » d'hébergement de contenus.

Afin de permettre le signalement par les ayants droit de liens pointant vers des contenus contrefaisants, les moteurs de recherche disposent de mécanismes automatisés de retrait (dit « *Take down notices* »). Google publie ainsi par exemple un « *Transparency Report* »^[28] actualisé en temps réel dans lequel figure le nombre de notifications des ayants droit que le moteur de recherche a reçu ainsi que l'auteur de la demande et le site concerné.

Dans la très grande majorité des pays étudiés, le rôle des moteurs de recherche dans la lutte contre le piratage est évoqué concernant, d'une part, le déréférencement ou le sous-référencement de l'offre illégale et, d'autre part, le sur-référencement de l'offre légale. Si l'implication des moteurs à ces différents égards passe de plus en plus souvent par des accords conclus dans le cadre d'une démarche volontaire, la question peut cependant se poser de la création d'un régime de responsabilité propre aux moteurs de recherche. Ces mêmes dispositions pourraient également encourager à la signature d'accords volontaires entre les parties prenantes et les moteurs de recherche, sous l'égide de l'autorité publique le cas échéant, de nature à permettre la mise en place d'une stratégie commune agile s'agissant du déréférencement des sites illicites – et notamment dans le cadre de l'actualisation de mesures de blocage ordonnées par le juge ou l'autorité publique – voire du sous-référencement de l'offre illicite. La proposition de règlement *Digital Services Act* précitée ne qualifie pas expressément les moteurs de recherche. Il a seulement été précisé que ce texte ne remettait pas en cause les instruments sectoriels spécifiques existants tel que le Règlement 2019/1150 du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne, lequel concerne expressément les moteurs de recherche. Des voix se sont cependant élevées pour demander à ce que leur prise en considération par ce texte soit clarifiée.

Les moteurs pourraient ainsi être visés par les dispositions créant un cadre général pour la régulation des plateformes en lien avec la lutte contre les contenus illicites et préjudiciables et instaurant une nouvelle norme de transparence à leur charge. Ces nouvelles obligations comprennent notamment l'obligation pour les plateformes les plus importantes de donner accès à leurs algorithmes et de fournir des explications à leur sujet, sur injonction de la Commission européenne. Par ailleurs, le dispositif de régulation envisagé par le DSA octroie un rôle prépondérant au régulateur local, avec lequel les moteurs seront tenus de collaborer (sur la régulation des plateformes, voir également ci-après au 2.3).

[27] La directive prévoyait en son article 21 (réexamen) qu'un rapport relatif à son application et son adaptation, notamment concernant la responsabilité des moteurs de recherche, serait dressé par la Commission tous les deux ans. Un tel rapport a été présenté au Parlement européen le 21 novembre 2003. Il y était précisé que « [s]i la couverture des [...] moteurs de recherche par la directive n'a pas été considérée comme nécessaire, la Commission a encouragé les États membres à renforcer la sécurité juridique pour les prestataires intermédiaires de services internet ». Ce rapport mentionnait également le fait que la Commission continuerait à « [examiner] la nécessité d'adapter le cadre actuel pour tenir compte de ces développements, par exemple d'ajouter des limitations supplémentaires de responsabilité pour [...] les services de moteurs de recherche ».

[28] www.google.com/transparencyreport/removals/copyright/?hl=fr

Le déréférencement de liens pointant vers une œuvre contrefaisante

En matière de droit d'auteur, les ayants droit obtiennent semble-t-il sans trop de difficultés le déréférencement de liens pointant vers des pages de site mettant à disposition des œuvres contrefaisantes. Toutefois, ce type d'action pris isolément n'a pas d'effet sur l'indexation du site lui-même et son rang dans les résultats des recherches des internautes formulées sur le moteur.

Par ailleurs, cela implique pour les ayants droit de devoir solliciter la désindexation d'une œuvre, lien par lien, et donc d'obtenir son retrait, page par page, pour un site qui en compte des milliers. Or, de telles notifications sont longues et coûteuses.

C'est pour pallier ces difficultés que l'on constate la multiplication d'accords volontaires entre les ayants droit et les moteurs de recherche aux fins de fluidifier et faciliter le déréférencement de liens pointant vers une œuvre contrefaisante.

Le défi de l'implication des moteurs tient – outre les enjeux de transparence des modalités de fonctionnement de leurs dispositifs – davantage à résoudre les difficultés rencontrées par les ayants droit pour obtenir le sous-référencement d'un site illicite sans avoir à procéder à la notification massive de liens pointant vers les œuvres illicites présentes sur ledit site.

Le sous-référencement de sites illicites

Le sous-référencement dégrade le positionnement du site (comme celui de ses pages) dans les résultats de recherche mais ne le supprime pas de l'index. La conclusion d'accords volontaires entre ayants droit et moteurs de recherche semble de nature à faciliter le sous-référencement des sites illicites par ces derniers sur signalement des ayants droit. Toutefois, ces accords rencontrent certaines limites, notamment en cas de changements de nom de domaine ou de sous-domaine, car le nouveau site met alors un certain temps avant d'être à son tour déclassé.

Dans son rapport « *How Google fights piracy* »^[29], Google évoque, au titre des efforts mis en œuvre depuis plusieurs années, une fonctionnalité permettant de donner plus de poids aux demandes de retrait des ayants droit intitulée « *Demotion signal* ». Cette fonctionnalité établit une corrélation entre les demandes de retrait concernant un site et son classement. Dans le cadre de discussions locales, Google a amélioré

l'efficacité de cet outil. Un des problèmes identifiés tient notamment aux différences sectorielles s'agissant du nombre de notifications envoyées. Le secteur musical est en effet assez actif (car il lui est possible de notifier par exemple l'ensemble des chansons d'un album sur un même site), quand les ayants droit de l'audiovisuel ou de l'édition demandent le retrait d'un seul film ou d'un seul livre. Google indique qu'il accorde désormais plus de poids aux notifications concernant certaines œuvres telles que par exemple les œuvres audiovisuelles non encore sorties ou encore diffusées en salle.

Aux États-Unis, l'administration américaine soutient le développement de bonnes pratiques pour parvenir à des solutions adaptées au problème du positionnement des sites massivement contrefaisants dans les résultats des recherches faites *via* les moteurs de recherche. Google y met dorénavant en œuvre son outil de pondération des demandes de retrait, de la même façon qu'au Royaume-Uni.

Au Royaume-Uni, les engagements pris par les moteurs portent à ce stade principalement sur le sous-référencement des offres illégales dans la version britannique de leur moteur. Un accord a été conclu en février 2017, sous l'égide du gouvernement, entre les moteurs de recherche^[30] et les ayants droit^[31]. Cet accord est un code de bonne conduite juridiquement non contraignant. Il a pour objet d'engager les moteurs à respecter des règles conduisant à sous référencer ou à rétrograder des résultats de recherche (et donc à faire disparaître des premières pages) les sites massivement contrefaisants signalés. Il cherche à optimiser tant les résultats des recherches effectuées avec des mots-clés neutres par des consommateurs qui ne cherchent pas spécifiquement des offres illicites que les premiers résultats de recherche (les plus pertinents pour la génération de trafic vers des sites). C'est notamment dans le cadre de cet accord que des discussions ont eu lieu sur la nécessité de pondérer les demandes de retrait et sur les moyens d'améliorer l'efficacité du sous-référencement en lien avec les demandes de retrait.

[29] https://blog.google/documents/27/How_Google_Fights_Piracy_2018.pdf

[30] Google, Microsoft (Bing) et Yahoo pour les moteurs de recherche.

[31] La British Phonographic Industry (BPI) pour la musique et la Motion Picture Association (MPA) pour l'audiovisuel.

Le déréférencement de sites illicites

Le déréférencement d'un site implique pour le moteur de le supprimer totalement de l'index de recherche et donc des résultats.

Sauf à ce qu'une autorité publique ou judiciaire ou une législation particulière les y enjoignent, les moteurs de recherche ne mettent généralement pas en œuvre de politique interne de déréférencement des sites, et ce pour des motifs de neutralité à l'égard des contenus, de pluralisme, de respect de la liberté d'expression ou encore de la liberté d'entreprendre et de la libre concurrence.

Dans ce contexte, seuls quelques pays ont expressément introduit une disposition dans leur *corpus* juridique

permettant d'obtenir le déréférencement de sites entiers (Australie, Espagne, France, Russie, Vietnam).

Toutefois, on assiste récemment à une multiplication des accords volontaires concernant le déréférencement de sites illicites entre ayants droit et moteurs de recherche. Le cas échéant, ces accords peuvent être conclus sous l'égide de l'autorité publique. Certains de ces accords ont fait l'objet d'une communication officielle mais il semble qu'ils aient souvent vocation à demeurer confidentiels. Une autre tendance forte est que même dans les pays qui avaient adopté une législation permettant expressément le déréférencement dans le cadre d'une procédure visant à voir également ordonné le blocage des sites à déréférencer, la voie de l'accord est aujourd'hui également privilégiée.

En Australie, une loi (*Copyright Amendment (Online Infringement) Bill 2018*) adoptée en novembre 2018 permet aux ayants droit d'obtenir des mesures judiciaires de déréférencement. Cette disposition ne semble cependant pas avoir été mise en œuvre : en effet, en mai 2019, Google a volontairement consenti à déréférencer 832 sites illicites. Ces déréférencements ont fait suite à un accord convenu entre les ayants droit et les fournisseurs d'accès à internet australiens.

En Espagne, l'administration souhaiterait également mettre en place un code de conduite volontaire entre les ayants droit et les intermédiaires d'internet, et notamment les moteurs de recherche.

En France, l'article L. 336-2 du Code de la propriété intellectuelle prévoit une procédure *sui generis* qui permet au juge d'ordonner « toutes mesures propres à prévenir ou à faire cesser une atteinte au droit d'auteur [...] à l'encontre de toute personne susceptible d'y remédier ». Ce dispositif donne donc la possibilité aux ayants droit de solliciter une injonction à l'égard des moteurs de recherche de procéder au déréférencement de sites illicites. Toutefois, il résulte de la jurisprudence récente que les décisions de blocage ne visent désormais plus les moteurs de recherche en même temps que les fournisseurs d'accès à internet, les demandes d'injonctions de déréférencement de sites étant, le cas échéant, formées par les ayants droit dans le cadre de procédures simplifiées et dédiées à cette seule demande.

Au Japon, en juillet 2019, Google et les représentants des ayants droit ont signé un accord pour échanger sur le référencement des sites illicites, dans le cadre duquel les parties s'engagent à échanger sur la lutte contre le piratage sous l'égide de l'agence des Affaires culturelles.

En Russie, un accord en vigueur depuis 2018 entre les ayants droit, des plateformes et des moteurs de recherche, oblige ceux-ci à prendre des mesures à l'égard des sites figurant sur une base de données centralisée, créée par le régulateur local. Toutes les cinq minutes, les opérateurs des plateformes de recherche doivent interroger la base de données pour obtenir des mises à jour. Ils doivent alors supprimer les URL obtenues de leurs résultats en Russie dans un délai de 6 heures. En cas de conflit entre les signataires, l'accord prévoit une procédure de médiation, avec l'aide du régulateur.

Une autre limite tient au fait que ce type de mesures doit, en tout état de cause, être associé à une amélioration du référencement de l'offre légale. Tel est d'ailleurs l'objet de la contrepartie des engagements pris par les moteurs au Royaume-Uni, les ayants droit devant faire en sorte que l'offre légale soit mieux référencée par les moteurs de recherche en optimisant leur stratégie de référencement (*Search Engine Optimization*).

Le sur-référencement de l'offre légale

Le sur-référencement de l'offre légale ou la présentation de l'offre légale dans une rubrique dédiée a longtemps semblé exclu par les moteurs eux-mêmes, pour des raisons notamment de neutralité à l'égard des contenus et de libre concurrence.

On distingue toutefois deux types d'initiatives en faveur de l'offre légale susceptibles d'être menées par les moteurs de recherche consistant :

- à améliorer l'articulation des fonctionnalités du moteur de recherche (dites « *Search* ») avec celles proposant des suggestions de mots-clés (dites « *AutoComplete* »), en évitant des suggestions de mots qui mènent le consommateur vers des sites illégaux ;
- plus spécifiquement pour Google, à développer les initiatives du type « *Watch and listen* » pour mettre en valeur l'offre légale dans le cadre de partenariats commerciaux.

Aux Pays-Bas, l'industrie cinématographique a lancé en février 2017, après la création d'un portail référençant les plateformes de l'offre légale, un moteur de recherche de l'offre légale par œuvre qui vise les internautes qui cherchent une œuvre audiovisuelle en particulier. L'originalité de cet outil est qu'il vise aussi les internautes qui cherchent une œuvre illégalement mise à disposition. En effet, la description des œuvres comporte des mots-clés comme « *torrents* » ou « *téléchargement illégal* » pour que les internautes qui utilisent ces mots-clés puissent être redirigés sur l'offre légale. Ensuite, pour chaque œuvre audiovisuelle, dans la description, un message est disponible pour dissuader les internautes de se tourner vers l'offre illégale de type « *Ne téléchargez pas illégalement. Dirigez-vous vers une offre légale sûre et rapide* ».

• 2.1.E | LES SERVICES D'OPTIMISATION DU TRAFIC OU RÉSEAUX DE DIFFUSION DE CONTENUS

Les services de *Content delivery networks* (CDN) ou réseaux de diffusion de contenus fournissent à leurs clients des infrastructures réseaux capables d'optimiser la mise à disposition de contenus auprès des utilisateurs, en particulier lorsque la clientèle du service est domiciliée dans différents pays. Ces services sont utilisés par des acteurs tant licites qu'illicites et en particulier par des acteurs diffusant des contenus audiovisuels en quantité, opération gourmande en bande passante qui justifie le recours aux services des CDN. Un des CDN les plus importants de ce secteur est l'opérateur technique Cloudflare, établi aux États-Unis, dont les services sont utilisés par nombre de sites contrefaisants – mais également par des services licites.

Ce service, outre ses prestations de CDN, offre également plusieurs services techniques dont un service dit de « *reverse proxy* », qui consiste à centraliser toutes les connexions entrantes ou sortantes de/vers un site dans l'optique de protéger le site contre d'éventuelles attaques. Cela a cependant pour effet de masquer l'adresse IP et l'identité du véritable hébergeur d'un site. L'anonymisation des sites illicites qui en découle gêne ainsi considérablement les opérations de lutte contre le piratage car cela complique la localisation précise du site internet.

À ce titre, il figurait sur la première édition de la liste des marchés physiques et numériques signalés à la Commission européenne comme portant atteinte aux droits de propriété intellectuelle ou facilitant ces atteintes – « *Counterfeit and Piracy markets watch list* » – publiée par la Commission européenne en décembre 2018. La seconde édition de cette liste, publiée en décembre 2020, ne recense plus Cloudflare parmi les acteurs illicites.

La Commission fait état en revanche du débat quant à son rôle dans la lutte contre le piratage et l'importance de la coopération avec les titulaires de droits, abordé dans nombre de contributions à la consultation publique préalable à la constitution de la liste. Elle rapporte que des parties prenantes ont demandé à Cloudflare d'améliorer sa coopération avec les titulaires de droits, notamment sa réactivité aux notifications et ses pratiques lors de l'ouverture de comptes afin d'empêcher les sites illégaux d'utiliser ses services. Elle relate que Cloudflare a, pour sa part, indiqué que la mise à disposition générale des adresses IP des sites utilisant ses services compromettrait la protection des sites de ses clients contre les menaces ou les cyberattaques. La société a également fait savoir qu'elle prend des mesures appropriées, par le biais d'un système de signalement des abus et d'un programme facilitant les notifications pour les acteurs de confiance, de sorte que les ayants droit disposent des informations nécessaires pour initier des démarches auprès des fournisseurs d'hébergement et des opérateurs de sites en mesure de donner suite à leurs plaintes.

En conclusion, la Commission invite les CDN et les titulaires de droits à coopérer davantage de façon à contribuer à faciliter l'application des droits violés par les clients des CDN.

En France, la jurisprudence la plus récente met notamment en exergue, pour caractériser l'illicéité des sites à bloquer, l'anonymisation intégrale de ces sites par le biais notamment du prestataire Cloudflare, différents éléments qui « *tendent à démontrer la connaissance du caractère entièrement illicite des liens postés sur les sites litigieux par les personnes qui contribuent à cette diffusion et l'impossibilité pour les auteurs et produc-*

teurs de poursuivre les responsables de ces sites ».

Dans le contexte du *Digital Services Act*, au regard du rôle joué par les CDN et de la multiplicité des services qu'ils proposent, la question se pose d'encourager ces acteurs à lutter contre l'utilisation de leurs services à des fins illicites par différents biais tels que par exemple la possibilité de mise en place de mesures de blocage géographiques de sites reconnus comme illicites ; la communication de l'adresse IP de sites aux autorités publiques et aux organisations reconnues du secteur privé dans des délais et des conditions qui permettent une lutte effective contre les sites

illicites. Le considérant 27 du *Digital Services Act* précise seulement que les réseaux de diffusion de contenus pourront bénéficier du même régime de responsabilité que les autres intermédiaires techniques, dès lors qu'il est possible de les rattacher à une des catégories prévues par ce texte, à savoir les services offrant une infrastructure de réseau, les services de cache et les hébergeurs. On peut ainsi en déduire que des mesures de cessation pourront être prises à leur encontre mais des voix s'élèvent déjà pour demander à ce que leur statut et leurs obligations soient expressément clarifiées, et ce pour l'ensemble de leurs activités et notamment celles dites de *reverse proxy*.

En Allemagne, dans le cadre d'une procédure intentée par les ayants droit de la musique, le tribunal de Cologne a estimé le 30 janvier 2020^[32] qu'un fournisseur d'un réseau de diffusion de contenu ou CDN (en l'espèce Cloudflare) pourrait voir sa responsabilité engagée s'il ne prenait pas des mesures à l'encontre du site illicite en cause. Le tribunal l'a ainsi enjoint de cesser de faciliter l'accès aux contenus protégés visés dans la procédure en bloquant l'accès sous peine de devoir payer une amende allant jusqu'à 250 000 euros par infraction ou, à titre subsidiaire, le directeur général de Cloudflare pourrait être condamné à une peine de six mois de prison.

En Italie, dans le cadre d'une procédure intentée contre Cloudflare par Reti Televisive Italiane s.p.a. (RTI), le Tribunal des entreprises de Rome a, par décision de juillet 2019^[33], confirmé en appel que certaines des activités de Cloudflare s'apparentaient à des services d'hébergement par opposition à une simple mise en cache, ce qui incluait notamment la fonction par laquelle Cloudflare copie une partie des sites sur son serveur, afin de les rendre accessibles en cas de problèmes techniques avec les fournisseurs d'hébergement des sites.

La décision pose également que Cloudflare avait connaissance de l'existence des activités illicites de ses clients et n'avait par conséquent pas droit au bénéfice du régime de responsabilité limitée prévu pour les intermédiaires techniques.

En 2020, Cloudflare a par ailleurs conclu un accord volontaire avec l'autorité publique locale, l'AGCOM, permettant à celle-ci d'avoir connaissance de l'adresse IP et donc de l'hébergeur réel d'un service illicite ou, si le site est hébergé par Cloudflare, lui garantissant que sa notification de l'AGCOM est transmise à l'opérateur du service pour action.

En Russie, au cours du mois d'octobre 2019, l'action concertée de l'ACE, de la BREIN et de la MPA a entraîné la fermeture du réseau de diffusion de contenu *Moonwalk* fournissant des contenus audiovisuels à environ 80 % des sites illicites russes.

[32] Tribunal de Cologne, 30 janvier 2020, n° 140 171/19,

http://www.hadopi.info/dj/news/ressources/20200316%20Cloudflare%20judgment%20Cologne%20first%20instance%20ENGLISH_redacted.pdf

[33] CloudFlare - CloudFlare Inc. and Reti Televisive Italiane s.p.a. (RTI) R.G.26942/2019, juillet 2019.

2.1.F | LES GESTIONNAIRES DE REGISTRE ET LES BUREAUX D'ENREGISTREMENT DES NOMS DE DOMAINE

L'implication des gestionnaires de registre ou des bureaux d'enregistrement constitue également l'un des outils de la lutte contre la contrefaçon.

Les gestionnaires de registre dits « *registries* » en anglais sont les entités en charge de la gestion de la base de données des noms de domaine de premier niveau ou des adresses IP pour une région définie. Les bureaux d'enregistrement dits « *registrars* » sont des organismes qui assurent, dans le cadre d'une prestation payante, l'enregistrement et l'hébergement de noms de domaine auprès des gestionnaires pour lesquels ils sont accrédités. En pratique, les bureaux d'enregistrement permettent l'enregistrement de domaines de premier niveau dits génériques (.com, .net, .org, etc.). Ils doivent être accrédités par l'*Internet Corporation of Assigned Names and Numbers* (ICANN). Les domaines de premier niveau nationaux (.fr, .eu, .uk, etc.) sont quant à eux gérés par des entités locales, qui accréditent le plus souvent les bureaux à même de proposer l'enregistrement des noms de domaine afférents.

Le « *WHOIS* » est un annuaire recensant les données techniques et de contact des noms de domaine principalement administré par les registres et les bureaux d'enregistrement.

Tant les bureaux d'enregistrement que les gestionnaires de registres sont en principe susceptibles de suspendre ou ordonner le transfert de noms de domaine lorsqu'un compte est associé à des activités répréhensibles, ce qui oblige par exemple les sites massivement contrefaisants à changer de nom de domaine.

Certains bureaux d'enregistrement ont mis en place des politiques qui interdisent l'utilisation des noms de domaine à des fins illicites et sont réactifs lorsqu'ils reçoivent des plaintes ou encore pour suspendre ou verrouiller les noms de domaine de sites illicites.

Suite à l'adoption du Règlement général européen sur la protection des données (RGPD) du 23 mai 2018, s'est cependant posée la délicate question de l'articulation entre les exigences de protection des données personnelles et la publication des informations d'identification et de contact des titulaires et responsables de noms de domaine contenus dans les « *WHOIS* », essentielle aux fins d'identification des titulaires de noms de domaine utilisés à des fins illicites.

Par ailleurs, la Commission européenne assimilerait vraisemblablement le régime des bureaux d'enregistrement à celui applicable aux fournisseurs d'accès à internet tel qu'issu de la proposition de DSA précitée. Reste que ces acteurs étant souvent basés hors de l'Union européenne, obtenir que ceux-ci mettent en œuvre des mesures de cessation sera vraisemblablement moins aisé et rapide qu'une action à l'encontre d'acteurs locaux.



En Allemagne, il a été jugé dans le cadre d'une procédure intentée par les ayants droit de la musique qu'un bureau d'enregistrement pouvait être tenu responsable des infractions commises par un site contrefaisant si celui-ci n'a pas procédé à la suspension de son nom de domaine alors qu'il a reçu une notification lui signalant le caractère manifestement illicite de ce site^[34].

En Belgique, les registres ont été pleinement reconnus par la jurisprudence comme étant des services de la société de l'information contre lesquels les titulaires de droits peuvent solliciter des mesures^[35].

Au Danemark, un code de 2014 entre les ayants droit et les fournisseurs d'accès à internet définissait les conditions de blocage de sites. Celui-ci a été amendé en 2020 sur différents points, et notamment pour permettre le blocage des noms de domaine locaux en « dk. » Ceux-ci étaient auparavant exclus du code car les titulaires de droits devaient en principe pouvoir obtenir leur désactivation par les bureaux d'enregistrement – mais il s'est avéré à l'usage qu'obtenir cette désactivation était un processus compliqué.

Aux États-Unis, il n'est pas possible en l'état du droit positif d'obtenir des mesures de blocage. En revanche, la saisie de noms de domaine peut être obtenue *via* les actions conduites par le *National Intellectual Property Rights Coordination Center*, entité chargée de la lutte contre la contrefaçon qui dépend de l'Office des douanes et de l'immigration américain, en particulier dans le cadre d'une opération dite « *In Our Sites* », conduite en lien avec Europol et Interpol. À la place des sites saisis, les internautes accèdent à une bannière pédagogique.

En Espagne, parmi les mesures que peut solliciter, sous le contrôle du juge, l'autorité publique espagnole en charge de la lutte contre le piratage, figure la demande à un hébergeur de cesser de fournir ses prestations et la demande de suspension du nom de domaine du site si celui-ci est en « .es » ou sous une autre extension gérée par le registre national.

Au Royaume-Uni, l'identification d'un site illicite par la police de Londres conduit à l'envoi d'un courrier au bureau d'enregistrement du nom de domaine ou à l'organisme en charge de la gestion de l'extension sous laquelle le nom de domaine a été enregistré pour demander la suspension du nom de domaine.

Au Pérou, l'autorité publique locale, l'Indecopi, cherche à conclure un accord avec GoDaddy, l'un des principaux bureaux d'enregistrement de noms de domaine du monde, basé aux États-Unis, afin de donner un cadre à la collaboration informelle qui s'est déjà nouée entre les deux entités, dans le but que l'Indecopi puisse demander la suspension de noms de domaine enregistrés aux États-Unis mais visant le public péruvien.

2.2 | L'IMPLICATION DES PLATEFORMES DE PARTAGE DE CONTENUS EN LIGNE

2.2.A | LA QUESTION CENTRALE DU STATUT DES PLATEFORMES

Le développement des grandes plateformes du numérique interroge depuis plusieurs années les pouvoirs publics sur le cadre réglementaire à appliquer à ces nouveaux acteurs afin d'établir un jeu concurrentiel sain tout en respectant les spécificités d'internet.

En concurrence avec des services tels que les éditeurs de services de *streaming* musicaux ou audiovisuels, les intermédiaires d'internet remettent en question les fondements mêmes du droit d'auteur et des droits voisins qui ont notamment pour objet de permettre à leurs titulaires d'autoriser – en négociant les conditions –

ou au contraire de refuser l'exploitation de leurs œuvres et objets protégés. Pendant plus d'une décennie, les titulaires des droits sont restés désarmés face aux plateformes. En l'absence de contrats autorisant l'exploitation des contenus protégés, ces services – invoquant le statut d'hébergeur – revendiquaient comme seule obligation celle de retirer promptement les contenus contrefaisants dès lors qu'ils auraient connaissance de leur caractère manifestement illicite.

Dans la pratique, certaines plateformes dont le contenu est créé par les utilisateurs dites « *User Generated Content* » ou « UGC », telles que YouTube, ont déployé des outils de reconnaissance des contenus permettant de faciliter l'identification des contenus présents sur les plateformes et assurer soit leur monétisation par les ayants droit soit leur retrait.

[34] Tribunal supérieur de Sarrebruck, 19 décembre 2018, n° 1 U 128/17 décision IFPI.

[35] Tribunal de première instance de Bruxelles, 9 août 2013, n° 2012/12072/A.

Les procédures de notification des ayants droit sont facilitées grâce à l'utilisation de ces technologies : l'ayant droit fournit les empreintes, le site ou service compare ces empreintes aux contenus en ligne et alerte l'ayant droit qui peut choisir soit le retrait du contenu, soit sa monétisation à travers notamment un partage des recettes publicitaires générées par le contenu.

2.2.B | L'ADOPTION DE LA DIRECTIVE EUROPÉENNE SUR LE DROIT D'AUTEUR ET LES DROITS VOISINS DANS LE MARCHÉ UNIQUE NUMÉRIQUE

C'est dans ce contexte que l'article 17 de la directive 2019/790 sur le droit d'auteur et les droits voisins dans le marché unique numérique du 17 avril 2019 a créé un régime spécifique de responsabilité des plateformes numériques, qui sont désormais considérées comme réalisant un acte de communication au public ou de mise à disposition pour lequel elles doivent obtenir une autorisation de la part des titulaires de droits ou, en l'absence d'autorisation, fournir leurs « meilleurs efforts » pour empêcher la disponibilité de leurs œuvres et objets protégés sur leur service.

En adoptant cette disposition, le législateur européen a souhaité favoriser une juste répartition de la valeur entre secteur culturel et monde du numérique, tout en encourageant le développement du partage légal de contenus et celui du marché des licences. Par ailleurs, le législateur européen a veillé à prendre en compte les préoccupations de diverses parties prenantes, par exemple en allégeant les obligations pesant sur les « petites » plateformes ou en prévoyant des garanties dont pourraient se prévaloir les usagers dans leurs rapports avec les plateformes et les ayants droit. Ainsi, l'article 17 protège les exceptions existantes, notamment en matière de citation et de parodie, et instaure

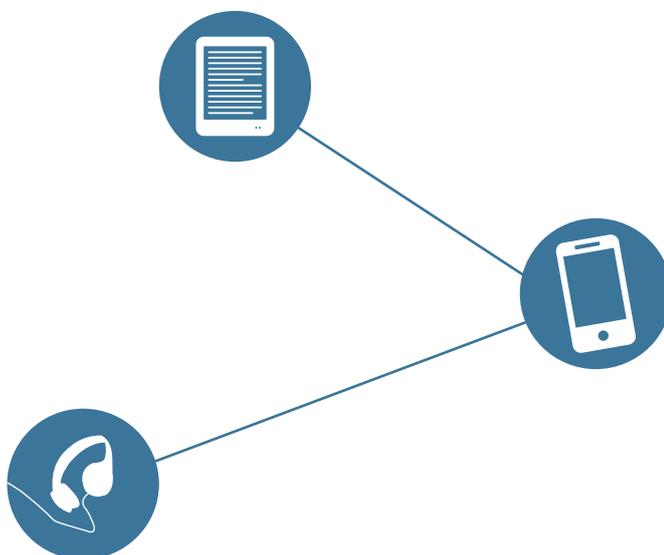
un mécanisme de règlement extrajudiciaire des litiges permettant aux utilisateurs de contester les éventuelles blocages considérés comme injustifiés.

Les États membres ont jusqu'au 7 juin 2021 pour adopter les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive.

Parallèlement, la Commission européenne organise, en coopération avec les États membres, des dialogues entre parties intéressées afin d'examiner les meilleures pratiques pour la coopération entre les fournisseurs de services de partage de contenus en ligne et les titulaires de droits.

Plusieurs États membres ont d'ores et déjà initié le processus de transposition et notamment :

- les Pays-Bas ont adopté leur loi de transposition de la directive sur le droit d'auteur et les droits voisins dans le marché unique numérique en décembre 2020 ;
- le ministère allemand de la Justice et de la Protection des Consommateurs a également dévoilé son projet de transposition, lequel a fait l'objet d'importants débats, notamment en ce qui concerne les exceptions et autorisations qui seraient accordées aux utilisateurs ;
- des consultations des parties prenantes ont été initiées en Autriche, au Danemark, en République tchèque ;
- en France, le 3 décembre 2020, a été adoptée une loi habilitant le Gouvernement à transposer par ordonnance différentes directives et notamment la directive sur le droit d'auteur et les droits voisins dans le marché unique numérique.



MISSION FRANÇAISE SUR LES OUTILS DE RECONNAISSANCE DES CONTENUS PROTÉGÉS SUR LES PLATEFORMES

En France, l'Hadopi a conduit conjointement avec le Conseil supérieur de la propriété littéraire et artistique (CSPLA) et le Centre national du cinéma et de l'image animée (CNC) une mission visant à dresser un état des lieux actualisé des outils de reconnaissance de contenus dont certains sont déjà utilisés par ces plateformes pour reconnaître les contenus des ayants droit, et en bloquer ou monétiser l'accès.

La mission a ainsi été chargée :

- d'évaluer l'efficacité et la pertinence des outils techniques existants, à la fois en appréciant leur performance et en mesurant leurs éventuelles limites, ainsi que leur finesse, en analysant les risques de retraits injustifiés de contenus ;
- de formuler des recommandations sur l'utilisation de ces technologies dans le cadre de la directive sur le droit d'auteur.

À l'issue de près d'une soixantaine d'auditions et de la rencontre de plus de 200 personnalités par les équipes de l'Hadopi, du CSPLA et du CNC, le rapport de la mission^[36], publié en avril 2020, procède, sur la base de tests techniques détaillés, à une évaluation approfondie des technologies pertinentes et des outils de reconnaissance existants. Il conclut à leur réelle efficacité, tout en mettant en évidence des points possibles d'amélioration et en offrant une approche prospective du sujet. Sur la base des auditions conduites en France et à l'étranger ainsi que d'enquêtes d'opinion quantitatives et qualitatives, le rapport dresse un panorama des perceptions et attentes des acteurs, tant utilisateurs qu'ayants droit ou plateformes.

Le rapport esquisse enfin les premières pistes pour une mise en œuvre à la fois ambitieuse et concertée de cet article 17. Bien qu'ayant initialement fait l'objet de débats virulents, l'article 17 semble en réalité éloigner le risque de filtrage généralisé et vise plutôt à pérenniser et encadrer une situation préexistante en permettant une protection renforcée du droit d'auteur mais également une meilleure prise en compte des équilibres entre protection et usages.

Dans la continuité de ce rapport, une nouvelle mission conjointe a été lancée en avril 2020, celle-ci ayant pour objectif de faire connaître les conclusions du premier rapport et d'approfondir les propositions que celui-ci comporte. Le rapport publié le 19 janvier 2021^[37] souligne le rôle que devront jouer les outils automatiques de reconnaissance des contenus d'ores et déjà déployés sur les plus importantes plateformes. Il précise les modalités d'intervention de ces outils préventifs indispensables à la protection du droit d'auteur et décrit les conditions de l'équilibre à assurer avec les exceptions à ce droit et avec la liberté d'expression, dont le respect peut et doit être assuré sans paralyser pour autant le fonctionnement des outils automatiques. Le rapport plaide pour une lecture rigoureuse du texte de la directive et donne au régulateur un rôle de garant de l'équilibre à instituer entre les droits des différentes parties prenantes : utilisateurs, titulaires de droit d'auteur et plateformes. Seule une telle lecture, qui fait toute leur place aux outils technologiques disponibles, permettra à la directive de produire tous ses effets avec des contenus légaux plus largement disponibles au bénéfice de chacun.

Les propositions présentées s'inscrivent dans cette logique en développant la transparence des pratiques et la responsabilité de tous les acteurs : inscription dans la loi du bénéfice des exceptions, traitement rapide et efficace des plaintes, définition du rôle du régulateur, transparence des algorithmes mis en œuvre par les plateformes et des règles de gestion de droits appliqués, déclinaison fine de la mise en œuvre de la directive aux différents domaines, y compris l'image et l'écrit.

[36] https://hadopi.fr/sites/default/files/sites/default/files/ckeditor_files/Rapport_CSPLA_Hadopi_CNC%20Outils_de_reconnaissance_VF.pdf
[37] https://www.hadopi.fr/sites/default/files/sites/default/files/ckeditor_files/2021_01_19_Rapport_CSPLA_Hadopi_CNC_Outils_de_reconnaissance.pdf

La république de Pologne a de son côté demandé, en mai 2019, en invoquant un moyen tiré de la violation du droit à la liberté d'expression et d'information garanti par l'article 11 de la Charte des droits fondamentaux de l'Union européenne^[38], l'annulation de certaines dispositions de l'article 17.

2.2.C | LA JURISPRUDENCE DE LA COUR DE JUSTICE EUROPÉENNE ET LA PROPOSITION DE DIGITAL SERVICES ACT

Parmi les jurisprudences pertinentes en matière de lutte contre le piratage, on peut relever deux arrêts qui ont précisé la teneur et la portée de ce qui peut être demandé à des plateformes de partage de contenus :

- S'agissant de la portée des mesures de retrait qu'une plateforme peut être enjointe à prendre par injonction judiciaire, une décision du 3 octobre 2019^[39] de la Cour de justice de l'Union européenne a considéré que la directive dite « commerce électronique » ne s'oppose pas à ce que l'autorité judiciaire enjoigne un hébergeur tel que Facebook de supprimer des commentaires « identiques » ou, sous certaines conditions, « équivalents » à un commentaire précédemment déclaré illicite. Cette décision a également posé qu'une telle injonction pouvait produire des effets dans le monde entier dans le respect du droit international pertinent, qu'il appartient aux juridictions nationales d'apprécier.
- S'agissant des informations d'identification de leurs utilisateurs indélébiles, un arrêt du 9 juillet 2020 de la Cour de justice de l'Union européenne est venu préciser la portée de la notion d'« adresses » figurant à l'article 8, paragraphe 2, sous a) de la directive 2004/48. La Cour a jugé que, dans le cadre du téléversement d'un film sur une plateforme de partage de vidéos en ligne (YouTube) sans l'accord du titulaire du droit d'auteur, la directive 2004/48 1 n'oblige pas les autorités judiciaires à ordonner à l'exploitant de la plateforme vidéo de fournir l'adresse courriel, l'adresse IP ou le numéro de téléphone de l'utilisateur ayant téléversé le film litigieux. La directive 2004/48, qui prévoit la fourniture des « adresses » des personnes ayant porté atteinte à un droit de propriété intellectuelle, vise ainsi uniquement l'adresse postale.

Postérieurement à ces arrêts, la proposition de règlement *Digital Services Act* (DSA), qui a notamment vocation à mettre à jour le cadre juridique actuellement en vigueur pour les services numériques, a prévu un régime adapté aux plateformes, au sein desquelles le texte distingue d'ailleurs les plateformes et les très grandes plateformes. Les très grandes plateformes, au sens de la proposition de DSA, sont celles qui représentent le plus haut niveau de risques systémiques pour l'Union européenne et qui, à ce titre, ont la capacité d'assumer une charge plus grande dans la cadre de la lutte contre les contenus illicites et les risques sociétaux en ligne : la proposition de DSA leur fait donc supporter des obligations supplémentaires plus lourdes liées à l'évaluation des risques qu'elles engendrent et leur impose de prendre des mesures visant à atténuer ces risques.

Ces nouvelles règles applicables aux plateformes dans leur ensemble ne remettent pas en cause les instruments sectoriels spécifiques existants tels que l'article 17 de la directive sur le droit d'auteur du 17 avril 2019. Parmi les dispositions de ce texte venant s'ajouter au dispositif de lutte contre la diffusion des contenus contrefaisants, on peut relever en particulier celles prévoyant que :

- les plateformes devront traiter en priorité les notifications faites par les « signaleurs de confiance » dont le statut aura été labellisé par la nouvelle autorité publique locale chargée de l'application du règlement dans son ensemble, dite « Coordinateur des services numériques » ;
- à l'instar des dispositions prévues dans le cadre de l'article 17 de la directive dite droit d'auteur, les plateformes et les très grandes plateformes devront prévoir un système de contestation à l'encontre des décisions de retrait et ou de suspension de compte ;
- les plateformes devront également permettre l'accès à un organisme de règlement extrajudiciaire des litiges certifié par le nouveau régulateur local dédié, créé par ce texte.

[38] La république de Pologne affirme en particulier que l'obligation faite aux fournisseurs de services de partage de contenus en ligne de fournir leurs meilleurs efforts pour garantir l'indisponibilité d'œuvres et autres objets protégés spécifiques pour lesquels les titulaires de droits ont fourni aux fournisseurs de services les informations pertinentes et nécessaires (article 17, paragraphe 4, sous b), de la directive 2019/790) et l'obligation faite aux fournisseurs de services de partage de contenus en ligne de fournir leurs meilleurs efforts pour empêcher que les œuvres et autres objets protégés, pour lesquels les titulaires de droit ont présenté une notification suffisamment motivée, soient téléversés dans le futur (article 17, paragraphe 4, sous c), in fine de la directive 2019/790) a pour conséquence – afin d'éviter la mise en cause de leur responsabilité – que les fournisseurs de services doivent procéder à une vérification automatique préalable (filtrage) des contenus partagés en ligne par les utilisateurs, ce qui implique par conséquent de mettre en place des mécanismes de contrôle préventif. De tels mécanismes mettent en cause l'essence même du droit à la liberté d'expression et à l'information et ne respectent pas l'exigence de proportionnalité et de nécessité de toute atteinte à ce droit.

[39] CJUE, 3 octobre 2019, C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*.

De façon générale, la proposition de DSA entend mettre en place une norme plus élevée en matière de transparence, au titre de laquelle des nouvelles obligations pèseront sur les plateformes s'agissant de la transparence de leurs algorithmes. Cette question est en effet primordiale dans la gestion des outils de reconnaissance de contenus et la mise en œuvre des dispositions de l'article 17 de la directive dite droit d'auteur. Cette transparence permettrait de vérifier que les outils et algorithmes utilisés ne comprennent pas de biais en la défaveur des ayants droit ou des utilisateurs. Ainsi, une des recommandations du rapport sur les outils de reconnaissance des contenus sur les plateformes numériques de partage publié en janvier 2021 vise à accroître la transparence des algorithmes et solutions techniques mises en œuvre par les plateformes pour protéger le droit d'auteur, en prévoyant une intervention appropriée du régulateur.

2.2.D | LES INITIATIVES HORS DE L'EUROPE POUR RESPONSABILISER LES PLATEFORMES

Dans la perspective de responsabiliser les plateformes, des initiatives existent déjà ou des réflexions sont menées dans certains pays pour se doter d'une disposition similaire à celle de l'article 17 de la directive européenne sur le droit d'auteur du 17 avril 2019.



Au Canada, dans un rapport de juin 2019 sur la loi sur le droit d'auteur du *Standing Committee on Industry, Science and Technology*^[40], ce comité reconnaît l'écart de valeur (*value gap*) au détriment des ayants droit et se dit favorable à une approche équilibrée. Sans faire de proposition concrète, le comité entend dans un premier temps observer la mise en œuvre dans d'autres juridictions de l'octroi de licences collectives étendues ainsi que les législations conditionnant le bénéfice du régime de responsabilité limitée des plateformes aux mesures prises par ces acteurs contre la violation du droit d'auteur.

En Corée du Sud, depuis 2009, la loi prévoit un dispositif dit de « réponse graduée » qui permet d'adresser, *via* les plateformes, des notifications aux internautes qui partagent du contenu sur ces plateformes.

Aux États-Unis, il ressort du rapport du Bureau du droit d'auteur publié le 21 mai 2020^[41] que les titulaires de droits ont manifesté le souhait de se doter d'une disposition similaire à celle de l'article 17 de la nouvelle directive sur le droit d'auteur. Le Bureau du droit d'auteur a considéré qu'une telle modification impliquerait une réforme de fond du régime de responsabilité actuel nécessitant un travail de recherches pour examen du Congrès. Une première ébauche de réforme a été publiée par un parlementaire en décembre 2020, celle-ci prévoyant notamment d'introduire une obligation de « *stay down* » pour les plateformes, sans préciser les moyens à utiliser à cette fin.

Une loi promulguée en décembre 2020 prévoit qu'une instance rattachée au Bureau du droit d'auteur est désormais chargée de résoudre les conflits en matière de droit d'auteur portant sur des montants peu importants (« *small claims* »). Pour certains, cette instance pourrait notamment être chargée de résoudre les litiges relatifs aux utilisations illicites de photographies sur internet, tout comme les litiges en rapport avec des demandes de retrait auprès de plateformes telles que YouTube.

En Inde, un nouveau projet de réglementation sur le commerce électronique a été publié début 2019. Celui-ci prévoit d'inviter les plateformes à mettre en place, sur une base volontaire, des mesures pour empêcher la diffusion en ligne de contenus piratés.

En Russie, en novembre 2018, les ayants droit, des plateformes et des moteurs de recherche locaux ont signé un accord de coopération les obligeant à prendre des mesures à l'égard des contenus figurant sur une base de données centralisée, créée par le régulateur local, le *Roskmonadzor*, actualisée en continu.

La Suisse ne disposait auparavant pas de régime légal spécifique pour les intermédiaires techniques. Une nouvelle législation a cependant introduit des dispositions visant à encadrer les activités des hébergeurs en imposant une obligation spécifique aux plateformes qui « *en raison de [leur] fonctionnement technique ou de [leurs] objectifs économiques favorisent les violations du droit, génère[nt] un risque particulier qu'une telle violation soit commise* ». Ceux-ci doivent désormais prévenir les nouvelles mises en ligne de contenus protégés qui leur ont préalablement été notifiées (*Stay down*) en prenant « *les mesures qui peuvent être raisonnablement exigées d'[eux] d'un point de vue technique et économique compte tenu du risque de violation* ».

À Taïwan, un mécanisme législatif d'avertissement graduel prévoit notamment que les plateformes doivent transmettre les notifications aux internautes et se doter d'un dispositif permettant de suspendre ou résilier les comptes des internautes qui ont porté plusieurs fois atteinte au droit d'auteur. À défaut, celles-ci ne pourraient pas bénéficier du régime de responsabilité limitée.

Au Vietnam, une circulaire impose aux fournisseurs de services intermédiaires, soit les fournisseurs d'accès à internet, les fournisseurs de services d'hébergement, les moteurs de recherche, les plateformes et les réseaux sociaux, à la demande des ministères de l'Information et de la Communication, du ministère de la Culture, des Sports et du Tourisme ou de toute autre autorité gouvernementale, de supprimer ou de désactiver l'accès aux contenus litigieux et de mettre un terme à la fourniture de leurs services lorsque le droit d'auteur et les droits voisins seraient menacés.

[40] <https://www.ourcommons.ca/DocumentViewer/en/42-1/INDU/report-16/page-285>

[41] <https://www.copyright.gov/policy/section512/section-512-full-report.pdf>



LA RESPONSABILISATION DES INTERNAUTES

Outre la question de la responsabilité des services qui sont à l'origine de « l'offre » de services, se pose également la question des modalités d'approche du rôle joué par les internautes en tant que récipiendaires et parfois acteurs de ces services.

Les leviers complémentaires ou alternatifs à la répression selon les pays sont, d'une part, la mise en valeur de l'offre légale et, d'autre part, la création d'outils de sensibilisation et de communication à destination du grand public ou de catégories spécifiques du public.

3.1 | LES DISPOSITIFS VISANT LES INTERNAUTES QUI PARTAGENT DES ŒUVRES SUR LES RÉSEAUX PAIR À PAIR

Les mesures visant à responsabiliser les internautes se partageaient historiquement entre deux tendances : les dispositifs d'avertissement et les solutions de mise en demeure indemnitaires, lesquels sont d'ailleurs susceptibles de cohabiter dans un même pays. Les expériences de dispositifs d'avertissement à l'origine principalement conçus pour combattre les usages illicites en pair à pair ont souvent rencontré d'importantes limites ou difficultés de mises en œuvre ayant conduit à leur déclin ou leur abandon définitif (États-Unis, Nouvelle-Zélande, Royaume-Uni). Ainsi le débat se focalise sur la nécessité de mieux cibler ce type de procédure à l'égard des internautes en matière de pair à pair et de renforcer les sanctions associées.

Les dispositifs à l'égard des internautes sont restés essentiellement cantonnés à un seul usage, le pair à pair et ne sont pas étendus au *streaming* et au téléchargement direct, compte tenu notamment des contraintes techniques pour déterminer le rôle de l'internaute. Il faut relever le cas des Pays-Bas et de la Corée du Sud, qui visent les internautes mettant à disposition des contenus sur les plateformes.

Aux Pays-Bas, la BREIN, l'association d'ayants droit qui lutte contre le piratage, met en œuvre un dispositif indemnitaire qui se concentre sur les internautes gros partageurs de fichiers (dits « *uploaders* ») sur certains réseaux sociaux ou sur les plateformes dites UGC notamment.

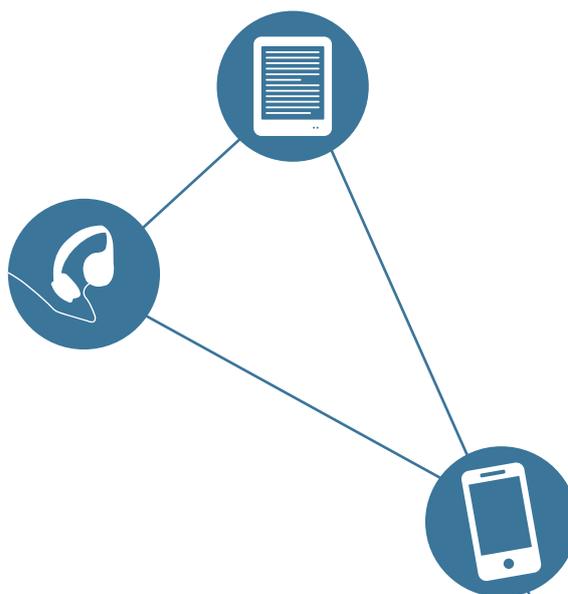
En Corée du Sud, un dispositif permet d'adresser des notifications aux *uploaders* mettant à disposition du contenu sans autorisation sur des plateformes dites UGC.

3.1.A | LES DISPOSITIFS D'AVERTISSEMENT À DESTINATION DES INTERNAUTES

Les dispositifs d'avertissement à destination des internautes consistent à leur rappeler la loi et les risques encourus. Ils peuvent être associés à un dispositif de sanction.

Les retours d'expérience sur les dispositifs pédagogiques d'avertissement à l'égard des internautes à l'étranger mettent en évidence trois grands enseignements :

- la nécessaire collaboration des fournisseurs d'accès à internet, principalement lorsque leur implication n'est pas imposée par la loi, dans la mesure où leurs carences n'engagent pas – ou seulement marginalement – leur responsabilité ;
- les difficultés liées à la maîtrise et à la répartition des coûts (entre fournisseurs d'accès à internet et ayants droit) du fait du large spectre d'abonnés susceptibles d'être visés ;
- les enjeux liés à l'effectivité des sanctions encourues au-delà de la seule approche pédagogique.



Aux Pays-Bas, la BREIN, l'association d'ayants droit qui lutte contre le piratage, met en œuvre un dispositif indemnitaire qui se concentre sur les internautes qui partagent un nombre important de fichiers et dispose à cette fin d'un logiciel dédié qui permet d'identifier leurs adresses IP des *primo-uploaders* sur les réseaux pair à pair. Elle a récemment adapté ce logiciel pour détecter les *uploaders* fréquents ou prolongés et lancé fin 2020 une campagne d'envoi d'avertissements éducatifs de six mois à destination de ces internautes, pendant laquelle un maximum de 1 000 comptes par mois recevront un avertissement par email.

Au Royaume-Uni, un mécanisme d'envoi d'emails aux internautes, dépourvu de sanction (« *Voluntary Copyright Alert Programme* »), a fonctionné de 2017 à 2019. Il a été décidé de mettre fin au programme pour des raisons qui n'ont pas été rendues publiques.

3.1.B | LES DISPOSITIFS INDEMNITAIRES

Les ayants droit sollicitent des entreprises spécialisées dans la surveillance des réseaux pair à pair afin que celles-ci collectent les adresses IP des internautes qui ont commis des infractions aux droits d'auteur. Selon les règles de protection des données personnelles, l'ayant droit doit ensuite obtenir une décision du juge autorisant le fournisseur d'accès à internet à lui communiquer, à partir d'une adresse IP, l'identité du titulaire de la connexion à internet utilisée. Une fois ces coordonnées transmises, il revient au conseil juridique des ayants droit d'adresser une mise en demeure à l'intéressé en lui indiquant le montant indemnitaire sollicité et le risque de poursuites judiciaires à défaut de solution amiable.

Outre leur faible acceptabilité par le grand public, ce type d'action soulève, selon les traditions juridiques propres à chaque pays, des questionnements quant aux risques d'abus, quant à la place du juge et quant à la protection des données personnelles.

Cette approche soulève également des difficultés financières qui constituent une dernière limite à son déploiement de masse. Les frais supportés par les ayants droit sont démultipliés (frais de surveillance des réseaux, frais de justice et d'avocats – notamment

en vue de la mise en demeure – pour solliciter devant le juge l'identification de l'abonné, frais d'identification payés aux fournisseurs d'accès). Or, les possibilités de mettre ces frais à la charge des abonnés ont souvent été limitées par la loi ou le juge. Enfin, et en tout état de cause, les chances de recouvrer les sommes demandées restent incertaines pour les ayants droit au stade de la seule mise en demeure, sauf à devoir ensuite agir en justice contre l'internaute en cas d'échec de la voie transactionnelle.

Malgré ces écueils, les tentatives de mise en œuvre de tels dispositifs se multiplient. De telles actions semblent cependant être davantage le fait des ayants droit de l'audiovisuel que des ayants droit de la musique, l'IFPI privilégiant les actions civiles et pénales à l'encontre des sites illicites ou les mesures de blocage.

Il faut relever que des questions préjudicielles relatives à ce procédé ont été posées en 2019 à la Cour de justice de l'Union européenne. Dans le cadre d'un contentieux opposant en Belgique un fournisseur d'accès à internet à un prestataire spécialisé dans l'envoi de demandes d'indemnisation aux internautes partageant des films pornographiques *via BitTorrent*, le 6 août 2019, un tribunal situé à Anvers a en effet posé plusieurs questions préjudicielles à la Cour. Ces questions portent pour partie sur le cas d'espèce, à savoir la possibilité pour un prestataire qui a acquis les droits de diffusion *BitTorrent* de films pornographiques et ne les diffuse pas par ce biais, de se contenter de formuler des demandes d'indemnisation. Elles portent également sur la compatibilité au regard du règlement général sur la protection des données de la collecte et du traitement des adresses IP des internautes qui partagent les contenus^[42].

[42] CJUE, C-597/19, M.I.C. M. Mircom International Content Management & Consulting Limited/Telenet BVBA.

L'Allemagne suscite beaucoup d'intérêt car elle organise par la loi un mécanisme indemnitaire à portée générale. Les ayants droit allemands sollicitent des entreprises spécialisées dans la surveillance des réseaux pair à pair afin que celles-ci collectent les adresses IP des internautes qui ont commis des infractions au droit d'auteur. Compte tenu des règles de protection des données personnelles, l'ayant droit doit ensuite obtenir une décision du juge autorisant le fournisseur d'accès à internet à lui communiquer, à partir d'une adresse IP, l'identité du titulaire de la connexion à internet utilisée, non pas pour tenter directement une action à son encontre, mais pour pouvoir préalablement le mettre en demeure.

Aux Pays-Bas, certains ayants droit (dont le distributeur de films Dutch FilmWork – « DFW ») souhaiteraient envoyer des demandes d'indemnisation à l'ensemble des internautes. Fin 2017, l'autorité locale en charge de la protection des données personnelles a autorisé la collecte de données personnelles par un ayant droit aux fins d'envoyer des demandes de compensation financière. DFW a cependant été débouté en première instance et en appel lors d'une procédure engagée à l'encontre d'internautes. Les juges ont estimé que la protection des données personnelles des titulaires de comptes devait prévaloir dans la mesure où les demandes de DFW n'étaient pas claires et où une seule atteinte au droit d'auteur était en cause^[43]. DFW a formé un pourvoi devant la Cour suprême néerlandaise fin 2019.

Au Royaume-Uni, une décision de justice dite « *Golden Eye* » encadre les hypothèses de mises en demeure indemnitaires des internautes par les ayants droit, face aux nombreux abus constatés, et prévoit notamment que la lettre de l'ayant droit doit faire apparaître que, malgré l'injonction pour dévoiler l'identité d'un internaute, celui-ci n'est pas encore regardé comme un contrefacteur ; le délai de réponse laissé à l'internaute doit être raisonnable.

En Suède, les ayants droit peuvent saisir le juge pour obtenir l'identité d'un internaute qui a partagé illicitement des contenus culturels sur les réseaux pair à pair et dont l'adresse IP a été identifiée. Une fois les coordonnées de l'internaute obtenues auprès du fournisseur d'accès à internet en vertu de la décision de justice, les ayants droit peuvent lui envoyer un courrier de mise en demeure de leur payer une somme d'argent au titre de leurs dommages et intérêts. À défaut de régler cette somme, il est indiqué à l'internaute qu'il pourra être poursuivi en justice. Cette pratique fait toutefois l'objet de nombreuses controverses.

En Suisse, la loi entrée en vigueur le 1^{er} avril 2020 a introduit une nouvelle disposition concernant la collecte des données personnelles afin de faciliter la mise en œuvre du droit d'auteur dans les cas de mise à disposition non autorisée (le téléchargement à partir de sources illicites reste couvert par l'exception de l'utilisation privée). Pour les cas de mise à disposition non autorisée, la nouvelle réglementation prévoit que le titulaire de droit d'auteur qui subit une violation peut initier une procédure et, dans cette perspective, il est autorisé à « *traiter des données personnelles [...] pour déposer une plainte ou une dénonciation pénale [...]. Il peut également utiliser ces données pour faire valoir des conclusions civiles par voie d'adhésion ou pour les faire valoir au terme de la procédure pénale. Il est tenu de déclarer publiquement le but, le type de données traitées et l'étendue de leur traitement* ». Le droit d'auteur modernisé prend ainsi le contrepied d'une jurisprudence suisse de 2010, dite « *Logistep* », très protectrice en matière de données personnelles, et qui avait créé une incertitude quant à la licéité de la collecte d'adresses IP par les ayants droit en vue d'initier des poursuites pour les cas de mises à disposition illicites et par conséquent une incertitude quant à l'admissibilité des adresses IP en tant que preuve dans le cadre de poursuites pour violation de droits d'auteur.

3.2 | LA SENSIBILISATION DU PUBLIC

3.2.A | LES ACTIONS DE COMMUNICATION

Les actions conduites pour sensibiliser les internautes portent notamment sur les risques de toutes natures encourus par les internautes lorsqu'ils partagent ou consomment des contenus de manière illicite. Ces actions de communication peuvent cibler des populations spécifiques, le jeune public en particulier.

Un autre axe de communication par les acteurs de la lutte contre la contrefaçon consiste à présenter, le cas échéant avec l'appui des internautes dont la culpabilité a été reconnue, les actions conduites dans le cadre de la lutte anti-contrefaçon et les condamnations obtenues sur de nombreux supports, dont les vecteurs utilisés par les internautes ayant illégalement partagé des contenus (plateformes UGC, réseaux sociaux...).

[43] <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHARL:2019:9352>

En Australie, plusieurs campagnes ont été lancées *via* une organisation regroupant les ayants droit de l'audiovisuel appelée « *Creative content Australia* ». Un site internet dédié a été créé, comportant notamment des vidéos explicatives sur les dangers de la consommation illégale et des spots publicitaires. La campagne 2020 « *Piracy – You're exposed* » insiste à nouveau sur les risques encourus par les internautes ayant des usages illicites.

En Espagne, en octobre 2017, le gouvernement espagnol a lancé une campagne de sensibilisation intitulée « *No piratees tu futuro* » (ne pirate pas ton futur) destinée aux jeunes publics afin de les sensibiliser en montrant les conséquences du piratage sur les futures carrières des jeunes sans insister sur la répression pénale de ces pratiques.

En France, l'Hadopi a développé de nombreux outils de sensibilisation, en particulier du jeune public. En décembre 2020, l'Hadopi a notamment lancé une campagne de communication intitulée « *On a tous de bonnes raisons d'arrêter de pirater* »^[44]. En janvier 2021, l'Hadopi s'est en outre associée avec d'autres autorités publiques (la CNIL, le CSA et le Défenseur des droits) pour créer un kit pédagogique, qui regroupe l'ensemble des ressources conçues pour l'éducation du citoyen numérique, à destination des formateurs et des parents qui accompagnent les jeunes en matière de numérique^[45]. Enfin, le projet de réforme devait entériner l'approche pro-active de l'Hadopi en matière de sensibilisation, chargeant expressément l'autorité publique d'une mission de prévention et d'information auprès de tous les publics, notamment des plus jeunes, sur les risques et les conséquences du piratage.

En Grèce, l'autorité publique en charge de la lutte contre le piratage, l'OPI^[46], a élaboré au fil du temps une stratégie globale sur le droit d'auteur et l'éducation grâce à la mise en œuvre de programmes éducatifs s'adressant aux éducateurs et aux élèves de l'enseignement primaire et secondaire. En ce qui concerne l'enseignement primaire, les actions conduites ont obtenu le soutien de l'Union européenne, tandis que le programme a également reçu (et reçoit toujours sur une base annuelle) le soutien du ministère de l'Éducation. Un site dédié a été créé^[47]. L'initiative la plus récente dans ce domaine concerne la mise en œuvre du programme financé par l'Union européenne intitulé « *Éduquer les jeunes et les enseignants du secondaire au droit d'auteur en Grèce et à Chypre* ». Ce programme a été sélectionné pour financement par l'EU IPO et est conduit avec Chypre. Il prévoit différentes actions comprenant, entre autres, la production de matériel informatif et éducatif sur le droit d'auteur destiné aux jeunes et aux élèves de l'enseignement secondaire, et l'organisation de séminaires éducatifs pour les enseignants du secondaire.

Aux Pays-Bas, les titulaires de droits fournissent du matériel éducatif aux écoles, avec une subvention du ministère de la Culture, des Sciences et de l'Éducation ainsi que de l'EU IPO.

Au Pérou, un projet de loi destiné à renforcer la protection des droits de propriété intellectuelle a été soumis à consultation en janvier 2020.

Au Royaume-Uni, le gouvernement britannique envisage notamment de partager davantage les données de la lutte contre le piratage entre parties prenantes et autorités publiques, en s'assurant notamment de la publication des jugements, afin d'évaluer leur impact.

En Suède, le bureau d'enregistrement des marques et brevets a réalisé en 2018 une campagne de communication dans laquelle il est fait état du fait que les détenteurs de sites de *streaming* illégaux gagnent beaucoup d'argent et sont liés à d'autres réseaux illégaux (ventes de médicaments contrefaisants, drogues...).

En Suisse, l'Office fédéral de la communication réalise régulièrement des campagnes de communication pour sensibiliser aux dangers d'internet et a sorti en mai 2020 une bande dessinée numérique humoristique dans le cadre de ces campagnes^[48].

[44] <https://www.hadopi.fr/actualites/campagne-nationale-tous-de-bonnes-raisons-darreter-de-pirater>

[45] <https://hadopi.fr/ressources/kit-pedagogique-du-citoyen-numerique-retrouvez-toutes-les-ressources>

[46] Hellenic Copyright Organisation.

[47] <https://copyrightschool.gr/index.php/en/>

[48] <https://www.websters.swiss/fr/>

3.2.B | LES ACTIONS DE PROMOTION DE L'OFFRE LÉGALE

De façon générale, et aujourd'hui en particulier dans les pays s'étant engagés plus récemment dans la lutte contre le piratage de contenus protégés sur internet, l'arrivée des plateformes proposant légalement des contenus s'accompagne souvent d'un effet positif sur le niveau de piratage.

Des portails nationaux référençant les différentes offres légales sont de plus mis en place selon une approche soit transversale, soit uniquement pour le secteur audiovisuel, dans de nombreux pays. Des campagnes de sensibilisation sont également organisées en vue de la promotion de l'offre légale et constituent un des axes d'accompagnement vers un changement de comportement des internautes.

En Europe, cette initiative a été portée par l'Observatoire européen des atteintes au droit de propriété intellectuelle de l'Office de l'Union européenne pour la propriété intellectuelle (EUIPO) dans le cadre du projet Agorateka, qui a permis la création d'un agrégateur européen de l'offre légale. Fin 2020, la plateforme comptait 31 portails répertoriant les sites proposant légalement de la musique, des films et des séries télévisées, des livres numériques, des jeux vidéo et des événements sportifs dans 21 États membres. Une campagne de sensibilisation a été lancée par l'EUIPO le 26 avril 2020 dans 18 pays européens qui disposent déjà d'un ou plusieurs portails de contenu en ligne connectés à Agorateka.

L'EUIPO a un temps envisagé de créer un moteur de recherche par œuvre sur Agorateka mais face à la complexité de cette entreprise, ce projet a été abandonné. En effet, il est apparu que pour plusieurs types de contenus tels que la musique et les jeux vidéo, les consommateurs connaissent les offres légales locales et y recherchent les contenus souhaités. Un moteur de recherche global, lequel coûterait cher et serait complexe à créer et ensuite à actualiser, ne fait donc pas sens pour ces marchés. Cependant, un tel moteur pourrait être utile pour les œuvres audiovisuelles mais au seul niveau national. L'EUIPO étudie donc les différentes options possibles à cet égard avec les parties prenantes.

En-dehors de l'Europe, on peut notamment relever les initiatives suivantes :

En Australie, une campagne dédiée à l'encouragement de l'offre légale et à l'éducation au droit d'auteur a été mise en place par l'organisation regroupant les ayants droit de l'audiovisuel « *Creative content Australia* ».

En Corée du Sud, l'initiative « *Copyright OK* », un système de certification de la légalité d'une plateforme mettant à disposition des contenus culturels, est administrée par l'autorité publique locale, la KCOPA.

Au Japon, le projet « *manga-anime guardians anti-piracy project* » vise à renforcer la protection des mangas, produit culturel très consommé localement et particulièrement rémunérateur pour les ayants droit. Dans ce cadre, a été créé un site internet qui liste les mangas disponibles légalement sur internet. Le secteur de la musique a par ailleurs créé un label pour aider les internautes à reconnaître les offres légales.

3.2.C | LA DIFFUSION DE MESSAGES À DESTINATION DES INTERNAUTES SUR LES SITES FAISANT L'OBJET D'UNE MESURE DE BLOCAGE

On observe que de plus en plus de fournisseurs d'accès à internet sont tenus d'accompagner les mesures de blocage de messages de sensibilisation à l'attention des internautes. Ces messages ont vocation à expliquer les raisons de l'inaccessibilité du site recherché, voire à le renvoyer vers les services de l'offre légale. Pour les pays où il existe déjà une forte cohésion des ayants droit (Danemark) ou un fort degré d'intervention publique dans la mise en œuvre de ces mesures de blocage (Italie et Portugal), on observe un travail d'harmonisation et de pédagogie dans la rédaction des messages diffusés.



2^E PARTIE

FICHES

DESCRIPTIVES

PAR PAYS

AFRIQUE DU SUD

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

59,3 POPULATION^[1]
en millions

56,2 % TAUX DE PÉNÉTRATION
INTERNET (2017)^[2]

USAGES ILLICITES^[3]

1 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

29 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



En Afrique du Sud, si les secteurs créatifs sont en pleine croissance, tel est également le cas du piratage sur internet, et ce alors que le gouvernement vient d'ouvrir la voie à la mise en place de réseaux 4G et 5G. L'arrivée d'offres légales comme Netflix en 2016 aurait néanmoins drastiquement baissé le trafic sur les réseaux *BitTorrent* d'après les fournisseurs de service internet^[4].

Les boîtiers configurés pour le piratage et les clés USB préchargées de contenus ou d'applications contrefaisants sont de plus en plus populaires en Afrique du Sud. Des arrestations sont réalisées par la police à l'encontre des vendeurs de ces boîtiers. En janvier 2018, le *Durban Commercial Crime Unit*, un service de la police, a ainsi exécuté un mandat de perquisition et de saisie pour des boîtiers IPTV suite à une plainte.

Le dispositif législatif en vigueur ne prévoit cependant pas de dispositions spécifiques pour sanctionner les atteintes à la propriété intellectuelle en ligne. Le gouvernement sud-africain a récemment approuvé son adhésion aux traités de l'OMPI sur le droit d'auteur et dans cette optique, l'Assemblée nationale sud-africaine a adopté en 2017 deux projets de loi sur le droit d'auteur d'une part et sur les droits des artistes-interprètes d'autre part. Ces deux projets de loi doivent encore être approuvés par le Président du Conseil national des provinces, la chambre haute du Parlement.

Les autorités sud-africaines ont également introduit un projet de la loi sur la cybercriminalité et cybersécurité en 2017. Ce projet a été adopté par le Parlement mais doit encore être promulgué. Cette réforme devrait notamment comporter des dispositions relatives à la violation des droits de propriété intellectuelle causée par le partage d'œuvres protégées sur les réseaux pair à pair.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] <https://mybroadband.co.za/news/internet/321668-netflix-has-killed-torrents-in-south-africa.html>

ALLEMAGNE

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

83,8 POPULATION^[1]
en millions

88,1 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

2,9 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

39 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



L'Allemagne s'est dotée d'un dispositif de mise en demeure spécifique visant les internautes partageant illégalement des œuvres sur les réseaux

pair à pair et s'est engagée progressivement dans la lutte contre les services contrefaisants.

LES ACTIONS VISANT LES INTERNAUTES

LE DISPOSITIF DE MISE EN DEMEURE INDEMNITAIRE

L'Allemagne a développé une approche de la lutte contre la contrefaçon sur internet de nature indemnitaire, fondée sur une résolution amiable des litiges sur le terrain du droit civil entre internautes et ayants droit. La responsabilité civile des internautes identifiés comme ayant commis une négligence sur les réseaux peut ainsi être mise en cause par les ayants droit devant le juge. De manière alternative (et préalable) au litige, les ayants droit proposent aux internautes une procédure de règlement amiable pour mettre un terme à leur différend.

Il importe toutefois de préciser que depuis quelques années, les ayants droit, notamment dans le domaine

de l'industrie musicale, se tournent davantage vers des actions civiles et pénales à l'encontre des sites illícites mais également vers des mesures de blocages à l'encontre des intermédiaires techniques.

Le nombre de lettres de mise en demeure reste limité face au phénomène de masse que représente le piratage, la presse allemande faisant état d'environ 109 000 courriers par an envoyés pour un montant total de réclamations amiables sollicité de 90,3 millions d'euros. Les mises en demeure pour une œuvre telle qu'un film portent sur un total d'environ 700 euros (tous frais compris).

Le risque de sanction très important associé à ce dispositif semble néanmoins assez dissuasif si l'on observe la faible part des usages pair à pair en Allemagne.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

Pour autant, l'identification et la prise de contact avec les internautes impliquent une pluralité d'étapes assez coûteuses en frais de procédure pour les ayants droit allemands.

Pour la surveillance des réseaux pair à pair, les ayants droit sollicitent des entreprises spécialisées afin que celles-ci collectent les adresses IP des internautes qui mettent à disposition des œuvres sur les réseaux pair à pair.

L'identification de l'internaute par les fournisseurs d'accès à internet utilisant cette adresse IP au moment du constat doit ensuite être validée par le juge compte tenu des dispositions légales en matière de protection des données personnelles. Les dépenses liées aux frais de justice pour obtenir l'identification auprès du juge sont déterminées par le juge et fixées en moyenne à 200 euros par requête ou par œuvre. Outre ces frais, les ayants droit doivent ensuite payer aux fournisseurs d'accès à internet 35 euros par lot de dix adresses IP transmises pour identification. Des avocats spécialisés procèdent ensuite à la rédaction des courriers de mise en demeure envoyés aux internautes ainsi identifiés afin de leur demander le paiement d'une somme d'argent pour éviter d'être poursuivis en justice.

À défaut d'accepter le règlement amiable, il appartiendra à l'ayant droit d'attirer les internautes en justice. S'ajoute ainsi le caractère aléatoire du recouvrement à réception de la mise en demeure dès lors qu'en 2013, selon la presse allemande, seuls 15 % des internautes recevant ces courriers auraient réglé la somme demandée. Enfin, selon nos informations, le nombre d'actions en justice engagées contre les internautes ne se conformant pas à la mise en demeure ne serait que de l'ordre de quelques centaines par an.

UNE LOI ENCADRE LE CONTENU DES MISES EN DEMEURE

La loi est venue encadrer ces procédures pour plus de garanties.

Sur le plan formel, la lettre de mise en demeure doit comporter sous peine de nullité^[4] : le nom de l'ayant droit, la nature du droit violé, le détail des sommes réclamées selon la nature de frais ou préjudices en cause et les engagements que l'ayant droit attend de l'internaute, notamment de ne plus partager l'œuvre visée dans le courrier.

Sur le terrain financier, le dispositif des mises en demeure encadre le montant des sommes qui peuvent être réclamées aux internautes :

- le montant des dommages et intérêts pouvant être demandés est subordonné à un principe de proportionnalité, que le juge opère notamment au regard des œuvres en cause (ex. : la cour fédérale allemande a validé le montant de 200 euros pour un album de musique) ;
- le montant des frais de procédure et d'avocat susceptibles d'être mis à la charge de l'internaute a été limité par la loi à 500 euros.

LA JURISPRUDENCE A PRÉCISÉ LA PORTÉE DE CE DISPOSITIF ET LES CAUSES D'EXONÉRATION DE RESPONSABILITÉ POSSIBLES DE L'INTERNAUTE

Une question soulevée par ce dispositif est celle de l'éventuelle absence de responsabilité du titulaire de l'abonnement internet lorsqu'il apparaît qu'il n'est pas lui-même l'auteur des actes illicites.

Selon la jurisprudence, le détenteur de la connexion internet est présumé avoir commis l'atteinte signalée par les ayants droit^[5]. Toutefois, il semblerait que la jurisprudence allemande n'associe pas à ce dispositif une obligation de vigilance accrue pour le titulaire d'abonnement quant à la sécurisation ou l'utilisation par des tiers de sa connexion.

Ainsi, la responsabilité du titulaire peut être écartée par le juge allemand si la preuve est rapportée par ce dernier qu'une autre personne utilisait cette connexion internet au moment de ladite atteinte. Dans l'hypothèse où la connexion internet avait été sciemment laissée à la disposition d'autres personnes au moment de cette atteinte, le détenteur de cette connexion doit préciser, pour s'exonérer de sa responsabilité, l'identité des personnes qui avaient un accès autonome à sa connexion internet et qui sont dès lors susceptibles d'avoir commis l'atteinte alléguée au droit d'auteur.

S'agissant de l'utilisation de la connexion internet à des fins illicites par un enfant mineur de l'abonné, le 3 avril 2019, la cour fédérale a statué, après une décision en première instance et une décision en appel en 2017^[6] en sens similaire, que le droit fondamental au respect de la vie privée, notamment protégé par l'article 6 en droit constitutionnel allemand, ne devait pas faire obstacle à l'obligation qui pèse sur le titulaire de l'accès

[4] Article 97 a (2) de la loi allemande sur le droit d'auteur et les droits voisins telle qu'amendée par la loi du 1^{er} octobre 2013.

[5] Cour fédérale de justice, 8 janvier 2014 - I ZR 169/12.

[6] Cour fédérale de justice, 30 mars 2017, I ZR 19/16.

internet de divulguer quel membre de la famille avait commis l'atteinte aux droits d'auteur. Par conséquent, à défaut de divulgation, le titulaire de l'abonnement devra être considéré comme responsable de l'infraction lorsqu'il sait lequel de ses enfants mineurs avait partagé illégalement des œuvres mais qu'il a refusé de l'identifier.

Avant cette décision, une exonération semblait rester possible si les parents apportaient la preuve des mesures de sécurisation et de sensibilisation prises à l'encontre de leurs enfants^[7]. À l'inverse, un tribunal avait reconnu le père d'un enfant mineur responsable pour les actions de ce dernier dans la mesure où il n'avait pas suffisamment fait œuvre de pédagogie auprès de son enfant quant au partage illégal d'œuvres sur internet^[8].

S'agissant de l'utilisation de la connexion internet à des fins illicites par les membres majeurs du foyer de l'abonné, la cour fédérale allemande reconnaissait que l'abonné n'était pas tenu de fournir de précisions supplémentaires sur l'auteur de l'acte au sein de son foyer, eu égard à la protection du mariage et de la famille garantie par l'article 7 de la Charte des droits fondamentaux de l'Union européenne et aux dispositions respectives du droit constitutionnel allemand. L'abonné pouvait être exonéré de sa responsabilité après avoir établi qu'il ne pouvait s'agir de lui sans avoir à identifier et dénoncer la personne responsable au sein de son foyer. Il ne pouvait pas être exigé de lui qu'il surveille les activités de ces derniers pour obtenir cette information^[9].

La CJUE, saisie d'une question préjudicielle^[10], a jugé le 18 octobre 2018^[11] que la législation allemande telle qu'interprétée par la cour fédérale allemande n'assure pas un juste équilibre entre les droits fondamentaux en présence, à savoir le droit de propriété intellectuelle et le droit à un recours effectif d'une part, et le droit au respect de la vie privée et familiale d'autre part. La décision conclut que la jurisprudence de la cour fédérale est contraire au droit de l'Union en ce qu'elle prive les ayants droit d'un droit au recours effectif. En conséquence, le titulaire de l'abonnement doit voir sa responsabilité

engagée dès lors qu'il ne peut ou ne veut pas s'en exonérer en prouvant qu'il s'agit d'une autre personne majeure au sein du foyer. La cour souligne qu'il en va différemment si « *en vue d'éviter une ingérence jugée inadmissible dans la vie familiale* », une législation nationale prévoit que les titulaires de droits peuvent « *disposer d'une autre forme de recours effectif, leur permettant notamment, dans ce cas, de faire reconnaître la responsabilité civile du titulaire de la connexion à internet en cause* ».

LA SITUATION DES PROFESSIONNELS PROPOSANT À TITRE ACCESSOIRE UN ACCÈS WI-FI À LEURS CLIENTS

Une nouvelle législation sur le *Wi-Fi* est entrée en vigueur le 13 octobre 2017, amendant la loi sur les télémedias. Elle fait suite à la décision dite « *Mac Fadden* » de la CJUE du 15 septembre 2016^[12].

Dans cette décision, la Cour avait estimé que la directive dite « *commerce électronique*^[13] », qui prévoit un régime de responsabilité limité pour les intermédiaires techniques qui offrent un accès internet, s'applique y compris aux professionnels qui, à titre accessoire de leur activité économique, proposent un accès *Wi-Fi* à leurs clients.

Les ayants droit allemands ne pouvaient donc plus engager directement sur le fondement du droit commun la responsabilité des fournisseurs d'accès *Wi-Fi* en raison des actes illicites commis par leurs clients sur les réseaux pair à pair dans le cadre du dispositif indemnitaire.

La Cour de justice soulignait cependant que ces professionnels n'étaient pas pour autant exemptés de toutes obligations et pouvaient être enjoins de sécuriser leur réseau et de s'abstenir, à l'avenir, de permettre à des tiers de porter atteinte à une œuvre protégée *via* leur connexion internet. La nouvelle loi allemande tire donc les conséquences de cette jurisprudence avec pour

[7] Cour fédérale de justice, 15 novembre 2012, I ZR 74/12.

[8] Tribunal de Leipzig, 30 janvier 2017, 104 C 7366/16.

[9] Cour fédérale de justice, décision du 18 mai 2017, I ZR 154/15.

[10] Demande de décision préjudicielle présentée par le Landgericht München I (Allemagne) le 24 mars 2017 – Bastei Lübbe GmbH & Co. KG / Michael Strotzer (Affaire C-149/17) :

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=192289&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=2734>

La juridiction allemande a interrogé la Cour sur le point de savoir si la possibilité pour « le titulaire d'une connexion à l'internet par laquelle des atteintes au droit d'auteur ont été commises par un partage de fichiers » de ne pas voir sa responsabilité engagée « quand il désigne à tout le moins un membre de la famille qui avait comme lui la possibilité d'accéder à cette connexion à l'internet, sans donner davantage de précisions tirées de recherches faites sur le moment et la nature de l'utilisation de l'internet par ce membre de la famille » est compatible avec le droit de l'Union et notamment les dispositions relatives à la nécessité de prévoir des sanctions efficaces et dissuasives pour assurer le respect des droits de propriété intellectuelle.

[11] <http://curia.europa.eu/juris/document/document.jsf?text=&docid=206891&pageIndex=0&doclang=fr&mode=req&dir=&occ=first&part=1>

[12] CJUE, 15 septembre 2016, C-484/14, Tobias Mac Fadden c/ Sony Music Entertainment Germany GmbH.

[13] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.

objectif de promouvoir les *hot-spots Wi-Fi*, dont le développement en Allemagne aurait, selon la presse, pu être freiné par les craintes des professionnels de devoir indemniser les ayants droit et/ou de devoir sécuriser leur réseau par un mot de passe.

La nouvelle loi exclut que la responsabilité des fournisseurs d'accès *Wi-Fi* puisse être engagée pour les actes de contrefaçon commis par leurs utilisateurs. Elle exclut également l'obligation pour ceux-ci de sécuriser leur réseau par une identification par mot de passe et identifiant. Dans l'exposé des motifs du texte notifié à la Commission européenne, le gouvernement relevait en effet qu'un tel dispositif, avec la levée d'anonymat qu'il comporte, implique la collecte de données personnelles, ce qui entraîne des obligations juridiques supplémentaires et donc des coûts que certains opérateurs ne pourraient pas supporter. Ils ne pourront ainsi être mis en cause qu'à titre subsidiaire, si l'ayant droit a d'abord échoué dans son action contre le vrai contrevenant ou l'hébergeur, plus proches de la commission de l'infraction.

Le texte précise enfin que les opérateurs peuvent mettre en place des mesures de sécurisation sur une base volontaire telle que du filtrage de port pour empêcher l'accès aux réseaux pair à pair ou du blocage de pages *web*. Un système de liste noire a pu être évoqué par le gouvernement (à l'instar d'une liste allemande de sites dangereux pour la jeunesse pouvant être chargés sur le routeur afin de les filtrer).

LA PROMOTION DE L'OFFRE LÉGALE

Les initiatives privées se développent afin d'améliorer la visibilité de l'offre légale. Le syndicat de la musique a un temps utilisé un label (Playfair) octroyé aux sites considérés comme légaux. Un portail (*was-ist-vod.de*) qui liste les plateformes proposant une offre légale a été créé par les ayants droit de l'audiovisuel.

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES OPÉRATEURS DES SERVICES ILLICITES

Jusqu'à ce que celle-ci se déclare en faillite, des actions pénales étaient notamment entreprises par la *Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V. (GVU)*, une association de titulaires de droits de différents secteurs (cinéma, quelques chaînes de télévision dont des chaînes sportives, jeux vidéo, sociétés de gestion collective, livres) – à l'exception de l'industrie musicale – chargée d'initier au nom de ses membres des actions pénales visant à la fermeture des sites destinés spécifiquement au public allemand.

À la suite de l'action pénale engagée par la GVU, fin 2019, les autorités allemandes ont notamment procédé à la fermeture de *Share-online.biz*, le plus grand site d'hébergement de fichiers allemand.

LES ACTIONS DES AYANTS DROIT DE LA MUSIQUE CONTRE DES SITES DE STREAM RIPPING ILLICITES

Sony Music a assigné le service « *MusicMonster.fm* » devant la cour régionale de Munich. Ce service proposait à ses utilisateurs de créer des listes de morceaux de musique dont ils souhaitaient avoir une copie. Le service scannait ensuite les radios sur internet : lorsqu'il détectait les morceaux choisis par l'utilisateur, il les copiait et les offrait au téléchargement au format MP3 à ce dernier. Le service prétendait que sa démarche était légitime, estimant que les utilisateurs avaient déjà acquitté les droits dès lors que les stations de radio avaient payé leurs droits de licence et qu'à ce titre, l'exception de copie privée s'appliquait. En septembre 2017, la cour a estimé que le service ne pouvait se prévaloir de l'exception de copie privée. Le 22 novembre 2018, la haute cour régionale de Munich a confirmé cette décision de première instance.

Le 17 janvier 2019, la haute cour régionale de Hambourg a considéré que le service « ZeeZee », qui offre un service similaire à celui de « MusicMonster.fm », est également illicite^[14]. La haute cour ajoute que, dans le système automatisé mis en place par « ZeeZee », l'utilisateur n'est pas celui qui fait la copie, mais « ZeeZee » lui-même. Dès lors, l'exception de copie privée ne peut s'appliquer, à l'instar de « MusicMonster.fm ».

En juin 2019, le site « Convert2MP3 », à la suite de son assignation par des représentants de l'industrie musicale, a conclu un accord le contraignant à fermer, à transférer son nom de domaine à l'IFPI et à payer des dommages-intérêts aux ayants droit.

L'ACTION CONTRE UN HÉBERGEUR DE NEWSGROUPS

En juin 2018, dans une affaire initiée par la GEMA, l'homologue allemand de la SACEM, le tribunal de Hambourg a jugé qu'un hébergeur de *newsgroups* pouvait être tenu responsable des infractions commises par ses utilisateurs^[15].

LES MESURES JUDICIAIRES DE BLOCAGE

Les actions contentieuses des ayants droit allemands sont longtemps restées intentées directement contre les sites eux-mêmes (et leurs fondateurs) en raison de leur responsabilité. Le droit allemand ne prévoyait en effet pas, en matière de droit d'auteur (et à la différence d'autres enjeux comme la lutte contre la pédopornographie), de procédures impliquant les intermédiaires indépendamment de toute mise en cause de leur responsabilité ou sans avoir, de manière subsidiaire, épuisé préalablement les autres voies de recours – telles que prévues par l'article 8.3 de la directive

du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information. Les demandes de blocage de sites adressées aux fournisseurs d'accès à internet étaient donc peu usuelles car complexes à mettre en œuvre selon la tradition juridique allemande. La décision Goldesel rendue en 2015 par la cour fédérale allemande^[16] a cependant posé que le blocage de sites était possible en vertu dans le respect des principes du droit allemand de la responsabilité et en application de l'article 8.3 de la directive européenne sur le droit d'auteur. Suite à cette évolution, le gouvernement a également modifié la loi sur les télémedias, précitée, qui comprend désormais une base juridique au blocage^[17]. Bien que la loi ne s'applique en principe qu'aux opérateurs de réseaux *Wi-Fi*, dans une décision du 26 juillet 2018^[18], la cour fédérale allemande de justice a confirmé que la loi sur les télémedias permettait de solliciter le blocage de sites litigieux auprès des fournisseurs d'accès *Wi-Fi* ce qui était conforme au droit européen. C'est également ce qu'a estimé le tribunal de Munich dans une décision du 7 juin 2019^[19].

Il apparaît ainsi que la loi et la jurisprudence actuelles sont très proches de l'article 8.3 de la directive de 2001 mais que le principe de subsidiarité limite toujours ces actions car il est toujours exigé que les titulaires de droits aient intenté des actions directes contre les exploitants de sites et les fournisseurs d'hébergement. Ce n'est qu'en cas d'échec de ces tentatives directes qu'ils peuvent demander la mise en place de blocages de sites web.

Dans ce contexte, l'opérateur Vodafone a cependant bloqué en mars 2019 un site de partage de liens à la demande de la GEMA (équivalent allemand de la SACEM). Vodafone a considéré qu'il était soumis à une obligation subsidiaire de blocage des sites dès lors que la GEMA lui avait notifié l'illicéité du service.

[14] Haute cour régionale de Hambourg, 17 janvier 2019, n° 5 U 18/17.

[15] Tribunal de Hambourg, 22 juin 2018.

[16] Cour fédérale de justice, 26 novembre 2015 - I ZR 174/12.

[17] Loi sur les télémedias : « 7 (4) Si un service de télémedia a été utilisé par un utilisateur pour violer les droits de propriété intellectuelle d'une autre personne et si le titulaire de ce droit n'a pas d'autre recours contre la violation de son droit, le titulaire du droit peut alors exiger du prestataire de services concerné selon l'article 8, paragraphe 3, le blocage de l'utilisation des informations afin d'éviter la répétition de l'infraction. Le blocage doit être raisonnable et proportionné. Il n'y a aucun droit à l'encontre du prestataire de services au remboursement des frais précontentieux et extrajudiciaires encourus pour la revendication et l'exécution du droit selon la phrase 1, sauf dans les cas visés à l'article 8, paragraphe 1, phrase 3. »

[18] Cour fédérale Allemande de justice, 26 juillet 2018, n° I ZR 64/17,

<http://www.hadopi.info/dj/news/ressources/26%20july%202018%20Dead%20Island%20BGH.pdf>

[19] Tribunal de Munich, 7 juin 2019, n° 37 O 2516/18,

[http://www.hadopi.info/dj/news/ressources/20190607 Regional Court of Munich - Goldesel - website blocking \(English version\).pdf](http://www.hadopi.info/dj/news/ressources/20190607 Regional Court of Munich - Goldesel - website blocking (English version).pdf)

L'IMPLICATION DES BUREAUX D'ENREGISTREMENT

Dans une décision du 19 décembre 2018, le tribunal supérieur de Sarrebruck a jugé, dans le cadre d'une procédure intentée par les ayants droit de la musique, qu'un bureau d'enregistrement pouvait être tenu responsable des infractions commises par un site contrefaisant s'il n'a pas procédé à la suspension de son nom de domaine alors qu'il a reçu une notification lui signalant le caractère manifestement illicite de ce site^[20].

L'IMPLICATION DES RÉSEAUX DE DIFFUSION DE CONTENUS

Dans une décision du 30 janvier 2020^[21], dans le cadre d'une procédure intentée par les ayants droit de la musique, le tribunal de Cologne a en revanche estimé qu'un fournisseur d'un réseau de diffusion de contenu (en l'espèce Cloudflare) pourrait voir sa responsabilité engagée s'il ne prenait pas des mesures à l'encontre du site illicite en cause. Le tribunal l'a ainsi enjoint de cesser de faciliter l'accès aux contenus protégés visés dans la procédure en bloquant l'accès à ce site sous peine de devoir payer une amende allant jusqu'à 250 000 euros par infraction ou, à titre subsidiaire, le directeur général de Cloudflare pourrait purger jusqu'à six mois de prison. Celui-ci doit également fournir au demandeur des informations sur le nom et l'adresse des opérateurs du service visé. Cette décision a été confirmée en appel en octobre 2020.

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

Les ayants droit allemands ont initié des procédures afin d'obtenir des services de paiement l'identité des contrefacteurs afin de les poursuivre. Le 22 mars 2017, le tribunal de Hambourg^[22] a jugé que le service de paiement en ligne PayPal doit divulguer l'identité de l'administrateur d'un site illicite dès lors que ce dernier est financé au moyen de transactions réalisées via l'intermédiaire de paiement, mais aussi celle du client du site illicite qui achète un objet protégé par un droit de propriété intellectuelle et celle de l'administrateur de ce site.

En 2016, un juge allemand avait déjà ordonné à PayPal de divulguer l'identité du titulaire d'un compte qui vendait sur internet des objets contrefaisants^[23].

[20] Tribunal supérieur de Sarrebruck, 19 décembre 2018, n° 1 U 128/1,

http://www.hadopi.info/dj/news/ressources/Judgement%20of%20the%20Higher%20Regional%20Court%20of%20Saarbr%c3%bc-cken_Registrar%20Key%20System...pdf

[21] Tribunal de Cologne, 30 janvier 2020, n° 140 171/19,

http://www.hadopi.info/dj/news/ressources/20200316%20Cloudflare%20judgment%20Cologne%20first%20instance%20ENGLISH_re-dacted.pdf

[22] Tribunal de Hambourg, 22 mars 2017.

[23] Tribunal de Hambourg, 11 juillet 2016.

ARGENTINE

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

45,2 POPULATION^[1]
en millions

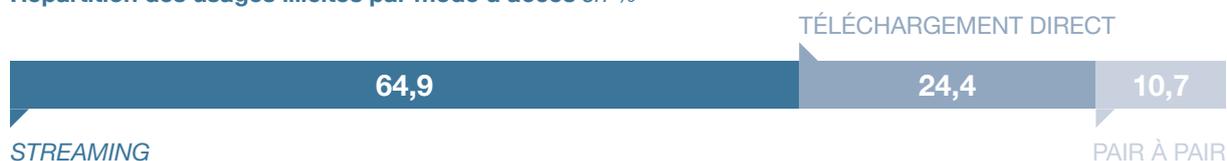
74,3 % TAUX DE PÉNÉTRATION
INTERNET (2017)^[2]

USAGES ILLICITES^[3]

1,7 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

50 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illégitimes par mode d'accès en %



En Argentine, l'offre légale musicale et audiovisuelle se diversifie de plus en plus (Spotify, Deezer, Netflix...) mais les usages illégitimes resteraient importants et se feraient par différentes technologies : *streaming*,

pair à pair, boîtier configuré avec une utilisation plus importante du téléchargement direct et du *stream ripping* illégitime.

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES MESURES JUDICIAIRES DE BLOCAGE

L'Argentine est le premier pays d'Amérique du Sud à avoir prononcé ce type de mesures en 2014. À la suite d'une action initiée par un représentant des producteurs de phonogrammes, *Cámara Argentina de Productores de Fonogramas*, d'un jugement favorable de la 67^e cour fédérale de district en 2014, l'autorité publique locale, la commission nationale de la communication a ordonné le blocage du site « *The Pirate Bay* » aux fournisseurs d'accès à internet (12 noms de domaine et 256 adresses IP).

Des studios américains ont également obtenu en décembre 2018 une injonction de blocage par les fournisseurs d'accès internet d'un site illégitime très célèbre, *Cuevana*, qui proposait aux internautes de visionner des films et des séries en *streaming*. Il s'agit d'une suspension préventive prévue par l'article 79 de la loi sur la propriété intellectuelle argentine qui permet aux juges, sur paiement d'une caution de la part de l'intéressé, d'ordonner la suspension préventive d'une pièce de théâtre, cinématographique, philharmonique ou tout autre spectacle similaire pour protéger efficacement les droits des auteurs.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

AUSTRALIE

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

25,5 POPULATION^[1]
en millions

86,6 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

1,6 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

73 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



L'Australie met aujourd'hui en œuvre des actions essentiellement pédagogiques à l'égard des internautes. L'Australie s'est en revanche dotée en 2015 d'une loi permettant le blocage des sites massivement contrefaisants situés à l'étranger. Une loi complémentaire a été adoptée en novembre 2018 pour permettre le blocage de sites locaux,

obtenir des mesures de déréférencement ou de sous-référencement et faciliter, dans le cadre d'accords auxquels renverra l'injonction judiciaire, le blocage et le déréférencement des sites de contournement. Des réflexions ont également été conduites pour responsabiliser les plateformes.

LES ACTIONS VISANT LES INTERNAUTES

LE DISPOSITIF DE MISE EN DEMEURE INDEMNITAIRE

En 2016, s'est achevée une procédure très médiatisée en Australie visant à l'envoi de mises en demeure indemnitaire aux internautes ayant partagé le film *Dallas Buyers Club* sur les réseaux pair à pair. La procédure avait été initiée par un ayant droit et visait à obtenir auprès de cinq fournisseurs d'accès à internet l'identification de 4 700 adresses IP.

La décision rendue par la justice australienne a précisé les contours de ce type d'action en indiquant que les identités des internautes pourraient être communiquées à l'ayant droit, sous réserve que celui-ci demande aux internautes des sommes estimées raisonnables par le juge.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

LES ACTIONS DE SENSIBILISATION

Une campagne dédiée à l'encouragement de l'offre légale et à l'éducation au droit d'auteur a été mise en place par des ayants droit de l'audiovisuel qui se sont regroupés au sein d'une organisation appelée *Creative Content Australia*^[4]. Un site dédié propose des contenus pédagogiques à destination des professeurs et des élèves, un lien vers un répertoire des plateformes légales par type d'œuvres^[5], des études et réponses à des questions fréquentes sur le piratage et les contenus culturels. Une étude sur les usages illicites en Australie est ainsi conduite chaque année depuis 2010^[6].

À la suite d'une décision de blocage de sites contrefaisants, *Creative Content Australia* a lancé le 18 août 2017 une nouvelle campagne de communication intitulée « *Price of piracy* » visant à alerter les consommateurs sur la présence de logiciels malveillants sur les sites illégaux de *streaming* et de pair à pair. Un site internet

dédié^[7] a été créé : il comporte notamment des vidéos expliquant les dangers de la consommation illégale et des spots publicitaires avec un célèbre acteur australien qui alerte les consommateurs sur les effets de la consommation illégale.

En 2018, le même organisme a lancé une autre campagne de communication « *Say no to piracy* » qui a pour but de célébrer la création et l'innovation et de montrer l'importance de consommer légalement pour permettre la création de films. La campagne 2020 « *Piracy – You're exposed*^[8] » insiste à nouveau sur les risques encourus par les internautes ayant des usages illicites, s'appuyant notamment sur les données collectées lors de l'étude sur les usages de 2019, aux termes de laquelle près d'un adolescent australien sur quatre connaît quelqu'un qui a été victime de logiciels malveillants ou de virus liés au piratage, tandis que 62 % des adultes et 75 % des adolescents ayant régulièrement des usages illicites ont subi des failles de sécurité.

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES OPÉRATEURS DES SERVICES ILLICITES

La *Coalition Against Piracy* (CAP), qui regroupe les acteurs de l'écosystème de la fourniture de services de télévision en Asie^[9], et l'ACE ont collaboré dans le cadre d'une opération conduite fin 2017 en Australie. Cette action a permis de faire cesser les activités contrefaisantes d'un vendeur de boîtiers configurés pour permettre d'accéder illicitement à des contenus à la demande vendus avec un abonnement d'un an à un bouquet de chaînes retransmises sans autorisation^[10].

LES MESURES JUDICIAIRES DE BLOCAGE

LES PROCÉDURES INTENTÉES DANS LE CADRE DE LA LOI DE 2015

Une loi entrée en vigueur en juin 2015, *Copyright Amendment (online infringement) Act 2015*^[11], prévoit la possibilité pour les ayants droit de demander en justice le blocage par les fournisseurs d'accès à internet de services localisés à l'étranger qui ont pour objet principal de porter atteinte ou de faciliter les atteintes au droit d'auteur. La loi prévoit que le demandeur doit contacter tous les services dont il demande le blocage pour les aviser de la procédure.

[4] www.creativecontentaustralia.org.au

[5] www.digitalcontentguide.com.au

[6] <https://www.creativecontentaustralia.org.au/research/2020>

[7] <https://thepriceofpiracy.org.au/>

[8] <https://contentcafe.org.au/articles-stories-everything/if-you-visit-pirate-websites-even-the-law-cant-protect-you/>

[9] BeIN Sports, casbaa, The Walt Disney Company, Fox Networks Group, HBO Asia, NBCUniversal, Premier League, Turner Asia-Pacific, A&E Networks, Astro, BBC Worldwide, CANAL+, Cignal, Media Partners Asia, National Basketball Association, PCCW Media, Singtel, Sony Pictures Television Networks Asia, TVB, True Visions, TV5MONDE et Viacom International Media Networks.

[10] <http://www.casbaa.com/news/casbaa-news/alliance-for-creativity-and-entertainment-ace-and-casbaas-coalition-against-piracy-cap-close-down-australian-illicit-streaming-device-operation/>

[11] <https://www.legislation.gov.au/Details/C2015A00080>

Sur ce fondement, pour la première fois en février puis en avril 2016, des ayants droit de l'audiovisuel ont assigné des fournisseurs d'accès à internet devant un tribunal fédéral pour obtenir le blocage de sites et de leurs *proxies* (notamment *KickassTorrents*). La première décision rendue en la matière, en décembre 2016^[12], relève qu'il incombe aux ayants droit de supporter les coûts du blocage (environ 30 euros par nom de domaine). Les internautes qui chercheront à accéder aux sites bloqués seront accueillis par une page leur indiquant que le site a été bloqué à la suite d'une décision de justice. À cette occasion, *Village Roadshow*, ayant droit du secteur audiovisuel à l'origine de ces procédures de blocage, a lancé une campagne de communication dans différents médias sur les risques associés à ce type de sites pour leurs utilisateurs, et notamment sur le fait qu'ils contiennent beaucoup de virus.

Depuis, trois décisions de blocage ont été rendues en 2017 et une en 2018^[13] : trois en faveur des ayants droit de l'audiovisuel et une en faveur des ayants droit de la musique^[14], lesquelles ont conduit au blocage de plus de 500 sites. En avril 2018, une galaxie de services proposant *via* une application une offre payante illégale de contenus en direct (chaînes payantes) et à la demande a également été bloquée^[15].

Pour diminuer le coût des procédures, un opérateur de télévision payante, Foxtel, a demandé en 2018 au juge de ne pas solliciter la présence d'experts lors du procès et de remplacer la démonstration de l'illicéité *in vivo* du site lors de l'audience par des vidéos et des captures d'écran. Ces requêtes ont été accueillies favorablement par le juge.

Le juge laisse aux fournisseurs d'accès à internet le choix de la mesure de blocage, en précisant qu'un blocage DNS ou un blocage IP notamment sont acceptables.

LA NOUVELLE LOI ADOPTÉE EN NOVEMBRE 2018^[16]

Une loi (*Copyright Amendment (Online Infringement) Bill* 2018) a été adoptée fin novembre 2018^[17] :

- elle allège la charge de la preuve pour les ayants droit en créant une présomption réfragable selon laquelle le site visé est à l'étranger ;
- elle permet d'obtenir le blocage de sites qui ont pour effet substantiel de porter atteinte au droit d'auteur ;
- elle permet aux ayants droit d'obtenir des mesures de déréférencement ou de sous-référencement ;
- elle introduit la possibilité d'obtenir des injonctions facilitant le blocage et le déréférencement des services de contournement sans avoir besoin de retourner devant le juge en permettant que ces injonctions renvoient à des accords entre les parties.

La loi n'a pas retenu la proposition des ayants droit de la musique (*Music Rights Australia*) visant à l'uniformisation du texte de la page vers laquelle les internautes allaient être renvoyés s'ils visitaient un site bloqué, alors que la plupart des fournisseurs d'accès (très nombreux en Australie) utilisent une page développée en interne et non celle créée par les ayants droit.

Elle ne traite pas non plus des coûts des mesures de blocage alors que *Music Rights Australia* avait indiqué que le montant de 30 euros par nom de domaine et par fournisseur d'accès à internet arrêté par la jurisprudence semblait peu élevé, mais pouvait cependant rapidement devenir prohibitif dans la mesure où un seul site illicite peut avoir jusqu'à des centaines de « miroirs » et où il y existe une centaine de fournisseurs d'accès à internet en Australie. Les ayants droit de la musique ont d'ailleurs relevé qu'à l'international, 27 pays ont prononcé des décisions de blocage concernant 2 800 URL et dans la plupart des cas, les fournisseurs d'accès à internet n'ont pas demandé à être indemnisés pour mettre en œuvre ces mesures.

[12] www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2016/2016fca1503

Le 15 novembre 2019, la Cour fédérale d'Australie a ordonné le renouvellement des injonctions de blocage de site prononcées aux termes de la décision du 15 décembre 2016,

[http://www.hadopi.info/dj/news/ressources/2%20Orders%20\(NSD%20239%20of%202016\)%2015%20November%202019.pdf](http://www.hadopi.info/dj/news/ressources/2%20Orders%20(NSD%20239%20of%202016)%2015%20November%202019.pdf)

[13] <http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2018/2018fca0933>

[14] <http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2017/2017fca0435>

[15] <http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2018/2018fca0582>

[16] <https://parliinfo.aph.gov.au/parliInfo/search/display/display.w3p?page=0;query=BillId:r6209%20Reconstruct:billhome>

[17] <https://www.legislation.gov.au/Details/C2018A00157/Html/Text>

LA MISE EN ŒUVRE DE LA LOI DE 2018

À la suite de l'entrée en vigueur de la loi, les procédures se sont multipliées. Ces procédures visent pour la plupart un nombre important de sites et s'attaquent à de nouvelles catégories de sites tels que des proxys, qui sont des services qui servent de site « intermédiaire » pour accéder à un site bloqué par exemple, et ce grâce à la disposition permettant de viser des sites ayant pour effet substantiel de porter atteinte au droit d'auteur. De même, on peut notamment relever que quatre sites illicites de *stream ripping* ont pour la première fois fait l'objet de mesures de blocage en mai 2019^[18]. L'un de ces sites a également fait l'objet d'une décision de blocage au Danemark et les trois autres d'une procédure aux États-Unis. Pour trancher dans le sens des ayants droit, le juge a retenu que c'est le site de *stream ripping* qui met en réalité à disposition le fichier à l'utilisateur final, réalisant ainsi une communication au public illicite, à une échelle industrielle. Les fournisseurs d'accès sont également tenus de rediriger les utilisateurs qui tentent d'accéder à ces sites vers une page d'information leur indiquant que le site a été bloqué sur décision de justice^[19] ou vers une page d'accueil de leur propre conception.

L'ACTUALISATION DES MESURES JUDICIAIRES DE BLOCAGE

La première décision portant sur une demande d'injonction dynamique a été rendue le 27 août 2019^[20]. Elle prévoit que l'actualisation des mesures de blocage passe par le biais d'un *affidavit* préparé par le demandeur indiquant que les sites visés par la décision sont accessibles *via* de nouveaux noms de domaine, ainsi qu'un procès-verbal, également rédigé par le demandeur, proposant d'amender l'injonction en ce sens.

Ces documents devront être transmis au juge et signifiés aux fournisseurs d'accès à internet. Ceux-ci auront ensuite sept jours ouvrables pour faire savoir s'ils s'opposent à ce que l'injonction du juge soit amendée conformément à ce qui est indiqué dans le procès-verbal. Si l'un des défendeurs ou si le juge s'oppose à ces

demandes, les parties devront être entendues par le juge. Dans le cas contraire, les mesures de suivi de la décision de blocage pourront être mises en œuvre une fois la modification de l'injonction validée par la cour.

Le dispositif mis en œuvre par cette décision est prévu pour une durée initiale de trois ans. Au moins deux mois avant son échéance, le demandeur doit transmettre d'une part un *affidavit* qui déclare que tous ou certains des noms de domaine cibles continuent d'avoir le but principal et/ou le principal effet de porter atteinte ou de faciliter la violation du droit d'auteur ; et, d'autre part, un procès-verbal demandant le prolongement des mesures pour ces noms de domaine pour une nouvelle période de trois ans.

La jurisprudence en matière d'actualisation des mesures de blocage a un peu évolué depuis la décision d'août 2019. Ainsi, l'injonction judiciaire rendue dans une nouvelle affaire le 20 avril 2020^[21] double le délai laissé aux fournisseurs d'accès à internet et au juge pour répondre à un *affidavit* indiquant que les sites bloqués sont accessibles *via* d'autres adresses, celui-ci passant de sept à quatorze jours. Le juge semble également introduire une troisième voie face aux réponses à l'*affidavit* : les fournisseurs d'accès qui ne s'opposeraient pas à l'actualisation des mesures de blocage pourraient seuls mettre en œuvre ces mesures d'actualisation alors que les fournisseurs d'accès réfractaires pourraient quant à eux être à nouveau entendus par le juge.

L'IMPLICATION DES MOTEURS DE RECHERCHE

La loi de 2018 permettait de demander le déréférencement de sites, dispositif auquel Google s'était opposé lors des travaux relatifs à l'adoption de la loi mais ce dispositif ne semble pas avoir été mis en œuvre. En effet, en mai 2019, Google a volontairement consenti à déréférencer 832 sites illicites de son moteur de recherche. Ces déréférencements font suite à un accord convenu entre les ayants droit et les fournisseurs d'accès à internet australiens.

[18] <https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2019/2019fca0751>

[19] <http://www.copyrightpage.com/>

[20] <https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2019/2019fca1450>

[21] <https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2020/2020fca0507>

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

Depuis octobre 2013, suivant l'approche « *Follow the money* », un groupement d'ayants droit du secteur musical, *Music Rights Australia*, collabore avec une association regroupant des acteurs de la publicité, *Audited Media Association of Australia*, afin de les sensibiliser au financement des sites contrefaisants par la publicité et au préjudice causé par ces sites.

Le but de cette initiative est de diffuser et faire appliquer un code de bonne conduite devant permettre de réduire le placement de publicités sur de tels sites. Bien qu'un accord ait été trouvé et que ce code soit déjà élaboré, il reste des résistances au sein des acteurs de la publicité pour le mettre en œuvre.

LES ACTIONS VISANT À RESPONSABILISER LES PLATEFORMES DE PARTAGE DE CONTENUS

Il existe en Australie un régime de responsabilité allégée pour les intermédiaires techniques mais, contrairement à ce qui est le cas ailleurs, ce régime ne s'appliquait qu'aux seuls fournisseurs d'accès à internet à l'exclusion des autres intermédiaires techniques et assimilés, dont les plateformes.

Le gouvernement a réalisé une consultation en avril 2017 sous la forme de réunions et discussions avec les parties prenantes pour savoir si ce régime devait évoluer. Les ayants droit se sont opposés à une telle réforme en se basant sur les difficultés que rencontrent les ayants droit en Europe et aux États-Unis pour obtenir le retrait de contenus contrefaisants sur ces plateformes. Le gouvernement n'a finalement pas étendu le dispositif aux plateformes pour le moment^[22].

[22] <https://www.legislation.gov.au/Details/C2018A00071>

BELGIQUE

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

11,6 POPULATION^[1]
en millions

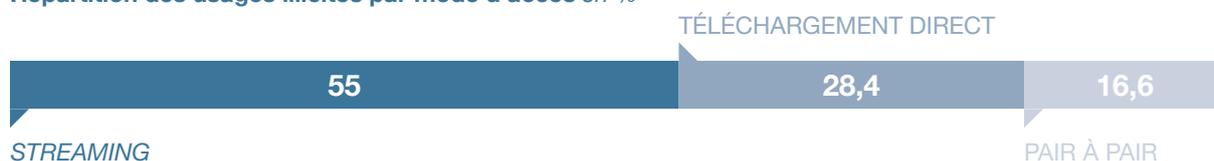
90,3 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

0,7 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

68 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



Le dispositif mis en œuvre en Belgique allie des actions visant à modifier le comportement des

internautes et des actions pour lutter contre les services contrefaisants.

LES ACTIONS VISANT LES INTERNAUTES

LE DISPOSITIF DE MISE EN DEMEURE INDEMNITAIRE

Dans le cadre d'un contentieux opposant un fournisseur d'accès à internet à un prestataire spécialisé dans l'envoi de demandes d'indemnisation aux internautes partageant des films pornographiques *via BitTorrent*, le 6 août 2019, un tribunal situé à Anvers a posé plusieurs questions préjudicielles à la CJUE. Ces questions portent pour partie sur le cas d'espèce, à savoir la possibilité pour un prestataire qui a acquis les droits de diffusion *BitTorrent* de films pornographiques et ne les diffuse pas par ce biais, de se contenter de formuler des demandes d'indemnisation. Elles portent également sur la qualification, au regard du droit de communication au public, des « segments » d'œuvres qui sont partagés par les internautes en même temps que ceux-ci les téléchargent ainsi que sur la compatibilité au regard

du règlement général sur la protection des données de la collecte et du traitement des adresses IP des internautes qui partagent les contenus^[4].

LES ACTIONS DE SENSIBILISATION

Une campagne de sensibilisation a été lancée en janvier 2018 par la *Belgian Entertainment Association (BEA)*, qui regroupe les différents ayants droit, afin notamment de sensibiliser les internautes au fait que le téléchargement illégal n'est pas sans conséquences. Des sous-titres susceptibles d'être téléchargés par les internautes inscrivent des messages de type « ne téléchargez pas illégalement ». Lorsque des internautes téléchargent ces sous-titres pour les lire en lien avec une œuvre également illicitement mise à disposition, ceux-ci pourront voir, par exemple dans le film « *Hitman & Bodyguard* », l'acteur

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] CJUE, C-597/19, M.I.C. M. Mircom International Content Management & Consulting Limited/Telenet BVBA.

Samuel L Jackson dire « *je n'ai pas besoin de faire de recherche pour voir qu'il s'agit de mauvais sous-titres* » ou encore « *tu voulais devenir policier jusqu'à ce que tu télécharges* ».

LA PROMOTION DE L'OFFRE LÉGALE

Afin de diriger les internautes vers l'offre légale, la BEA a créé un site internet référençant l'offre légale pour les films, les séries, la musique, les livres et les jeux vidéo.

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACCORDS DE COOPÉRATION AVEC LES FOURNISSEURS D'ACCÈS À INTERNET

Dès 1999, un accord a été signé entre l'association belge des fournisseurs d'accès à internet (ISPA) et le gouvernement fédéral. Cet accord prévoit notamment de mettre en place une collaboration entre les fournisseurs d'accès à internet et la police judiciaire (*Computer Crime Unit*), aux fins de blocage de contenus constitutifs d'infractions pénales.

En 2005, l'ISPA et les représentants de l'industrie musicale (IFPI) ont conclu un accord visant à lutter contre le partage de musique sur des groupes de discussion. Selon cet accord, l'IFPI peut demander aux fournisseurs d'accès à internet de bloquer l'accès des groupes de discussion sur lesquels sont partagés un nombre significatif de contenus musicaux illicites ou de liens vers de tels contenus.

LES MESURES JUDICIAIRES DE BLOCAGE

La Société belge des auteurs, compositeurs et éditeurs (SABAM) a initié dès 2004 une procédure contre un fournisseur d'accès à internet afin d'obtenir que celui-ci bloque l'intégralité des communications d'œuvres illicites, et notamment *via* les réseaux pair à pair. En 2009, elle a ensuite sollicité d'un réseau social qu'il mette en œuvre des mesures de filtrage des contenus. Ces deux procédures ont donné lieu à des questions préjudicielles soumises à la CJUE, mais les demandes des ayants droit telles que formulées à l'époque avaient été regardées comme disproportionnées^[5].

C'est finalement en 2011 qu'une première décision de blocage a été prononcée en Belgique, à l'encontre de deux fournisseurs d'accès à internet, leur enjoignant de mettre en œuvre un blocage DNS à l'égard du site « *The Pirate Bay* » et de plusieurs noms de domaine associés^[6]. À la suite de cette décision, la *Belgian Anti-Piracy Federation* (BAF), association concentrant à l'époque les initiatives des ayants droit visant à lutter contre le piratage, a mis en demeure d'autres fournisseurs d'accès à internet non parties à l'instance de procéder aux blocages des sites visés par cette décision afin d'éviter les frais liés à une action judiciaire à leur encontre.

Dans le cadre d'une procédure pénale, un juge d'instruction a également enjoint tous les fournisseurs d'accès à internet de rendre inaccessible l'accès au service « *ThePirateBay.org* » et aux services associés dans la mesure où ils sont liés aux adresses IP des serveurs identifiés ou aux contenus hébergés sur ces serveurs. Cette décision, confirmée par la Cour de cassation le 22 octobre 2013^[7], prévoit également :

- que les fournisseurs d'accès à internet seront informés par la police belge, la *Federal Crime Computer Unit* (FCCU) et la *Regional Computer Crime Unit* (RCCU Mechelen), des noms de domaine à bloquer ;
- que les internautes cherchant à accéder à l'un des noms de domaine concernés seront renvoyés vers une page d'information publique.

En janvier 2018, à la suite d'une assignation en justice de la BEA contre les trois principaux fournisseurs d'accès à internet (Proximus, Telenet et Voo), les parties ont déposé une requête conjointe visant le blocage d'une trentaine de sites illicites *via* 450 noms de domaine. Cette approche conjointe a notamment pour objectif d'accélérer la procédure de blocage. Chaque partie

[5] CJUE, 24 novembre 2011, C-70/10, *Scarlet Extended SA contre Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) et autres* ; CJUE, 16 février 2012, C-360/10, *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) contre Netlog NV*.

[6] Cour d'appel d'Anvers, 26 septembre 2011, *Belgian Anti-Piracy Federation (BAF) contre Telenet et Belgacom*.

[7] Cour de cassation, 22 octobre 2013, P.13.0550.N, https://lex.be/fr/doc/be/jurisprudence-belgique/cour-de-cassation-arret-22-octobre-2013-bejc_201310223_fr

supporte en outre ses propres coûts. Les parties ont indiqué au juge qu'elles se réservaient la possibilité de le saisir à nouveau aux fins d'actualisation de la liste. Le 30 mars 2018, le juge^[8] a ordonné le blocage DNS des 450 noms de domaine et la publication d'un message d'information à l'attention des internautes.

Le 3 août 2018, le juge^[9] a ordonné le blocage DNS de 98 noms de domaine dans le cadre d'une nouvelle procédure qui avait deux objets :

- actualiser les mesures de blocage ordonnées en mars 2018 en demandant d'une part le déblocage de 181 noms de domaine bloqués depuis la décision de mars et d'autre part le blocage de 36 noms de domaine associés aux sites visés par la décision de mars ;
- demander le blocage de 62 noms de domaine, en lien avec 17 sites internet non visés par la décision de mars.

Afin d'actualiser les mesures de blocage prononcées par les jugements des 30 mars et 3 août 2018, le tribunal de commerce francophone de Bruxelles a ordonné le 30 janvier 2019^[10] :

- le blocage de 92 noms de domaine dont une partie sont des noms de domaine alternatifs qui renvoient vers des sites ayant d'ores et déjà fait l'objet de mesure de blocage aux termes desdits jugements ;
- la suppression des mesures de blocage concernant 111 noms de domaine mises en place à la suite desdits jugements et ne renvoyant plus vers du contenu contrefaisant.

L'IMPLICATION DES REGISTRES

Dans une décision rendue par le tribunal de première instance de Bruxelles le 9 août 2013, les registres ont été pleinement reconnus comme étant des services de la société de l'information contre lesquels les titulaires de droits peuvent solliciter des mesures^[11]. La demande visant à obtenir la désactivation des futurs noms de domaine contrefaisants notifiés par les ayants droit, sans examen du tribunal, a toutefois été rejetée, le juge considérant qu'une décision de justice est nécessaire pour s'assurer qu'un site est en infraction.

[8] Tribunal de commerce francophone de Bruxelles, Chambre des actions en cessation, 30 mars 2018, numéro de rôle A/18/00217.

[9] Tribunal de commerce francophone de Bruxelles, Chambre des actions en cessation, 3 août 2018, numéro de rôle A/18/02607.

[10] Tribunal de commerce francophone de Bruxelles, Chambre des actions en cessation, 30 janvier 2019, numéro de rôle A/18/05226, [http://www.hadopi.info/dj/news/ressources/5%20BE%20190130%20District%20Court%20Brussels,%20BEA%20v%20ISPs,%2030%20January%202019%20\(27%20sites%20-%2092%20domains\)%20OL%20FR.pdf](http://www.hadopi.info/dj/news/ressources/5%20BE%20190130%20District%20Court%20Brussels,%20BEA%20v%20ISPs,%2030%20January%202019%20(27%20sites%20-%2092%20domains)%20OL%20FR.pdf)

[11] Tribunal de première instance de Bruxelles, 9 août 2013, n° 2012/12072/A.

BRÉSIL

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

221,6 POPULATION^[1]
en millions

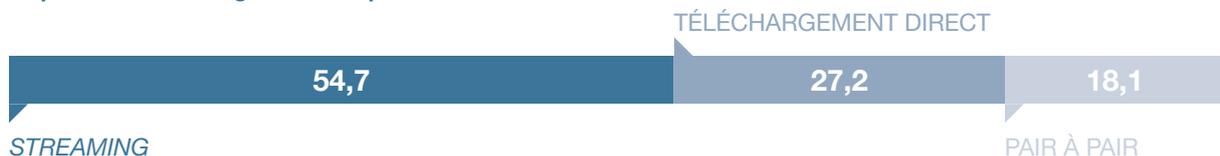
73,9 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

5 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

31 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



Au Brésil, si l'offre légale est abondante (au moins 80 plateformes proposent légalement des contenus audiovisuels^[4] et plus de la moitié des écoutes de musique se font *via* des services de *streaming* légaux^[5]), le piratage reste une pratique répandue, et notamment le pair à pair^[6].

La lutte contre le piratage est mise en œuvre *via* plusieurs instances réunissant des acteurs publics et privés, dont notamment le Conseil national de lutte contre le piratage et les crimes contre la propriété intellectuelle (CNCP). Cet organisme rattaché au ministère de la Justice et créé par décret en 2004 est très actif dans la lutte contre le piratage depuis 2017.

Siègent au CNCP plusieurs industries du secteur : il s'agit tant des secteurs touchés par le piratage (secteur audiovisuel, logiciels, jeux vidéo, sport) que de secteurs touchés par la contrefaçon de droits de propriété industrielle (mode, médicaments, etc.). Seize représentants du secteur

public sont membres du CNCP, dont notamment l'homologue brésilien du Centre national du cinéma, l'ANCINE – qui a parallèlement créé un groupe de travail dédié à la lutte contre le piratage ; le régulateur des télécommunications, l'ANATEL ; l'Institut national de la propriété industrielle ; un représentant du Parlement, de la police fédérale, etc.

Les missions du CNCP sont diverses : faire des propositions de modification de la législation ; réaliser des études ; initier des actions de promotion de l'offre légale et des campagnes de sensibilisation ; promouvoir la coordination de leurs actions avec différents acteurs tels que les services des impôts, la police, etc.

Il faut en outre relever qu'entre juin et septembre 2019, le Secrétariat aux droits d'auteur et à la propriété intellectuelle (SDAPI) a tenu une consultation publique pour réformer la loi locale sur le droit d'auteur.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] <https://videomind.com/ott-opportunity-in-brazil-grows-as-do-woes-for-pay-tv/>

[5] <https://www.pro-music.org/legal-music-services-latin-america.php>

[6] TruOptik Data Corp., "Digital Unmonetized Demand and Peer-to-Peer File Sharing Report: 2014 Review".

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES SERVICES ILLICITES ET LEURS OPÉRATEURS

Les autorités brésiliennes ont initié différentes actions répressives en 2019. Dès janvier 2019, l'opération policière dénommée « *Operation Copyright* » a permis la fermeture de services illicites notoires, qui attiraient 104 millions de visites annuelles.

En novembre 2019, le CNCP et le *Secretaria de Operações Integradas* ont coordonné l'Opération 404, qui s'est notamment soldée par la fermeture de 210 sites et 100 applications illicites dans 12 des différents États du Brésil. Les démantèlements réalisés dans le cadre de cette opération sont les plus importants de ce type jamais réalisés au Brésil et les premiers à inclure un soutien opérationnel direct de juridictions étrangères.

LES MESURES DE BLOCAGE

S'il n'y a pas de procédure spécifique permettant d'obtenir en justice le blocage des sites contrefaisants, des titulaires de droits ont obtenu des injonctions de blocage. Les fournisseurs d'accès à internet brésiliens seraient généralement coopératifs, dès lors qu'il y a une décision judiciaire, car beaucoup d'entre eux sont également des distributeurs de télévision payante. Dans ce contexte, l'ANCINE et le régulateur des télécommunications, l'ANATEL, discutent actuellement de la possibilité de créer un dispositif de blocage administratif.

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

En décembre 2019, le CNCP a signé un protocole d'accord avec les principaux acteurs de la publicité au Brésil pour mettre en place un mécanisme de conformité pour empêcher la publicité sur les sites illicites. Dans la suite de ces accords, le Brésil a également signé un accord avec le Royaume-Uni et les États-Unis. Le Brésil est en outre un des premiers pays à avoir adhéré au dispositif « *WIPO ALERT* » de l'OMPI destiné à mettre en œuvre l'approche « *Follow the money* » au niveau international.

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

37,7 POPULATION^[1]
en millions

92,7 % TAUX DE PÉNÉTRATION
INTERNET (2017)^[2]

USAGES ILLICITES^[3]

3 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

86 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



Selon une étude de 2018^[4], l'utilisation de logiciels de pair à pair de type BitTorrent a fortement diminué ces dernières années, passant de 15,1 % en 2014 à 1,6 % en 2017. En revanche, 9,7 % des foyers canadiens disposeraient d'un boîtier configuré avec un logiciel de type Kodi et 70,9 % de ces détenteurs l'utilisent à des fins de piratage.

La loi canadienne sur le droit d'auteur prévoit depuis 2012 à la fois des actions spécifiques à l'égard des internautes et des actions impliquant les intermédiaires dans la lutte contre le piratage. Des réflexions ont également été conduites pour responsabiliser les plateformes.

LES ACTIONS VISANT LES INTERNAUTES

LE DISPOSITIF PÉDAGOGIQUE
D'AVERTISSEMENT ET LES MISES
EN DEMEURE INDEMNITAIRES

Le Canada a adopté un dispositif d'avertissement dit d'« Avis et Avis » dans le cadre de la loi sur la modernisation du droit d'auteur entrée en vigueur depuis le 2 janvier 2015.

Cette loi est venue encadrer un dispositif d'autorégulation mis en œuvre par des fournisseurs d'accès à internet canadiens et les ayants droit de l'audiovisuel dans le cadre d'un accord volontaire depuis une dizaine d'années.

La loi prévoit l'obligation pour les fournisseurs d'accès à internet canadiens et pour les hébergeurs de faire suivre à leurs frais l'avertissement de l'ayant droit (dit « avis ») à l'internaute par courrier électronique.

Les avis contiennent notamment le nom et l'adresse du demandeur, l'œuvre piratée et les droits du demandeur sur cette œuvre, l'infraction alléguée, la date et l'heure de l'acte de contrefaçon. Dans l'esprit de la loi, le dispositif semble avoir une finalité uniquement pédagogique dès lors qu'aucune sanction pour l'internaute n'y est directement intégrée.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] « Video piracy in Canada » Sandvine Global Internet Phenomena Spotlight, mars 2018.

En cas de non-transmission, l'intermédiaire technique doit en exposer les raisons à l'ayant droit. Cette carence est passible d'une amende infligée par le juge qui peut aller de 5 000 à 10 000 dollars canadiens (soit environ 3 600 à 7 300 euros). Malgré cette sanction, tous les fournisseurs d'accès à internet ne respecteraient pas leur obligation de transmission ou limiteraient le nombre d'avis envoyés.

Les ayants droit peuvent agir contre les internautes qui partagent des œuvres sur les réseaux pair à pair sur le fondement de la contrefaçon. La sanction maximale encourue par les internautes pour contrefaçon non commerciale est une amende qui ne peut excéder 5 000 dollars canadiens (soit environ 3 654 euros).

Le dispositif a pu être détourné de sa finalité initiale par des ayants droit qui l'ont utilisé pour demander aux fournisseurs d'accès internet de transmettre des demandes indemnitaires aux internautes. C'est pour cela que le *Copyright Act* canadien a été amendé en décembre 2018, et prohibe désormais l'insertion de demandes indemnitaires dans les avis transmis aux internautes^[5]. Cet amendement ne prévoit toutefois

aucune sanction pour les ayants droit qui continueraient à insérer des demandes indemnitaires.

En juin 2019, le *Standing Committee on Industry, Science and Technology*, une commission de la chambre des communes, a publié son rapport sur la loi sur le droit d'auteur canadienne^[6]. S'agissant du dispositif d'avis, face aux plaintes des fournisseurs d'accès à internet concernant le fait que la mise en œuvre du dispositif nécessite des ressources importantes car il n'existe pas de format d'avis standard, le Comité recommande la standardisation du format des avis afin de permettre l'automatisation des envois.

S'agissant de la question des frais supportés par les fournisseurs d'accès à internet, en septembre 2018^[7], la Cour suprême canadienne a posé le principe que les fournisseurs d'accès à internet devaient obtenir une compensation par les ayants droit pour la fourniture de l'identité des internautes en vue des actions qu'ils étaient susceptibles d'intenter contre eux au pénal. La Cour a renvoyé aux juges du fond le soin de fixer le montant de cette compensation.

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES SITES ILLICITES ET LEURS OPÉRATEURS

UNE INCRIMINATION DÉDIÉE CONTRE LES ADMINISTRATEURS DES SERVICES MASSIVEMENT CONTREFAISANTS

La loi canadienne de modernisation du droit d'auteur de 2012 a instauré un régime de sanction pour ceux qui faciliteraient les actes de contrefaçon. Il est ainsi prévu que « *constitue une violation du droit d'auteur le fait pour une personne de fournir un service sur internet ou tout autre réseau numérique principalement en vue de faciliter l'accomplissement d'actes qui constituent une violation du droit d'auteur, si une autre personne commet une telle violation sur internet ou tout autre réseau numérique en utilisant ce service* ».

La loi ajoute que le tribunal peut prendre en compte différents éléments d'analyse tels que :

- le fait que le responsable du service utilise comme argument de promotion le caractère contrefaisant du site ;
- la connaissance par le responsable du site du fait que son service était utilisé pour faciliter la contrefaçon ;
- le fait que le service est significativement utilisé à d'autres fins que pour commettre des contrefaçons ;
- les mesures prises pour limiter la contrefaçon ;
- les avantages retirés des contrefaçons ou la viabilité économique de la fourniture du service si celui-ci n'était pas utilisé pour commettre des contrefaçons.

[5] <https://www.parl.ca/DocumentViewer/en/42-1/bill/C-86/royal-assent>

[6] <https://www.ourcommons.ca/DocumentViewer/en/42-1/INDU/report-16/page-285>

[7] <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/17254/index.do>

Les peines encourues par les responsables des sites massivement contrefaisants et les dommages-intérêts dus relèvent, depuis la loi de 2012, des infractions de contrefaçon à des fins commerciales, lesquelles font encourir des peines plus sévères et impliquent une réparation plus importante pour les ayants droit.

En octobre 2015, sur ce fondement, la cour fédérale du Canada^[8] a émis une injonction contre les développeurs canadiens du logiciel *PopcornTime* de désactiver les noms de domaine permettant de télécharger la version la plus populaire de l'application. Ce fondement a également été utilisé avec succès en 2015 et en 2016 tant par l'industrie audiovisuelle que musicale pour obtenir la fermeture de sites de liens *torrent*.

LES ACTIONS PÉNALES CONTRE LES VENDEURS DE BOÎTIERS FACILITANT LE PIRATAGE

La vente de boîtiers dotés de modules permettant notamment de visionner illégalement des programmes télévisés non accessibles sans abonnement connaît une expansion importante. Dans le cadre d'un jugement partiel, des ayants droit ont obtenu de la cour fédérale les premières injonctions de cesser leurs activités à l'encontre de vendeurs (62) de ces boîtiers en juin 2016.

L'injonction était motivée par le fait que ces terminaux réalisent des communications au public non autorisées et que les vendeurs de tels boîtiers ne sont pas des simples intermédiaires neutres mais incitent au contraire leurs clients à se détourner des moyens légaux de consommer des contenus protégés^[9]. Ces actions ont incité des vendeurs de boîtiers à cesser leurs activités volontairement en transigeant avec les ayants droit.

En juin 2017, une action a été introduite auprès de la Cour fédérale par des ayants droit de l'audiovisuel contre l'opérateur d'un site (« *TV Addons* ») distribuant des modules permettant de configurer le logiciel Kodi à des fins de piraterie. Celui-ci est accusé d'avoir porté atteinte au droit d'auteur en communiquant illicitement des dizaines de programmes télévisés, en développant,

hébergeant, distribuant et promouvant des extensions illicites. La procédure a débuté favorablement pour les ayants droit et a permis le transfert des différents noms de domaine et comptes sur les réseaux sociaux utilisés par « *TV Addons* » au cabinet d'avocat en charge du contentieux. Un mandat de recherche au civil a de plus accordé aux plaignants l'autorisation de pénétrer dans les locaux du défendeur afin de conserver et de copier les preuves à l'appui de leur cause, avant que celles-ci ne puissent être détruites ou falsifiées. Dans les derniers développements de la procédure, le juge a considéré que le défendeur communiquait lui-même des œuvres au public et qu'il ne pouvait pas valablement invoquer être un simple hébergeur alors que le site cible clairement les internautes qui veulent s'épargner les coûts d'un abonnement légal à un service de télévision.

Une action judiciaire engagée par l'ACE a conduit à la fermeture de *Vader Streams*, l'un des services d'abonnement IPTV les plus populaires du pays, ainsi que sa condamnation au paiement de la somme de 10 millions de dollars (un peu moins de 9 millions d'euros) selon une injonction permanente de la Cour fédérale du Canada du 21 août 2019.

LES MESURES DE BLOCAGE

Le droit positif canadien ne comporte pas de disposition permettant aux ayants droit d'obtenir le blocage des sites contrefaisants. Plusieurs initiatives visent cependant à introduire cette possibilité dans le corpus législatif.

En janvier 2018, des ayants droit et des fournisseurs d'accès à internet regroupés dans une entité appelée *FairPlay Canada*^[10] ont saisi le régulateur des télécommunications, *Canadian Radio-television and Telecommunications Commission* (CRTC), en janvier 2018 afin de militer pour obtenir la création d'un dispositif permettant le blocage des sites contrefaisants sous le contrôle du régulateur. Le CRTC a alors lancé une consultation sur ce projet au terme de laquelle il a décidé de rejeter^[11] cette demande.

[8] *Federal court, Ottawa, Ontario, 16 octobre 2015, Paramount Pictures Corporation & Ors v/ David Lemarier & Ors* <https://fr.scribd.com/document/288405925/Injunction>

[9] *ell Canada et al v. 1326030 Ontario Inc. dba ITVBox.net et al, T-759-16 (2016 FC 612)*.

[10] *Bell, Cineplex, Directors Guild Of Canada, Maple Leaf Sports and Entertainment, Movie Theatre Association of Canada, Regoers Media*.

[11] <https://crtc.gc.ca/eng/archive/2019/2019-342.htm>

En juillet 2019, des ayants droit, également membres du groupement *FairPlay Canada* (et ayant en outre des activités de fournisseur d'accès à internet) ont demandé en justice le blocage de noms de domaine et d'adresses IP d'un service illicite d'IPTV pour une durée de deux ans. Cette demande a été accueillie favorablement par la cour fédérale, malgré l'absence de fondement législatif, qui a ordonné pour la première fois au Canada le blocage du site par les 12 principaux fournisseurs d'accès à internet le 15 novembre 2019^[12]. Le juge a fondé sa décision sur la jurisprudence développée par le Royaume-Uni en matière de blocage de sites. En cas de réapparition de sites dits miroirs, les parties pourront revenir devant le juge avec une nouvelle liste de noms de domaine et/ou d'adresses IP. Les fournisseurs d'accès à internet pourront alors s'opposer à l'actualisation de la mesure de blocage mais, en l'absence de contestation dans les dix jours, la cour pourra enjoindre à l'actualisation des mesures de blocage. Les ayants droit sont tenus de payer les coûts marginaux raisonnables de mise en œuvre des mesures de blocage, sur envoi de factures par les fournisseurs d'accès. Un des fournisseurs d'accès canadien, TekSavvy, a interjeté appel de la décision^[13].

Dans le rapport précité sur la loi sur le droit d'auteur du *Standing Committee on Industry, Science and Technology*, le comité indique que la lutte contre le piratage devrait se concentrer davantage sur la contrefaçon commerciale que sur les particuliers. Le comité se montre également sensible au besoin des ayants droit de pouvoir obtenir des mesures de blocage. À cette fin, il est suggéré que la loi sur les télécommunications puisse être révisée afin de rationaliser le processus de blocage. La commission s'oppose cependant à la mise en œuvre d'une procédure de blocage qui n'accorderait pas une place centrale au juge.

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

Le gouvernement canadien a publié en novembre 2016 un rapport examinant la possibilité et l'opportunité de mettre en œuvre l'approche dite « *Follow the money* ». Cette analyse, qui s'inspire des différents rapports et modèles étrangers, indique que cette approche peut participer à la lutte contre la contrefaçon commerciale même si elle ne peut pas, à elle seule, l'éradiquer. Afin de sécuriser le dispositif, le rapport préconise que le gouvernement intervienne pour caractériser les sites.

Il est également recommandé que le gouvernement augmente en parallèle ses efforts pour sensibiliser le public aux risques sociétaux et financiers inhérents à l'utilisation de sites massivement contrefaisants car ces efforts auraient eu un effet positif à l'étranger. Le rapport souligne ainsi la possibilité de faire une campagne de sensibilisation de la population en axant la communication sur les risques encourus par les utilisateurs.

Enfin, le rapport préconise un examen du rôle des hébergeurs et des différents intermédiaires techniques de l'internet car ces services peuvent contribuer à protéger l'identité des opérateurs des sites massivement contrefaisants.

Ce rapport n'a à ce jour pas donné lieu à une mise en œuvre concrète.

LES ACTIONS VISANT À RESPONSABILISER LES PLATEFORMES DE PARTAGE DE CONTENUS

Dans le rapport précité sur la loi sur le droit d'auteur du *Standing Committee on Industry, Science and Technology*, le comité reconnaît le problème du « *value gap* » pour les détenteurs de droits, il souligne que les droits des utilisateurs d'internet devraient également être pris en compte et souhaite qu'une approche équilibrée soit mise en œuvre. Le comité ne fait pas de proposition concrète à cet égard mais propose de suivre attentivement les développements européens. Il est ainsi préconisé que

le gouvernement du Canada surveille la mise en œuvre, dans d'autres juridictions, de l'octroi de licences collectives étendues ainsi que de la législation conditionnant le bénéfice du régime de responsabilité limitée des plateformes aux mesures prises par ces acteurs contre la violation du droit d'auteur. Dans le même sens, le gouvernement est invité à assurer que les systèmes de gestion des contenus utilisés par les plateformes respectent les droits tant des titulaires de droits que des usagers.

[12] Cour Fédérale, Ottawa, Ontario, 15 novembre 2019, the Honourable Mrs Justice Gleeson, 2019 FC, 1432, <https://decisions.fct-cf.gc.ca/fc-cf/decisions/en/item/424753/index.do>

[13] <https://torrentfreak.com/images/2020.03.12-Factum-of-the-Appellant.pdf>

CHINE

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

1 439,3 POPULATION^[1]
en millions

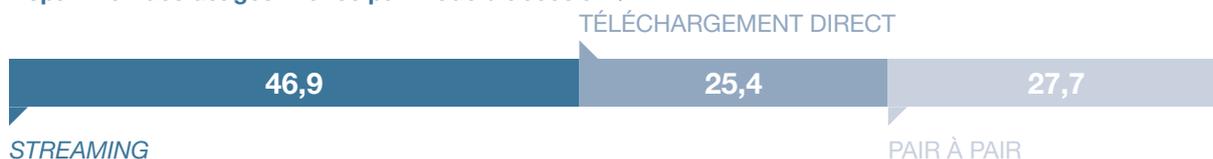
64,6 % TAUX DE PÉNÉTRATION
INTERNET^[2]

USAGES ILLICITES^[3]

6,8 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

7 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



Compte tenu de sa population, le marché chinois constitue un enjeu financier important pour le marché de l'offre légale : la Chine est le quatrième marché de la musique en *streaming* en termes de revenus^[4]. Cependant, le marché des applications qui facilitent le piratage des contenus musicaux y est très développé et le pays est par ailleurs pointé du doigt par les autorités américaines comme étant la place centrale de la production des boîtiers préconfigurés pour le piratage des contenus audiovisuels et sportifs^[5].

Dans ce contexte, une amélioration du dispositif de lutte pourrait être mise en œuvre, comme cela a été annoncé en novembre 2019 par le Comité central du Parti communiste chinois et le Conseil d'État dans des lignes directrices sur le renforcement de la protection des droits de propriété intellectuelle.

Ces lignes directrices prévoient que des mesures seront prises d'ici 2022 et que l'ensemble du système de protection des droits de propriété intellectuelle sera amélioré en 2025. Il faut relever qu'une nouvelle loi sur le commerce électronique a été adoptée en 2018 mais que les dispositions relatives aux procédures de notification et de retrait seraient peu claires.

En l'état, le dispositif public de lutte contre le piratage en Chine semble essentiellement mis en œuvre *via* des actions administratives menées par l'Administration nationale du droit d'auteur de Chine (NCAC) en lien avec les ayants droit, la police et les juridictions.

La NCAC, créée en 1985, a plusieurs missions, dont celle d'office d'enregistrement des droits de propriété intellectuelle, ainsi que notamment :

- participer à l'élaboration des lois, règlements et règles en matière de droit d'auteur, élaborer des politiques et mesures administratives en matière de droit d'auteur et organiser leur mise en œuvre ;
- élaborer la stratégie nationale du droit d'auteur ;
- organiser les enquêtes et traiter les cas importants de violation du droit d'auteur.

La NCAC peut également, en coopération avec les titulaires de droits, prendre des mesures administratives à l'encontre des services illicites ou des services qui facilitent le piratage.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] <https://www.iipa.org/files/uploads/2020/02/2020SPEC301CHINA.pdf>

[5] https://ustr.gov/sites/default/files/2019_Special_301_Report.pdf

La NCAC mène depuis 14 ans, avec d'autres entités, une campagne annuelle de protection des droits intitulée « *Sword Net* », qui se focalise à chaque édition sur une action ou un mode de piratage donné. C'est par exemple dans ce cadre qu'en 2015 la NCAC a exigé que les fournisseurs de services de stockage en ligne prennent des mesures proactives pour empêcher les utilisateurs de télécharger du contenu portant atteinte au droit d'auteur. En 2019, de mai à novembre, le NCAC et d'autres administrations ont lancé conjointement la quinzième édition de cette campagne, qui s'est concentrée sur la lutte contre le piratage des films au moment de leur sortie en salles et la lutte contre l'accès non autorisé aux services de *streaming* vidéo. Elle a permis la suppression d'1,1 million de liens et initié des investigations dans 450 affaires dont 160 ont donné lieu à des poursuites pénales.

Au niveau judiciaire, les autorités chinoises ont par ailleurs initié en 2015 des expérimentations visant à mettre en place des chambres spécialisées dans les litiges relatifs à internet.

La haute cour de la province de Zhejiang a ainsi instauré une chambre dédiée au commerce électronique, qui entendait notamment les affaires de droit d'auteur sur internet. Depuis, grâce au succès de cette expérimentation, deux tribunaux spécialisés ont été créés, lesquels statuent chacun sur plus de 700 dossiers par an.

En outre, le 1^{er} janvier 2019 a été marqué par la création d'une nouvelle cour d'appel dédiée à la propriété intellectuelle au sein de la Cour suprême. Cette juridiction spécialisée entend les appels interjetés contre les décisions des tribunaux sur des sujets de propriété intellectuelle présentant une certaine complexité technique.

La Chine a en outre créé une cellule pénale dédiée au sein du Département des enquêtes sur les délits alimentaires et drogues, chargée, entre autres, d'enquêter et de poursuivre tous les cas d'atteintes aux droits de propriété intellectuelle.

CORÉE DU SUD

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

51,3 POPULATION^[1]
en millions

96,2 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

2,1 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

43 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



Depuis 2009, la Corée du Sud s'est dotée d'un dispositif très complet de lutte contre la contrefaçon, mis en œuvre par différents organismes tous en lien avec le ministère de la Culture, du Sport et du Tourisme^[4]. Depuis septembre 2016, c'est la *Korea Copyright Protection Agency* (KCOPA) qui est essentiellement chargée de mettre en œuvre les mesures de lutte contre la contrefaçon de droits d'auteur sur internet.

Ce dispositif inclut un volet qualifié de « réponse graduée » qui cible à la fois les plateformes qui permettent le téléchargement illégal et les internautes qui téléchargent tant sur ces plateformes que via les réseaux pair à pair. S'y ajoutent des actions de sensibilisation et de promotion de l'offre légale. Des mesures sont par ailleurs mises en œuvre contre les sites massivement contrefaisants.

LES ACTIONS VISANT LES INTERNAUTES

LE DISPOSITIF D'AVERTISSEMENT DES INTERNAUTES

Depuis 2009, la loi coréenne prévoit un dispositif dit de « réponse graduée » qui permet d'adresser, via les plateformes, des notifications aux internautes qui partagent du contenu sur ces plateformes.

Après vérification des éléments matériels du dossier par la KCOPA, le ministère de la Culture, du Sport et du Tourisme peut prononcer des recommandations, voire des injonctions en cas de refus d'obtempérer, à la plateforme pour qu'elle transmette un avertissement à l'internaute qui a mis à disposition le contenu litigieux, en indiquant à l'internaute qu'en cas de réitération, son compte sur la plateforme pourra être suspendu pour une

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] Jusqu'en 2016, la lutte contre la contrefaçon était mise en œuvre par plusieurs intervenants :

- le ministère de la Culture, du Sport et du Tourisme et la Korea Copyright Commission (KCC), qui dépend du ministère. Ils s'occupent essentiellement du dispositif dit de réponse graduée ;

- le Copyright Protection Center, organisme créé par le secteur privé auquel le ministère délègue des activités de lutte contre la contrefaçon, et plus particulièrement la lutte contre les sites massivement contrefaisants.

Une loi de 2016 a créé la Korea Copyright Protection Agency qui a absorbé le Copyright Protection Center et met en œuvre les missions de la KCC en lien avec la lutte contre le piratage.

durée limitée. Cette procédure vise également les *bulletin boards*, qui sont vraisemblablement des blogs et des forums, sous réserve qu'ils aient un but lucratif. Ceux-ci peuvent être destinataires de notifications transmises par leur hébergeur.

Au terme de la procédure, l'internaute risque que son compte sur la plateforme soit supprimé pour une durée maximale de six mois. Les plateformes qui exécutent les injonctions du ministère doivent en rendre compte dans un délai de dix jours. Une plateforme qui n'exécuterait pas les injonctions du ministère encourt une amende (7 300 euros environ). En pratique, aucune injonction n'a été émise depuis 2012, car les plateformes locales coopèrent efficacement. Face à l'évolution du piratage, la KCOPA souhaiterait aujourd'hui réduire les délais de réponse octroyés aux plateformes, aujourd'hui fixés à cinq jours, mais également négocier avec certaines plateformes pour que celles-ci retirent les contenus illicites sous 24 heures.

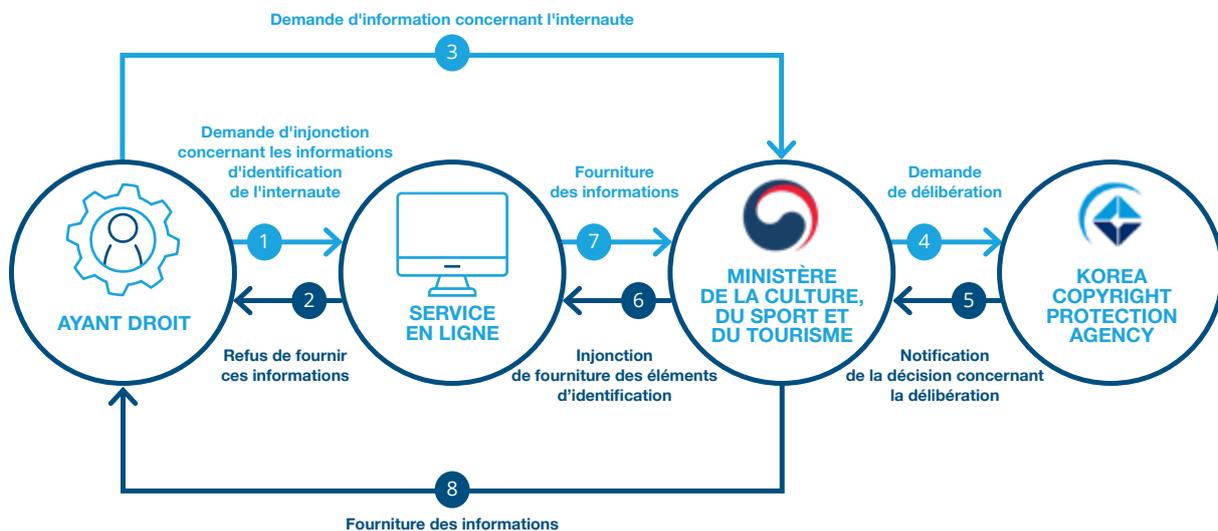
Le dispositif coréen diffère des autres dispositifs pédagogiques étrangers, notamment parce que :

- il ne vise pas spécifiquement le pair à pair ;
- la KCOPA est saisie par les ayants droit mais elle peut également être saisie par les internautes lorsque ceux-ci constatent une mise à disposition litigieuse de fichiers. Les signalements des internautes sont réalisés *via* un formulaire sur un site dédié (COPY 112), avec notamment une copie d'écran. Les internautes sont sensibilisés à la détection de contenus illicites et même incités à y participer. Ainsi, lorsqu'ils donnent leurs identifiants pour permettre les constats sur des plateformes à accès restreint, ils sont récompensés, notamment par des bons d'achat.

Des critiques ont été émises contre ce système qui relève uniquement de décisions administratives sans recours possible devant le juge.

Dans le cadre de ce dispositif, un ayant droit peut en outre demander à la KCOPA et au ministère de la Culture, du Sport et du Tourisme de lui permettre d'obtenir les informations permettant d'identifier un internaute qui a partagé illicitement des contenus protégés.

REQUEST FOR INFORMATION PROVISION OF THE PIRATES EN TRANSMITTERS (article 103 3 of copyright law)
 Deliberation on information provision of the pirates en transmitters
 Procedures of Request for Information Provision of the pirates and transmitters (article 103 3 of copyright law)



Source : KCOPA

LA PROMOTION DE L'OFFRE LÉGALE

La Corée du Sud est très active sur le volet de la pédagogie et mets en œuvre de nombreuses actions et campagnes de sensibilisation au droit d'auteur, notamment à destination des jeunes.

En 2012 a été lancée l'initiative « *Copyright OK* », système de certification de la légalité des plateformes mettant à disposition des contenus culturels, adminis-

tré par la KCOPA. Le processus de certification mis en œuvre implique de vérifier que la plateforme assure la protection du droit d'auteur. Pour ce faire, elle doit notamment permettre la notification des contenus illicites, consacrer un espace à la promotion de la légalité des contenus, mettre en œuvre une politique spécifique vis-à-vis des internautes récidivistes ou encore déployer des ressources ou lutter contre la contrefaçon. Les plateformes certifiées peuvent faire figurer le logo sur leur site. Celui-ci est octroyé pour une durée de deux ans.

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

En parallèle du dispositif de réponse graduée détaillé ci-avant, lequel implique largement les plateformes, la KCOPA met en œuvre le programme *Illegal Copyrights Obstruction Program* (ICOP) qui permet une surveillance continue des sites (*cyberlockers*, sites de liens pair à pair, plateformes UGC, blogs...) et un envoi aux plateformes de demandes de suppression des contenus (*Notice and Take down*). Il s'agit donc ici d'obtenir la coopération des plateformes plutôt que celle des fournisseurs d'accès à internet.

Les informations recueillies par le système ICOP sont transmises à la Commission de délibération et de protection des droits d'auteur, qui émet des notifications et demandes de retrait.

En outre, les résultats d'ICOP sont téléversés sur le système de réponse globale en cas d'infraction au droit d'auteur de la KCOPA. Ce système de lutte contre la contrefaçon fonctionne en temps réel 24 heures sur 24 et 7 jours sur 7 afin de garantir une action rapide et adéquate contre les atteintes au droit d'auteur. Le système fonctionne comme suit :

- suivi du cycle de vie des sites portant atteinte au droit d'auteur (création › en fonctionnement › changement › fermeture) ;
- vérifications réalisées *via* une base de données des œuvres protégées par le droit d'auteur (titre de l'œuvre, propriétaire, licencié, autres informations, etc.) ;
- utilisation des diverses informations recueillies sur les infractions *via* le *Big Data* pour en tirer des analyses et des prévisions ;

- fourniture des informations statistiques en temps réel ;
- fourniture d'une fonction de notification des infractions en cas d'urgence, de contenu particulièrement touché par le piratage du fait de son actualité (*Killer Content Early Warning System*) ;
- fourniture des informations demandées par les procureurs, la police, les titulaires de droits.

Le régulateur des télécommunications, la *Korea Communications Standards Commission* (KCSC), peut par ailleurs mettre en œuvre un dispositif de blocage administratif des sites qui vise essentiellement les sites étrangers. En cas d'infraction, un site peut être bloqué sur demande des ayants droit. Les sites en lien avec les sites bloqués font ensuite l'objet d'un suivi par la KCSC et la KCOPA. La KCOPA demande, lorsque cela est nécessaire, à la KCSC de mettre en œuvre la procédure de blocage à leur encontre. Depuis 2019, il faut relever que la KCSC a cessé d'exiger que plus de 70 % des contenus du site à bloquer soient mis à disposition illicitement.

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

Dans le cadre d'un programme intitulé « *Profit Source Research* », la KCOPA surveille la publicité pour des marques connues sur les sites portant atteinte au droit d'auteur et collabore avec les annonceurs (ou avec leurs agences de publicité) pour éviter que ces publicités réapparaissent.

La Corée du Sud est en outre un des premiers pays à avoir adhéré au dispositif « *Follow the money* » mis en place par l'OMPI.

La KCOPA a enfin chargé une université de conduire une étude sur la publicité sur les sites contrefaisants en 2019. Cette étude a montré que des produits et services licites aussi bien qu'illicites, connectés à de grandes marques et à des marques moins connues, font l'objet de publicité sur des sites portant atteinte au droit d'auteur. Il apparaît que si les acteurs de la publicité sont conscients de l'impact négatif de leur présence sur des sites portant atteinte au droit d'auteur, rares sont cependant ceux qui sont au courant de cet état de fait. Il est donc préconisé de faire connaître les résultats de l'étude afin d'inciter les acteurs de la publicité à agir sur une base volontaire^[5].

[5] https://www.wipo.int/wipo_magazine/en/2019/03/article_0004.html

DANEMARK

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

5,8 POPULATION^[1]
en millions

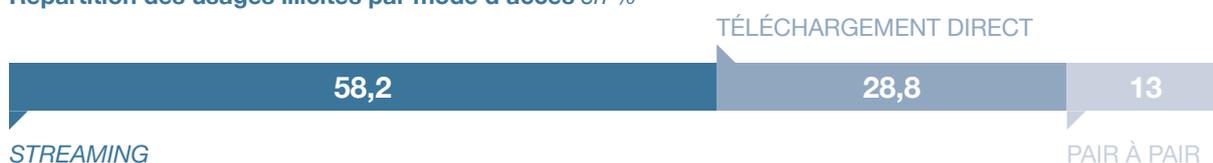
96,55 % TAUX DE PÉNÉTRATION
INTERNET^[2]

USAGES ILLICITES^[3]

0,45 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

80 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illicites par mode d'accès en %



Au Danemark, les ayants droit des différents secteurs se sont organisés en créant une entité dédiée à la lutte contre le piratage (*RettighedsAlliancen*), financée par ses membres.

Cette entité est notamment parvenue d'une part à conclure un accord facilitant le blocage avec les fournisseurs d'accès à internet, couplée à une initiative de promotion de l'offre légale, et d'autre part à mettre en œuvre une approche dite « *Follow the money* ».

LES ACTIONS VISANT LES INTERNAUTES

LE DISPOSITIF D'AVERTISSEMENT DES INTERNAUTES

Au Danemark, le gouvernement a songé en 2011 à faire passer une loi pour mettre en place un dispositif de type « réponse graduée ». Les fournisseurs d'accès à internet se sont très fortement opposés à un tel dispositif, qu'ils estiment coûteux et dommageable à leur relation avec leur clientèle. Le projet a donc été abandonné et la priorité du dispositif de lutte a été axée sur le blocage.

LE DISPOSITIF DE MISE EN DEMEURE INDEMNITAIRE

Certains ayants droit tentent de mettre en place au Danemark un dispositif indemnitaire en demandant aux fournisseurs d'accès à internet d'identifier les titulaires d'adresses IP. Cependant, une cour d'appel a rendu une décision le 7 mai 2018 dans laquelle elle a refusé de contraindre les fournisseurs d'accès à internet à transmettre l'identité des internautes qui partagent illégalement des contenus culturels sur internet, au regard de la gravité du délit en cause et de la nécessité de protéger les données personnelles des utilisateurs.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

En 2018, l'administrateur du site « *popcornTime.dk* » a été condamné en première instance à six mois de prison avec sursis. Le site en question ne communiquait pas d'œuvres au public mais diffusait des informations sur le téléchargement, l'installation et l'utilisation du service illicite de *streaming Popcorn Time*. Cette condamnation a été confirmée par la Cour suprême début 2020.

LA PROMOTION DE L'OFFRE LÉGALE

Jusqu'à récemment, l'action des pouvoirs publics danois se concentrait en premier lieu sur la sensibilisation. Dans le cadre d'une initiative globale intitulée « *Share with care* », des campagnes de sensibilisation à l'offre légale prévoyant la diffusion de messages sur des plateformes populaires telles que YouTube et Facebook ont ainsi été menées. Ces campagnes sont financées conjointement par les fournisseurs d'accès à internet et les titulaires de droits, avec le soutien du ministère de la Culture. La campagne « *Share with care* » a ensuite donné lieu à la création d'un portail de l'offre légale^[4], qui référence les différentes plateformes, vers lequel renvoient les messages diffusés par les fournisseurs d'accès à internet lorsqu'un internaute essaie d'accéder à un site bloqué.

RettighedsAlliancen, le ministère de la Culture et les fournisseurs d'accès à internet ont ensuite mis en œuvre la campagne « *Share with Care 2* » qui s'est traduite par la création d'un moteur de recherche de l'offre légale, « *FilmFinder*^[5] » (aujourd'hui limité aux œuvres audiovisuelles). Depuis fin 2018, les fournisseurs d'accès à internet accompagnent ainsi également les mesures de blocage d'un renvoi vers ce moteur de recherche.

Par ailleurs :

- en 2016 et 2017, une campagne intitulée « *We Film Lovers* », centrée sur les conséquences du *streaming* illicite, a été diffusée. Cette campagne avait plus particulièrement vocation à répondre à la hausse du *streaming* illégal de contenus audiovisuels, en particulier chez les jeunes. La campagne, utilisant un ton humoristique, diffusée sur de nombreux canaux, a été bien accueillie par le public. Elle a donné lieu, en août 2017, à une nouvelle campagne de trois ans sur la contrefaçon de livres et notamment de manuels scolaires (*We knowledge lovers*). Cette campagne associe les ayants droit et les ministères de la Culture, de l'Éducation et de la Recherche et a également reçu un bon accueil de la part du public ;
- en relation avec un éditeur de matériels pédagogiques et une société spécialisée dans les sciences comportementales, les ayants droit ont développé un concept de sensibilisation des 12-16 ans (« *NudgeIP* ») financée^[6]. La campagne a été très bien reçue dans les écoles (7 000 téléchargements du programme). Le ministère a donc décidé de financer une nouvelle campagne pour les 9-12 ans ;
- enfin, les ayants droit ont également pu recourir à l'insertion de messages publicitaires sur les sites illégaux afin d'alerter les internautes des conséquences dommageables de leurs pratiques illicites.

[4] www.sharewithcare.dk/

[5] <https://filmfinder.dk/>

[6] <https://www.youtube.com/watch?v=n8Qty84B86g&t=29s>

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

Le ministère a mis en place en 2013 le *Dialogue Forum*, dont l'objet était de réunir les parties prenantes, afin d'engager des discussions dans le cadre de groupes de travail. En mai 2015, une déclaration d'intention a été signée, sous l'égide du ministère de la Culture (*Code of conduct to promote lawful behaviour on the Internet*), par des fournisseurs d'accès à internet, des acteurs de l'écosystème de la publicité en ligne, des services de paiement (notamment Mastercard), des titulaires de droits, des moteurs de recherche (Google, Microsoft) et divers professionnels (ex. IT-Branchen, association de professionnels de l'informatique, de l'internet et des télécommunications, Omnicom Media Group). À la suite de cet accord, différents groupes de travail ont été formés.

Deux accords ont été conclus à ce jour dans le cadre de ces discussions : un accord avec les fournisseurs d'accès à internet destiné à faciliter le blocage et un accord avec les acteurs de la publicité en ligne qui fonctionne sur la base d'une liste de services illicites.

LES MESURES JUDICIAIRES DE BLOCAGE

LA PROCÉDURE DEVANT LE JUGE

Devant le juge, les ayants droit doivent démontrer que le contenu disponible sur le site leur appartient et qu'ils n'ont pas directement ou indirectement consenti à sa mise à disposition. En principe, une infraction est suffisante mais les ayants droit se concentrent sur les sites qui fournissent un nombre substantiel d'œuvres contrefaisantes. Au Danemark, il n'y a pas de seuil prédéfini pour déterminer le caractère contrefaisant d'un site internet comme au Royaume-Uni.

Les procédures judiciaires de blocage durent deux à trois mois, soit trois à six mois avec la préparation du dossier. Elles peuvent concerner des dizaines de sites. Quatre à six procédures de blocage sont engagées chaque année par l'association locale de lutte contre le piratage, chacune visant entre vingt et trente sites.

Un accord conclu en 2014 entre les ayants droit et l'organisation représentant les fournisseurs d'accès à internet a permis la mise en œuvre du dispositif suivant : les ayants droit assignent un seul fournisseur d'accès à internet dans le cadre des procédures de blocage devant le juge (avec une rotation régulière) afin de réduire les frais de justice. Les injonctions de blocage sont ensuite signifiées à l'organisation représentant les fournisseurs d'accès à internet (*Telecom Industry Association Denmark*), qui les transmet aux autres fournisseurs d'accès. Ceux-ci se sont engagés à rendre les sites inaccessibles, par un blocage DNS, sous sept jours à compter de cette signification, sans avoir au préalable été attrait à la procédure. Chaque partie assume ses propres frais.

Le blocage mis en œuvre par les fournisseurs d'accès à internet est un blocage DNS.

L'ACTUALISATION DES MESURES DE BLOCAGE

L'accord de 2014 permet également, sans avoir à repasser devant le juge, un blocage facilité des sites miroirs par les fournisseurs d'accès à internet, sous réserve que les ayants droit aient pu rapporter des preuves suffisantes. En pratique, les ayants droit utilisent un logiciel fourni par un prestataire privé (également utilisé par la MPA), qui analyse les similitudes entre les services et leur permet d'identifier les services de contournement et effectuent en complément des vérifications manuelles. En toutes hypothèses, les ayants droit garantissent les fournisseurs d'accès à internet contre les éventuelles contestations des sites miroirs.

De plus, la jurisprudence récente a rendu des injonctions dynamiques de blocage permettant aux ayants droit de demander le blocage non plus seulement de sites identifiés par leur nom de domaine mais de sites identifiés par leur contenu ou leur nature même, leur interface, quelle que soit l'extension du nom de domaine^[7], validant ainsi *a posteriori* le code de conduite.

[7] <http://rettighedsalliancen.dk/2017/02/08/retsafgoerelse-styrker-blokeringerne-af-de-ulovlige-tjenester-2/>

Dans ce contexte, le code de 2014 a été amendé en 2020 pour faciliter et accélérer encore le blocage des sites de contournement. Ainsi, alors que les ayants droit devaient auparavant contacter l'opérateur du site miroir avant de demander son blocage, ceci n'est plus une obligation dans l'hypothèse où aucune adresse de contact ne figure sur le site. Les ayants droit continueront en contrepartie d'assumer tout risque lié à un éventuel surblocage.

L'accord a également été adapté pour permettre le blocage des noms de domaine locaux en « .dk » Ceux-ci étaient auparavant exclus du code car les titulaires de droits devaient en principe pouvoir obtenir leur désactivation par les bureaux d'enregistrement – mais il s'est avéré à l'usage qu'obtenir cette désactivation était un processus compliqué.

Une liste des sites bloqués au Danemark est publiée sur les sites de l'organisation des fournisseurs d'accès à internet mais cette liste est aujourd'hui très peu consultée par le grand public.

LES SERVICES VISÉS

Les mesures de blocage ordonnées au Danemark visent différents types de sites illicites et notamment :

- en 2018, le Danemark a été le premier pays d'Europe et l'un des premiers pays dans le monde à obtenir des mesures de blocage à l'encontre d'un site de *stream ripping* illicite. Le juge a estimé que « *Convert2mp3* » enfreignait le droit de communication au public et que les utilisateurs danois du site faisaient des copies illégales lorsqu'ils téléchargeaient des fichiers du site. Les fournisseurs d'accès à internet ont ainsi été enjoins de bloquer le site « *Convert2mp3.net* » en juillet 2018^[8] ;
- plus récemment, l'opérateur du site flux Yout.com s'est opposé à une ordonnance de blocage. Le tribunal danois a rejeté tous les arguments avancés par l'opérateur et a estimé que, par l'exploitation de son service, le site communiquait avec le public et que le site jouait un rôle indispensable en mettant les œuvres à la disposition d'un nouveau public^[9]. Le tribunal a également estimé que le fait que le site ne stockait aucune copie sur ses serveurs était sans importance, car le site fournissait un outil permettant aux utilisateurs d'accéder à des œuvres protégées par le droit d'auteur ;

- en juin 2019, *RettighedsAlliancen* a obtenu le blocage d'un agrégateur d'articles de presse reproduisant intégralement ces publications.

Il faut enfin relever qu'en décembre 2019, face aux contournements par les internautes des mesures de blocage mises en place par les fournisseurs d'accès à internet à la suite d'une injonction judiciaire, *RettighedsAlliancen* s'est rapprochée d'un des sites bloqués (« *OpenSubtitles* », un service illicite de sous-titres). Celle-ci a demandé aux opérateurs du site de mettre en œuvre des mesures de blocage géographique empêchant les adresses IP danoises d'accéder à son service. Les opérateurs ont indiqué s'être pliés volontairement à cette mesure car le site était déjà bloqué au Danemark.

LA LUTTE CONTRE LE PIRATAGE DE CONTENUS SPORTIFS

En matière de *streaming* illicite de programmes TV en direct, les ayants droit danois estiment qu'il est crucial d'intervenir avant que ces usages ne prennent davantage d'ampleur et que le grand public ne s'habitue à bénéficier de tels services pour un prix dérisoire. Le nombre de visiteurs vers des pages proposant des abonnements à des bouquets de chaînes illicites aurait augmenté de 84 % entre janvier et décembre 2017. En 2017, les visites vers les sites de *live streaming* illicites proposant des contenus sportifs aurait augmenté de 28 %. Dans ce contexte, des discussions sont en cours sur la possibilité de mettre en œuvre des blocages IP à l'encontre de ces services. En avril 2019, la ligue de football espagnole *La Liga*, en coopération avec *RettighedsAlliancen*, a obtenu en justice le blocage DNS dynamique de neuf services illicites de diffusion de rencontres sportives. Le juge a cependant reporté à plus tard le blocage d'un des sites, « *Rojadirecta* », car celui-ci a souhaité présenter des arguments en défense. Le blocage du service a cependant été accordé par le juge en septembre 2019.

[8] Cour de Frederiksberg, 4 juillet 2018, n° BS-8065/2018-FRB, [http://www.hadopi.info/dj/news/ressources/BRFRB%20Kendelse%2004.07.18%20Convert2mp3%20EN%20\(English%20Translation\).pdf](http://www.hadopi.info/dj/news/ressources/BRFRB%20Kendelse%2004.07.18%20Convert2mp3%20EN%20(English%20Translation).pdf)

[9] Cour de Hoalbeck, 12 mars 2020, n° BS-25268/2019-HBK, [http://www.hadopi.info/dj/news/ressources/Kendelse%20af%20Holbaek%20byret%2012.3.2020%20\(ENG\)%20-%20Yout.com.pdf](http://www.hadopi.info/dj/news/ressources/Kendelse%20af%20Holbaek%20byret%2012.3.2020%20(ENG)%20-%20Yout.com.pdf)

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

Les travaux conduits sous l'égide du ministère de la Culture, avec le secteur de la publicité en ligne, ont abouti en 2017 à l'initiative dite « AdCodex », dans le cadre de laquelle avaient vocation à collaborer les ayants droit et les acteurs de la publicité.

La liste noire du Codex a cependant été suspendue en mars 2018 en raison de questions soulevées par l'autorité locale en charge de la protection des données personnelles : celle-ci estimait que *RettigheidsAlliancen*, en tant qu'organisme du secteur privé, ne pouvait pas légalement maintenir une liste de sites illicites, dans la mesure où une telle liste devait être considérée comme contenant des données personnelles sensibles au regard de la loi danoise, lesquelles peuvent seulement être traitées par des autorités publiques.

Il a ainsi été convenu d'une part de confier au ministère de la Culture la gestion de la liste des sites et d'autres part d'inclure les annonceurs, les services de paiement,

etc. et d'ouvrir l'accord aux autres parties prenantes intéressées. Une communication sur la signature du Codex a été faite en octobre 2020^[10]. Celui-ci a été signé par des acteurs des médias danois, des agences de publicité et les acteurs du paiement en ligne.

La liste réalisée en vertu du Codex, confidentielle, ne comprend aujourd'hui que les services considérés comme illégaux dans le cadre d'une injonction judiciaire dynamique et comprendraient fin 2020 environ 350 URL. Le nombre de noms de domaine visés pourrait cependant être ultérieurement supérieur à celui communiqué aux fournisseurs d'accès à internet car seuls les noms de domaine les plus populaires et donc les plus nocifs font l'objet de mesures de blocage alors que l'ensemble des noms de domaine d'une galaxie, et non les seules « têtes d'affiche », pourraient à terme être inclus dans le dispositif « *Follow the money* ». *RettigheidsAlliancen* souhaiterait ainsi *in fine* pouvoir gérer la liste, probablement à l'issue d'une réforme législative. Davantage de sources pourraient également être incluses pour la constitution de la liste et notamment les données de la police de Londres (PIP CU) ou de la MPA.

[10] <https://rettighedsalliancen.com/Codex/>

ÉGYPTE

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

102,3 POPULATION^[1]
en millions

57,3 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

1,42 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

24 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illicites par mode d'accès en %



En Égypte, la lutte contre le piratage passe essentiellement par la voie judiciaire. Si une violation est constatée, une action pénale peut être engagée et des réparations réclamées au moyen d'une procédure civile.

Les peines encourues en cas de contrefaçon sont au minimum d'un mois de prison et une amende comprise entre 5 000 à 10 000 pounds égyptiens (278,6 à 557,2 euros). Le faible montant de l'amende est critiqué comme étant peu dissuasif.

Des juges spécialisés en propriété intellectuelle exercent par ailleurs en matière civile au sein de la cour spécialisée en économie.

Si des mesures de blocage de sites peuvent être prononcées en cas de menace pour la sécurité égyptienne, il n'existe pas à notre connaissance de mesures de blocage de site en cas de violation de la propriété intellectuelle.

Le piratage de chaînes de télévision par satellite est un phénomène important en Égypte. Irdeto, société néerlandaise spécialisée dans la sécurisation des contenus audiovisuels, s'est alliée à l'opérateur, *Multichoice Africa Limited*, pour agir à l'encontre d'un réseau qui piratait des signaux vidéo et vendait des décodeurs et abonnements illégaux qui ont permis à plus de 863 999 téléspectateurs de suivre les émissions d'un certain nombre d'opérateurs internationaux.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

ESPAGNE

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

46,8 POPULATION^[1]
en millions

90,7 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

2,5 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

58 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illicites par mode d'accès en %



Le dispositif espagnol de lutte contre la contrefaçon comporte, depuis 2011, un mécanisme de blocage des sites contrefaisants *via* une autorité publique.

Parallèlement, le gouvernement espagnol et les ayants droit mènent des campagnes de sensibi-

lisation et des mesures sont mises en œuvre afin d'améliorer la visibilité de l'offre légale.

Après une présentation des principales actions menées à l'égard des utilisateurs sont décrites celles conduites à l'encontre des services illicites.

LES ACTIONS VISANT LES INTERNAUTES

LES ACTIONS À L'ENCONTRE DES UTILISATEURS « QUALIFIÉS »

La loi espagnole n'organise pas de dispositif d'avertissement gradué à destination des internautes mais la procédure civile permet aux ayants droit d'agir contre les utilisateurs dits « qualifiés », à savoir les internautes qui mettent massivement en ligne des contenus protégés^[4]. Il est en effet possible pour les ayants droit d'agir en justice afin d'obtenir que les fournisseurs d'accès à internet leur communiquent l'identité des internautes dont ils auraient collecté l'adresse IP. Les ayants droit

pourront alors agir contre ces derniers devant le tribunal civil ou pénal. Toutefois, au regard de récentes décisions de première instance^[5], il semblerait que le juge espagnol estime que l'identification d'un contrevenant par sa seule adresse IP soit insuffisante, car elle ne permettrait d'identifier que la personne détentrice de l'abonnement à internet et le juge estime que cette dernière n'est pas nécessairement celle de la personne qui s'est livrée aux actes de mise à disposition ou de téléchargement illicite des œuvres.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] Article 256 1) 11° de la loi 1/2000, du 7 janvier 2000 sur la procédure civile.

[5] Affaires Dallas Buyers Club, Sentencia CIVIL N° 240/2017, Juzgados de lo Mercantil - Donostia-San Sebastián, Sección 1, Rec 526/2017 de 02 de Noviembre de 2017 et Sentencia CIVIL N° 239/2017, Juzgados de lo Mercantil - Donostia-San Sebastián, Sección 1, Rec 524/2017 de 02 de Noviembre de 2017.

LES ACTIONS DE SENSIBILISATION

LA CAMPAGNE « NO PIRATEES TU FUTURO »

En octobre 2017, le gouvernement espagnol a lancé une campagne de sensibilisation intitulée « *No piratees tu futuro* » (ne pirate pas ton futur) destinée au jeune public afin de le sensibiliser à la lutte contre le piratage des contenus à la fois culturels et sportifs. La campagne a été réalisée dans le cadre d'un partenariat entre le ministère de la Culture et des Sports et des acteurs du secteur privé qui l'ont financée. Plus de vingt partenariats ont ainsi été conclus, avec notamment la *Coalición de Creadores e Industrias de Contenidos* (la coalition des créateurs et des industries de contenus), *La Liga* (la ligue de football), des médias de communication, la *Federación de Cines* (la fédération des cinémas) et l'*Administrador de infraestructuras ferroviarias* (gestionnaire d'infrastructures ferroviaires). Dans ce cadre, Atresmedia, Disney, Discovery Channel, Mediapro, Movistar +, PrisaRadio et Vodafone ont ainsi diffusé gratuitement la campagne sur leurs espaces. En outre, afin d'inciter les partenaires à diffuser les campagnes sur les chaînes de télévision, le ministère s'est rapproché du régulateur compétent (*Comisión Nacional de los Mercados y la Competencia* : autorité dont les fonctions sont équivalentes à celles de l'autorité de la concurrence et qui intervient également en matière de régulation de l'audiovisuel) afin que les diffusions des publicités de la campagne ne soient pas comptabilisées dans le temps d'antenne que les chaînes peuvent consacrer à la programmation de messages publicitaires.

Le double objectif de cette campagne est d'orienter la population vers l'offre légale et de provoquer l'empathie en montrant l'impact du piratage sur les futures carrières des jeunes, sans insister sur la répression pénale de ces pratiques.

La campagne a été diffusée très largement sur tous types de supports : à la télévision, à la radio, dans les

cinémas, sur les réseaux sociaux, par des bannières publicitaires et dans la presse^[6]. Des célébrités populaires auprès des jeunes (acteurs, sportifs...) ont participé à son lancement.

LA CAMPAGNE DE SENSIBILISATION DANS LES ÉCOLES DU MINISTÈRE DE LA CULTURE ET DES SPORTS

En collaboration avec le ministère de l'Intérieur et une association spécialisée en propriété intellectuelle, le ministère de la Culture et des Sports prépare des supports à destination des enseignants et des élèves pour que des policiers aillent dans les écoles afin de sensibiliser les jeunes publics au piratage.

LA CAMPAGNE DE SENSIBILISATION DANS LES ÉCOLES DE LA COALICION ET DE LA LIGA

Cette campagne existe depuis trois ans. Les élèves sont considérés comme des futurs professionnels du secteur culturel et de l'industrie du divertissement : l'objectif est de leur montrer les conséquences du piratage sur l'emploi et l'économie et qu'ils acquièrent de bonnes habitudes de consommation de contenus sur internet.

Au total, 15 000 élèves âgés de 10 à 13 ans ont participé à la campagne dans une centaine d'établissements scolaires. À l'issue de cette campagne, 80 % des élèves avaient une opinion très négative du piratage.

LA PROMOTION DE L'OFFRE LÉGALE

Un portail qui recense les différentes plateformes a été lancé grâce au soutien du gouvernement et de l'industrie du cinéma. Un moteur de recherche pour les œuvres audiovisuelles (films et séries), relevant d'une initiative privée, est également accessible^[7].

[6] Ci-dessous lien vers les spots de la campagne de communication : <https://www.youtube.com/playlist?list=PLmAw6SZis81I0oqHSBoRs9pGlyyhW0VpZ>

[7] www.encuentratupeli.com

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES SITES ILLICITES ET LEURS OPÉRATEURS

En Espagne, la brigade de la sécurité informatique, une unité de police, est chargée de lutter contre les sites de liens et la diffusion illégale de flux télévisés en *streaming*^[8].

Dans ce cadre, de nombreuses opérations ont été menées ces dernières années dont l'opération CASPER en avril 2017. Cette opération de la police espagnole, coordonnée en lien avec la Bulgarie, Europol et Eurojust, a permis de mettre à jour un réseau criminel, avec des opérateurs établis en Espagne et en Bulgarie, spécialisé dans la distribution illégale sur internet de 1 000 chaînes de télévision payantes à l'échelle européenne.

Plus récemment, en avril 2020, la police nationale espagnole a notamment indiqué avoir démantelé un réseau criminel impliqué dans la fourniture de contenus audiovisuels et télévisuels piratés dans l'ensemble du pays.

LES MESURES ADMINISTRATIVES DE BLOCAGE

Une loi de 2011, modifiée en 2014 et en 2019, a institué un dispositif administratif de notification des atteintes aux droits d'auteur constatées sur les sites internet pouvant aboutir au blocage des sites. Ce dispositif est assuré par une commission rattachée au ministère de la Culture et des Sports.

Les ayants droit peuvent également obtenir le blocage des sites contrefaisants auprès du juge civil et celui-ci est de plus en plus utilisé par les ayants droit depuis 2018.

Présidée par le ministre de la Culture et des Sports, la seconde section de la commission de la propriété intellectuelle (« IPC ») est composée de deux membres du ministère de la Culture et des Sports, un membre du ministère de l'Énergie, du Tourisme et du Numérique, un membre du ministère de la Justice, un membre du ministère de l'Économie et des Entreprises et un membre du ministère de la Présidence, des relations avec les Tribunaux et de l'Égalité.

La commission est saisie par voie électronique par les ayants droit, leurs représentants ou un organisme de gestion collective qui constatent la présence d'un ou plusieurs contenus contrefaisants sur un site d'hébergement de contenus ou de liens ayant un rapport suffisant avec l'Espagne^[9] (ex. : audience du site en Espagne, langue des œuvres diffusées, publicités en Espagnol, paiement en euros...). Les sites de *stream ripping* illicites peuvent également être visés.

La saisine comprend notamment les éléments suivants : identification des contenus illicites, preuve de la titularité des droits, preuve de la violation, preuve de l'intention de retirer des bénéfices pécuniaires des activités illicites ou bien preuve du dommage causé (même s'il n'est qu'éventuel), identification des données relatives au contrevenant et identification des données relatives à l'hébergement du service.

La présence d'une seule œuvre contrefaisante suffit à apprécier l'illicéité d'un site mais le site doit avoir un certain niveau d'audience en Espagne et un volume d'œuvres présumées contrefaisantes pour que la commission ouvre le dossier.

La procédure est gratuite et a une durée maximale de trois mois.

La saisine de la commission ne peut intervenir qu'après l'échec de la tentative de l'ayant droit de contacter le site pour lui demander de retirer le ou les contenus dans les 72 heures et le transfert à la commission de la preuve de cet échec.

Si la commission juge recevable la demande des ayants droit, elle peut enjoindre le responsable du site internet dans un délai de 48 heures :

- de faire valoir ses observations ;
- de faire en sorte que le contenu ne soit plus accessible en assurant son retrait pérenne (*stay down*) ou l'interruption de l'activité qui porte atteinte aux droits d'auteur.

La procédure a pour vocation première d'obtenir une cessation volontaire de la mise à disposition des contenus contrefaisants.

[8] Affaire « Roja Directa ».

[9] Le site internet n'a pas à être « massivement contrefaisant » pour faire l'objet d'une procédure devant la commission. Ce critère peut éventuellement être utilisé pour prioriser l'ordre dans lequel les dossiers doivent être traités.

À défaut de retrait des contenus ou de cessation du service sous 24 heures, la commission peut demander aux intermédiaires techniques de prendre les mesures nécessaires pour faire cesser l'atteinte dans un délai de 48 heures si elle reconnaît l'existence d'une infraction.

Une des modifications introduites par la réforme de 2019 consiste à faire en sorte que la procédure ne soit plus ralentie par l'impossibilité de contacter l'opérateur du service (et donc le non-respect des obligations prévues par la loi en matière d'identification des opérateurs de services internet). Il semble donc que dans ces hypothèses, la procédure se poursuit sans que les étapes détaillées plus haut soient respectées.

Les injonctions peuvent viser différents acteurs de l'écosystème du piratage et leur ordonner de prendre les mesures appropriées : cessation de l'hébergement pour les hébergeurs, blocage par les fournisseurs d'accès à internet d'une durée maximale d'un an lorsque les infractions sont commises par un service établi hors de l'Union européenne, déréférencement par les moteurs de recherche, suspension par le registre espagnol d'un nom de domaine en « .es » ou sous une autre extension gérée par le registre.

Toutefois, l'exécution forcée de ce type de décision est subordonnée à une autorisation du juge. Le juge s'assure alors de la conformité de la demande avec les libertés fondamentales prévues à l'article 20 de la Constitution espagnole, notamment la liberté d'expression^[10].

En cas de réitération, le secrétaire d'État à la culture peut prononcer une amende allant jusqu'à 600 000 euros après deux demandes de retrait de contenus contrefaisants contre les sites qui n'ont pas procédé aux retraits ou lorsque les contenus sont réapparus^[11].

Avec la réforme de 2019, lorsqu'un site web qui a déjà été sanctionné pour des infractions à deux reprises, avec les autorisations judiciaires correspondantes le cas échéant, met pour la troisième fois à disposition des contenus sans autorisation et refuse de les retirer de son site web, il sera possible d'agir plus rapidement et efficacement sans avoir besoin d'obtenir une autorisation judiciaire pour appliquer les mesures appropriées. Des mesures de blocage pourront alors être prononcées sans besoin d'une nouvelle validation par le juge.

Pour la première fois, le 20 juin 2018, après avoir été condamné à deux reprises par la commission en juin et juillet 2017, le propriétaire du site péruvien « www.x-caleta.com » devenu « www.x-caleta2.com » a été condamné à une amende de 375 000 euros pour infraction administrative continue. Outre cette amende, la sanction a été publiée aux dépens du sanctionné dans le journal officiel local, dans deux journaux nationaux et les sites en cause ont également été bloqués en Espagne pour une durée d'un an.

Le 20 juin 2019, les juridictions centrales du contentieux administratif ont autorisé l'exécution d'une décision de blocage de la commission portant sur plus de 60 pages internet liées au nom de domaine *ThePirateBay*.

La commission publie des rapports trimestriels sur son activité^[12]. De la date de sa création jusqu'en décembre 2020, la commission a été saisie de 703 demandes. Parmi les saisines remplissant les conditions prévues par la loi (386), 112 ont été clôturées car les sites ont accédé à la demande de retrait des contenus ou sont devenus caducs.

Les ayants droit souhaiteraient simplifier et accélérer la procédure, afin d'obtenir davantage de décisions de blocage. La commission travaille à améliorer l'efficacité et la durée de la procédure et traite aujourd'hui un dossier entre 90 et 50 jours en moyenne.

L'administration espagnole souhaiterait également mettre en place un code de conduite volontaire entre les ayants droit et les intermédiaires d'internet. Ce code aurait pour objet la mise en place de mesures de collaboration dans la lutte contre la contrefaçon sur internet.

LES MESURES JUDICIAIRES DE BLOCAGE

Le dispositif judiciaire est de plus en plus utilisé par les ayants droit, notamment américains, depuis 2018 car ils le jugent plus rapide que le dispositif administratif.

En février 2018, le tribunal de commerce de Barcelone, saisi par six studios de cinéma et de télévision, a jugé que deux sites de *streaming* portaient atteinte aux droits de ces derniers et a ordonné aux principaux fournisseurs d'accès à internet espagnols de bloquer l'accès à ces sites ainsi qu'aux noms de domaine, sous-domaines

[10] Article 20 de la Constitution espagnole : « 1. On reconnaît et on protège le droit : a) d'exprimer et de diffuser librement les pensées, les idées et les opinions par la parole, l'écrit ou tout autre moyen de reproduction ; [...] 2. L'exercice de ces droits ne peut être restreint par aucune forme de censure préalable. [...] ».

[11] Article 195 du code de la propriété intellectuelle.

[12] <https://www.culturaydeporte.gob.es/dam/jcr:17707579-59fb-42b6-92b1-9fc4926b48ed/2020-diciembre-boletin.pdf>

et adresses IP dont l'objet serait d'indirectement faciliter l'accès à ces sites^[13].

Au cours de l'année 2019, les ayants droit américains de l'audiovisuel ont assigné à plusieurs reprises les principaux fournisseurs d'accès à internet espagnols pour demander le blocage de sites illicites devant la cour commerciale de Barcelone. La cour commerciale^[14] a ainsi ordonné le blocage par les moyens et mécanismes techniques que les fournisseurs d'accès à internet jugeront le plus efficace pour empêcher ou réduire l'accès de leurs clients à un site visé. L'injonction vise également d'autres noms de domaine, sous-domaines et adresses IP dont le but unique ou principal est de faciliter l'accès aux pages du site visé.

Les ayants droit de la musique ont également assigné les fournisseurs d'accès à internet et ont obtenu le blocage de 17 sites de *stream ripping* illicites selon cette procédure.

En 2020, le tribunal de commerce de Barcelone, saisi par l'entreprise de jeux vidéo Nintendo, a ordonné le blocage, dans deux affaires distinctes, de l'accès à des noms de domaine de sites proposant des jeux piratés d'une part et des dispositifs permettant de jouer avec des jeux piratés sur des consoles Nintendo d'autre part.

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

La commission précitée a également en charge un dispositif « *Follow the money* » qui lui permet de demander aux intermédiaires de paiement et aux acteurs de la publicité de cesser de collaborer avec les sites qui refusent de retirer les contenus notifiés. L'objectif pour la commission consiste à identifier, lors des investigations préliminaires, quels organismes de paiement et de publicité sont partenaires du site en infraction. Si les intermédiaires de paiement et les acteurs de la publicité ne cessent pas leur relation contractuelle avec les sites, la commission peut leur infliger une sanction administrative allant jusqu'à 600 000 euros. Cette sanction n'a été prononcée qu'une seule fois en 2014.

En outre, la loi sur le droit d'auteur prévoyait déjà la promotion de codes de conduite mais visait seulement les intermédiaires techniques et les acteurs de la publicité et du paiement en ligne. Depuis la réforme de 2019, les ayants droit sont désormais également invités à conclure de tels accords, aux côtés de l'autorité publique, laquelle pourra non seulement participer, mais aussi promouvoir la signature de tels accords.

Enfin, l'Espagne a récemment adhéré au dispositif « *WIPO ALERT* » mis en place par l'OMPI qui vise à mettre en œuvre l'approche de démonétisation à l'échelle internationale.

LA LUTTE CONTRE LE PIRATAGE DE CONTENUS SPORTIFS

Le 11 février 2020, dans le cadre d'une procédure initiée par le diffuseur *Telefónica Audiovisual Digital*, le tribunal de commerce de Madrid^[15] a rendu une décision ordonnant le blocage dynamique de sites diffusant illicitement des matchs de football en direct. Le juge a ordonné le blocage de 44 sites ou services, et en particulier de serveurs d'authentification et d'aiguillage, lesquels permettent aux services IPTV illicites de vérifier que l'utilisateur qui veut accéder à l'offre est bien le titulaire d'un abonnement valide. Les ayants droit ont la possibilité de notifier les nouvelles adresses à bloquer aux fournisseurs d'accès à internet toutes les semaines sans avoir à repasser devant le juge. Les mesures de blocage devront être mises en œuvre dans les trois heures à partir de la notification des noms de domaine, URL et adresses IP à bloquer. La décision court jusqu'au 25 mai 2022, soit pour trois saisons de football.

L'IMPLICATION DES MOTEURS DE RECHERCHE

La Liga a conclu un partenariat en septembre 2018 avec le moteur de recherche Google pour procéder au déréférencement des résultats pointant vers les sites des vendeurs de bouquets de chaînes illégaux (vente, service client, FAQ, etc.).

[13] <https://www.poderjudicial.es/search/contenidos.action?action=contentpdf&datasematch=AN&reference=8293989&links=%20HDFull&optimize=20180220&publicinterface=true>

[14] Tribunal commercial I de Madrid, *Columbia V Telefonica*, 7 mars 2019 Ref131376, 16 mai 2019 Ref131847, 10 juillet 2019 132321, 24 octobre 2019 133090, 24 octobre 2019 133090, 29 novembre 2019 133737.

La première décision de blocage de sites illicites de *stream ripping* a été obtenue en avril 2019. Tribunal de commerce de Barcelone, *AGEDI v Telefonica* 29 avril 2019, 201910269787429, <http://www.hadopi.info/dj/news/ressources/20190429%20-%20Mercantile%20Court%20of%20Barcelona%20-%20Decision%20on%20the%20merits%20-%20Flvt0,%20conv,%20Flv2mp3.pdf>

[15] Tribunal de commerce de Madrid, 11 février 2020, 28079470072020100001 <http://www.poderjudicial.es/search/AN/openDocument/d1ecc270d29d6605/20200219>

ÉTATS-UNIS

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

331 POPULATION^[1]
en millions

88,5 % TAUX DE PÉNÉTRATION
INTERNET (2018)^[2]

USAGES ILLICITES^[3]

11,8 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

40 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



Aux États-Unis, malgré certaines initiatives pour engager des actions à l'égard des internautes, les ayants droit américains concentrent leurs actions sur les services illícites. Par ailleurs, une liste des services impliqués dans la contrefaçon

massive est réalisée par le gouvernement dans le but de sensibiliser le public et les États qui protègent insuffisamment la propriété intellectuelle. Des réflexions ont également été conduites pour responsabiliser les plateformes.

LES ACTIONS VISANT LES INTERNAUTES

LES ACTIONS VISANT À RESPONSABILISER LES INTERNAUTES

L'article 512 du *Digital Millennium Copyright Act* (DMCA), qui est le texte définissant le régime de responsabilité des intermédiaires techniques en présence de contenus portant atteinte au droit d'auteur, prévoit des dispositions visant à inciter les fournisseurs d'accès à internet à prendre des mesures spécifiques à l'encontre des titulaires d'abonnement qui commettent des infractions de façon répétée. Ces sanctions peuvent aller jusqu'à la résiliation de l'abonnement.

Certains ayants droit transmettent ainsi aux fournisseurs d'accès à internet des notifications pédagogiques à l'attention de leurs abonnés, leur indiquant qu'ils ont partagé une œuvre sur les réseaux pair à pair. Plusieurs fournisseurs d'accès à internet transmettent ces messages et indiqueraient à leurs abonnés qu'ils pourraient voir leur connexion interrompue en cas de réitération.

LE DISPOSITIF DE RÉPONSE GRADUÉE (2013-2017)

Un système de réponse graduée (*Copyright Alert System*) entièrement volontaire et d'initiative privée a fonctionné de février 2013 à janvier 2017. Il avait essentiellement une vocation pédagogique et d'orientation vers des alternatives légales.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

Un centre d'information sur le *copyright* (CCI), regroupant les ayants droit et les fournisseurs d'accès, coordonnait la mise en place du dispositif et la mise en œuvre d'actions de sensibilisation, notamment *via* un site dédié comportant des éléments sur la sécurisation du *Wi-Fi* et l'offre légale^[4]. L'accord précisait que le CCI était cofinancé à 50 % par les ayants droit et à 50 % par les fournisseurs d'accès à internet.

Les alertes étaient envoyées par les fournisseurs d'accès à internet après collecte des adresses IP par les ayants droit. Les sanctions qui pouvaient être mises en œuvre au terme de la procédure étaient modérément contraignantes pour l'abonné (par exemple obligation pour l'abonné de contacter son fournisseur d'accès à internet ou de suivre une courte formation en ligne sur le droit d'auteur, ralentissement du débit). Toutefois, la possibilité d'exiger des fournisseurs d'accès à internet qu'ils mettent en œuvre une sanction de résiliation de l'accès internet a été exclue par les parties à l'accord. Les fournisseurs d'accès à internet en avaient d'ailleurs fait un point essentiel lors des négociations.

Dès mai 2015, l'*Internet Security Task Force* (qui regroupe des studios américains indépendants) avait estimé que ce dispositif était inefficace en dénonçant notamment le fait que le nombre d'alertes envoyées par les fournisseurs d'accès à internet était limité mensuellement et que la simple pédagogie aurait trouvé ses limites. Début 2017, faute d'accord entre les parties, notamment sur l'éventuel renforcement des sanctions pour les abonnés réfractaires (en anglais « *repeat infringers* ») à la seule pédagogie, il a été décidé de mettre un terme à ce dispositif. Pour autant, certains fournisseurs d'accès à internet continuent à prendre des mesures à l'encontre de leurs abonnés similaires à celles pouvant être prises antérieurement dans le cadre de la réponse graduée.

La mise en œuvre du dispositif gradué n'interdisait pas par ailleurs que certains ayants droit, essentiellement du secteur des contenus pour adultes, recourent à d'autres procédés tels que l'envoi de demandes de dédommagement aux internautes. Ces procédés continuent aujourd'hui : plus de 1 000 actions de ce type auraient ainsi été intentées en 2017 et 1 700 sur le premier semestre 2018.

LES ACTIONS À L'ENCONTRE DES FOURNISSEURS D'ACCÈS À INTERNET

Le 1^{er} novembre 2015, le fournisseur d'accès à internet Cox Communications a été jugé responsable du fait de sa politique à l'égard de ses abonnés et notamment des *repeat infringers*, dans le cadre d'une action intentée par l'éditeur de musique BMG. Ce fournisseur d'accès à internet n'était pas partie à l'accord relatif au dispositif d'avertissement graduel mais s'était doté en application du DMCA de son propre dispositif graduel. Ce dispositif comptait plus de dix étapes à l'issue desquelles les comptes des abonnés ne pouvaient pas réellement être suspendus. La décision se fondait en partie sur la conclusion du tribunal selon laquelle, en raison de son incapacité à mettre en œuvre une politique prévoyant la résiliation dans des circonstances appropriées des comptes des abonnés qui se sont avérés être des contrefacteurs récidivistes, Cox Communications ne pouvait bénéficier du régime de responsabilité limitée des fournisseurs de services internet prévue par le DMCA. En août 2018, Cox Communications est parvenu à un accord avec BMG, l'éditeur de musique qui l'avait assigné.

Dans la suite de cette action, fin 2019, un jury fédéral de Virginie a déclaré Cox Communications responsable des violations des droits d'auteur commises par ses abonnés, celui-ci devant verser un milliard de dollars de dommages et intérêts à plusieurs majors de l'industrie musicale. Les fournisseurs d'accès à internet Grande Communications et Charter Communications font aujourd'hui face aux mêmes accusations dans des actions également initiées par l'industrie musicale.

Dans le cadre de ces actions contre les fournisseurs d'accès à internet, il a notamment été enjoint à Cox Communications et Charter Communications de dévoiler aux ayants droit des informations concernant plusieurs milliers de leurs abonnés, et notamment des abonnés à titre professionnel, qui ont été destinataires de notifications. Toutefois, l'un des abonnés professionnels de Cox Communications, une organisation à but non lucratif qui fournit des locaux hospitaliers ou de traitement médicaux, a contesté l'injonction. Elle fait savoir qu'elle fournit une connexion à internet publique et gratuite, de telle sorte que n'importe quel visiteur a pu télécharger illégalement sur son réseau. En outre, l'organisation ne conservant aucune donnée de connexion, il est impossible de déterminer quel visiteur s'est connecté, et fournir aux ayants droit les informations demandées ne présenterait aucun intérêt pour les parties. Le juge a fait droit en juin 2019 à la contestation de l'organisation, interdisant à Cox Communications de partager ces informations.

[4] www.copyrightinformation.org

LES ÉVOLUTIONS À VENIR : LE RAPPORT DU BUREAU DU DROIT D'AUTEUR

Après plusieurs consultations et tables rondes organisées depuis 2015 – la dernière table ronde datant d'avril 2019 – le Bureau du droit d'auteur (*Copyright Office*), l'entité publique chargée des questions de propriété intellectuelle, a publié le 21 mai 2020 un rapport relatif à l'impact et l'effectivité des dispositions relatives à la responsabilité limitée des intermédiaires techniques créé par l'article 512 du DMCA, adopté en 1998^[5]. Ce rapport estime que si l'objectif de l'article 512 était de créer un régime à même d'assurer la sécurité juridique des opérateurs afin de permettre le développement de l'internet tout en protégeant les ayants droit, aujourd'hui il s'avère que le fonctionnement du système de responsabilité limitée prévu par cet article est déséquilibré. Le Bureau ne recommande cependant pas de modification majeure de l'article 512, mais identifie plutôt certains domaines dans lesquels le Congrès pourrait souhaiter préciser les modalités de fonctionnement du DMCA afin de mieux équilibrer les droits et les responsabilités des fournisseurs de services en ligne et des titulaires de droits dans les industries créatives.

S'agissant de la disposition du DMCA prévoyant que les fournisseurs d'accès à internet doivent prendre des mesures vis-à-vis des *repeat infringers*, le rapport va dans le sens de la jurisprudence de 2018 contre le fournisseur d'accès à internet Cox Communications. Il estime que pour que cette disposition ait un effet utile, il n'est pas nécessaire qu'un internaute ait été reconnu coupable d'infraction au droit d'auteur par une juridiction pour que le fournisseur d'accès à internet puisse le considérer comme « récidiviste ». Alors qu'en l'état, pour bénéficier du régime de responsabilité limitée, les fournisseurs d'accès peuvent se contenter d'avoir une politique non écrite prévoyant la résiliation, dans les circonstances appropriées, de l'abonnement de l'internaute qui persiste à enfreindre le droit d'auteur. Le Bureau estime qu'il est peu probable que de telles politiques non écrites et non communiquées aux internautes aient un effet dissuasif. Il préconise donc que les intermédiaires rendent accessibles au public leur politique concernant les actes de contrefaçon répétés. Le rapport indique également que le Congrès pourrait vouloir examiner l'opportunité de légiférer sur ce qui constitue des « *circumstances appropriées* » et si de telles circonstances peuvent être constituées en l'absence de demande de retrait d'un titulaire de droits.

Le rapport met également en évidence les restrictions actuelles sur les informations qui peuvent être

demandées par voie judiciaire dans le cadre du DMCA. Ainsi, en droit positif, les ayants droit peuvent demander l'identité des propriétaires de sites à des intermédiaires tiers tels que Cloudflare ou les bureaux d'enregistrement, mais la jurisprudence a estimé que ces injonctions ne pouvaient pas être utilisées pour identifier les abonnés commettant des actes de contrefaçon. Le Bureau du droit d'auteur recommande une clarification des dispositions du DMCA à cet égard.

La sous-commission propriété intellectuelle de la commission judiciaire du Sénat a prévu une série d'auditions tout au long de l'année 2020 sur le DMCA. L'une de ces auditions portera sur le rapport du Bureau du droit d'auteur.

Enfin, le Bureau du droit d'auteur prévoit en outre de travailler sur des supports pédagogiques sur les droits et responsabilités de chacune des parties prenantes du système de l'article 512 du DMCA.

À noter qu'une première ébauche d'une réforme du DMCA a été publiée en décembre 2020, faisant suite à une série d'auditions avec des créateurs, utilisateurs et entreprises technologiques.

Ce document propose ainsi de se défaire de la formulation de « *repeat infringer* » pour adopter celle de « *personnes qui, à plusieurs reprises, ont fait l'objet de notifications (...) qui n'ont pas été contestées avec succès* ». L'administration américaine devrait par ailleurs préciser cette définition et le traitement des récidivistes.

Enfin, ce projet prévoit la création d'une liste de personnes ou entités envoyant à plusieurs reprises de fausses notifications, les services en ligne n'étant alors pas tenus d'agir en cas de notifications de la part de ces dernières.

LA PROMOTION DE L'OFFRE LÉGALE

Afin de diriger les internautes vers l'offre légale, la MPA a lancé en 2014 un moteur de recherche de l'offre légale audiovisuelle (films et séries télévisées), qui permet aux internautes d'effectuer une recherche par œuvre pour savoir où la trouver légalement. Le site a été supprimé à la fin de l'année 2017, la MPA estimant qu'il y a aujourd'hui plusieurs offres commerciales de moteurs de recherche sur ce segment et qu'il existe une offre légale importante aux États-Unis (plus de 140 plateformes) et dans le monde.

[5] <https://www.copyright.gov/policy/section512/section-512-full-report.pdf>

L'administration américaine a publié en décembre 2020 son *Joint Strategic Plan*, programme en matière de défense de la propriété intellectuelle pour les trois prochaines années. Ce document prévoit notamment que les agences fédérales américaines serviront de relais auprès des consommateurs afin de les sensibiliser à la valeur de la propriété intellectuelle et aux menaces que

représentent les produits contrefaits et les œuvres piratées (et notamment les virus). Afin de maximiser la portée des actions de sensibilisation auprès des publics cibles, les agences fédérales étudieront les moyens de tirer parti de la technologie (par exemple, la vidéoconférence) et des partenariats public-privé (par exemple, la collaboration avec les associations professionnelles).

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES SITES ILLICITES ET LEURS OPÉRATEURS

Aux États-Unis, nombre d'actions sont enfin intentées directement contre les acteurs illicites et permettent souvent aux ayants droit de se voir octroyer des dommages et intérêts importants.

L'*Alliance For Creativity and Entertainment* (ACE - créée à l'été 2017 et réunissant des ayants droit du monde entier^[6] (34 à ce jour) dans une association ayant vocation à lutter contre le piratage au niveau international) est à l'origine de plusieurs actions d'envergure telles que :

- en octobre 2017, l'ACE a engagé une action contre la société TickBox qui vendait sur un site dédié un boîtier qui permettait d'accéder à des contenus contrefaisants. En janvier 2019, l'ACE a obtenu du juge des dommages-intérêts à hauteur de 22 millions d'euros contre la société TickBox ;
- en janvier 2019, l'ACE a obtenu une victoire judiciaire contre le concepteur de boîtiers dédiés au piratage Dragon Media et un revendeur. Une injonction permanente leur impose de cesser toute activité de piratage et de payer 12,8 millions d'euros de dommages et intérêts ;
- en mai 2019, l'ACE a obtenu la fermeture du service illicite *One Step TV*, un fournisseur d'IPTV proposant des milliers de films et environ 600 chaînes de télévision en direct, ainsi que la saisie du nom de domaine associé. L'adresse renvoie désormais au site de l'ACE ;

- en juillet 2019, l'ACE a obtenu une injonction permanente à l'encontre de la société à l'origine de *SET TV*, un service IPTV populaire basé sur un logiciel qui était également vendu préchargé sur des boîtiers. En novembre 2019, l'ACE a obtenu un jugement par défaut à l'encontre des deux opérateurs du service et 6,76 millions d'euros de dommages et intérêts ;
- en novembre 2019, février 2019, le service *Omniverse*, qui vendait des services de *streaming* en direct à des distributeurs tiers, lesquels proposaient à leurs clients des bouquets IPTV, a cessé ses activités à la suite d'un accord homologué en justice intervenu en novembre 2019 et actant le paiement de 44,19 millions d'euros de dommages et intérêts.

Des actions ont également été engagées par l'industrie musicale contre des services de *stream ripping* illicites. On peut notamment relever qu'en septembre 2016, la *Recording Industry Association of America* (RIAA), l'*International Federation of the Phonographic Industry* (IFPI) et la *British Phonographic Industry* (BPI) ont déposé une plainte en Californie contre le site *YouTube-mp3*, géré par une entreprise, *PMD Technologie UG*, basée en Allemagne. Les ayants droit ont sollicité des dommages et intérêts très importants, ainsi que la saisie du nom de domaine *YouTube-mp3* et une injonction de ne plus porter atteinte à leurs droits pour l'avenir. En septembre 2017, les parties sont parvenues à un accord : le site a été fermé et *YouTube-mp3* s'est engagé à verser des indemnités (dont le montant n'a pas été divulgué) aux ayants droit.

[6] Amazon, AMC Networks, BBC Worldwide, Bell Media, Canal+ Group, 5, Charter communications, Comcast, CBS Corporation, Constantin Film, Discovery, Fox, Foxtel, Grupo Globo, HBO, Hulu, Lionsgate, Metro-Goldwyn-Mayer (MGM), NBCUniversal, Netflix, Paramount, SF Studios, Sky, Sony Pictures, Star, Studio Babelsberg, STX Entertainment, Telefe, Telemundo, Televisa, Univision Communications Inc., Viacom CBS, Village Roadshow, Disney, and Warner Bros. Entertainment Inc.

En août 2018, la RIAA a déposé une plainte au nom de 12 maisons de disques contre les sites illicites de *stream ripping* *Flvto* et *2conv*, demandant une injonction et des dommages-intérêts en invoquant des violations du droit d'auteur commises directement et par la fourniture de moyens notamment, ainsi que pour contournement de mesures techniques de protection. Cependant, les deux sites étant administrés depuis la Russie, pays de résidence de leur opérateur, et ne visant pas spécifiquement le public américain, ce dernier a introduit une exception d'irrecevabilité, estimant que le tribunal de Virginie n'était pas compétent. Le 22 janvier 2019, le tribunal fédéral du district est de Virginie a rendu sa décision de rejet de l'affaire de la RIAA pour défaut de compétence. Fin juin 2020, la RIAA a finalement eu gain de cause en appel.

En décembre 2020, une loi devant permettre les poursuites contre les opérateurs de services proposant illicitement des contenus en *streaming* à des fins commerciales a été promulguée (auparavant le *streaming* illicite était une infraction mineure faisant potentiellement encourir des peines moindres). Ainsi, elle punit la fourniture d'un service principalement conçu pour diffuser du contenu portant atteinte au droit d'auteur, n'ayant pas d'autre but commercial significatif que de tirer profit du *streaming* illicite ou étant intentionnellement commercialisé pour le promouvoir. Il est important de souligner que cette législation ne vise que les personnes ou les organisations qui fournissent un « service de transmission numérique », les utilisateurs ordinaires qui téléversent du contenu sur des plateformes de partage tel que YouTube ne sont donc pas visés, cette distinction ayant été au cœur des discussions. Les opérateurs des services visés risquent une amende et une peine de prison pouvant aller jusqu'à dix ans pour les récidivistes.

LES MESURES ALTERNATIVES AUX MESURES DE BLOCAGE

Aux États-Unis, depuis l'échec en janvier 2012 des propositions de loi dite SOPA et PIPA, qui visaient notamment à permettre le blocage de sites, l'introduction d'un dispositif de blocage des sites a été abandonnée jusqu'à nouvel ordre. En 2020, le rapport du Bureau du droit d'auteur précité a préconisé qu'une étude complémentaire soit conduite sur ce point. Il considère en effet que bien qu'il existe des preuves de l'efficacité de ces mesures dans d'autres pays, celles-ci ne sont pas toujours cohérentes et, en particulier, il est difficile d'avoir une vision exacte de l'efficacité de ces mesures face à l'impact potentiel sur la liberté d'expression.

À ces actions en cessation se sont substituées notamment des procédures de saisie de noms de domaine. La saisie de noms de domaine peut être obtenue *via* les actions conduites par le *National Intellectual Property Rights Coordination Center* (the « *IPR Center* »), qui est l'entité chargée de la lutte contre la contrefaçon et qui dépend du ministère de la Sécurité intérieure et du ministère de la Justice. Dans le cadre d'une opération intitulée « *In Our Sites* », en lien avec Europol et Interpol, en novembre 2017, l'*IPR Center* a saisi 20 520 noms de domaine offrant des produits contrefaits ou des biens culturels piratés.^[7] À la place des sites, les internautes accèdent à une bannière pédagogique hébergée par l'*IPR Center*.

Dans des actions judiciaires plus ciblées visant à empêcher le piratage de certains contenus culturels ou sportifs, le juge peut également prononcer des injonctions aux gestionnaires de noms de domaine, comme cela a par exemple été le cas dans les affaires suivantes :

- l'*Indian Cricket Premier League* (TCL) a ainsi obtenu en mai 2017 une injonction à l'encontre de différents sites listés de ne pas diffuser les matchs de l'*Indian Cricket Premier League*. La décision prévoyait d'autres injonctions, d'une part, à l'encontre d'une série d'intermédiaires financiers (solutions de paiement et intermédiaires de publicité) partenaires de ces sites et, d'autre part, à l'encontre d'autres acteurs (hébergeurs, CDN, bureaux d'enregistrement et registres de noms de domaine^[8]) qui redirigeraient vers ces sites afin qu'ils cessent de leur fournir leurs services jusqu'à la fin de la saison ;

[7] <https://www.europol.europa.eu/newsroom/news/biggest-hit-against-online-piracy-over-20-520-Internet-domain-names-seized-for-selling-counterfeits>

[8] Pendant la saison, les noms de domaine visés par l'injonction peuvent également faire l'objet d'une mesure de rétention par les bureaux d'enregistrement et/ou les registres (transfert des noms de domaine au cabinet d'avocat en charge du dossier des titulaires de droit).

- le diffuseur américain *Showtime* a agi de manière préventive pour empêcher des sites illicites de diffuser un match de boxe particulièrement attendu dès 2015 et à nouveau en août 2017 (*Mayweather vs McGregor*). Un tribunal fédéral en Californie a ainsi émis une injonction préliminaire à l'encontre de 44 noms de domaine différents annonçant le combat pour que le match n'y soit pas diffusé pendant une période donnée ;
- en juillet 2017, une cour fédérale en Floride a ordonné, sur demande d'un important acteur des médias philippins, une mesure temporaire de saisie de noms de domaine de sites contrefaisants ainsi qu'une indisponibilité des fonds destinés aux sites en cause qui sont détenus par les opérateurs de publicité^[9]. En juillet 2018, le même ayant droit a obtenu une injonction provisoire à l'encontre des bureaux d'enregistrement de noms de domaine et des registres de rendre inaccessibles les sites visés et à l'encontre des acteurs de la publicité ainsi que du paiement en ligne, de rendre indisponibles les fonds détenus pour ces sites et de communiquer à la cour un inventaire détaillé de ces fonds.

En juin 2017, la cour du district sud de l'État de New York a ordonné le transfert des noms de domaine du site Sci-Hub, spécialisé dans le partage illicite d'articles de presse et de revues scientifiques, au profit des ayants droit de ces articles. Un jugement distinct de la cour du district est de l'État de Virginie a accordé à un ayant droit 4,25 millions d'euros de dommages-intérêts.

L'IMPLICATION DES BUREAUX D'ENREGISTREMENT DE NOMS DE DOMAINE

Le programme en matière de défense de la propriété intellectuelle publié en décembre 2016 s'appuyait sur le constat que les responsables de sites massivement contrefaisants pratiquent le *domain name hopping*^[10], ou changement de noms de domaine, dès qu'un nom ne peut plus être utilisé car il fait l'objet d'une décision de blocage, voire d'une suspension. Dans ce contexte, les États-Unis avaient annoncé poursuivre leur évaluation des enregistrements abusifs de noms de domaine dans l'optique d'agir contre ces pratiques.

Dans cette perspective, la MPA a signé en février 2016 un accord avec le registre *Donuts* qui gère plusieurs extensions, et notamment les « .movie », puis en mai 2016 avec le registre *Radix*, localisé à Dubaï, qui gère également plusieurs extensions, et notamment les « .website » ou « .online ». Ces accords prévoient la possibilité de suspendre les noms de domaine des sites massivement contrefaisants notifiés par la MPA^[11]. Selon le plan d'action de l'administration pour la propriété intellectuelle de 2020, le succès de ces accords pourrait permettre au secteur privé d'en augmenter le nombre et la portée.

Dans le même ordre d'idée, le plan d'action publié en 2020 annonce que les États-Unis continueront de collaborer avec l'ICANN^[12] pour trouver une solution entre les exigences de protection des données personnelles, telles que prévues notamment par le Règlement général européen sur la protection des données, et la publicité des informations d'identification et de contact des titulaires et responsables de noms de domaine dans la base de données dite « WHOIS », ce dans le but de permettre aux tiers ayant des intérêts légitimes (tels que les services de police et les titulaires de droits de propriété intellectuelle) d'identifier les responsables de noms de domaine utilisés à des fins illicites.

[9] <https://torrentfreak.com/images/fccb57c7-b666-4495-aa07-783c429e6613.pdf>

[10] Pour ce faire, des centaines ou des milliers de noms de domaine sont enregistrés par les opérateurs de sites massivement contrefaisants, ce dans plusieurs juridictions, notamment celles qui protègent peu les droits de propriété intellectuelle. Ainsi, des sites miroirs peuvent aisément être créés, de sorte que l'efficacité des poursuites engagées est amoindrie.

[11] Dans ce cadre, la MPA deviendrait un *trusted notifier* et notifierait à *Donuts* ou *Radix* les sites qui sembleraient contrefaisants. *Donuts* ou *Radix* effectueraient ensuite une enquête et commenceraient par contacter le site. En l'absence de réponse ou en cas de réponse insuffisante, *Donuts* ou *Radix* procèdent à la suspension du nom de domaine.

[12] Internet Corporation for Assigned Names and Numbers, structure ayant notamment une mission d'administration de l'internet afférente notamment à la gestion de l'adressage IP et des noms de domaine, en lien avec les registres et les bureaux d'enregistrement.

L'IMPLICATION DES MOTEURS DE RECHERCHE

Aux États-Unis, comme au Royaume-Uni, Google a pu échanger avec les ayants droit sur l'optimisation de *demotion*, l'algorithme de sous-référencement des sites en fonction du nombre de notifications de contenus contrefaisants. Comme indiqué dans son rapport *How Google fights piracy*, Google a mis en œuvre une fonctionnalité permettant de donner plus de poids aux demandes de retrait visant par exemple des œuvres audiovisuelles pas encore sorties ou encore diffusées en salle.

Le programme en matière de défense de la propriété intellectuelle de 2020 constate que des progrès ont été réalisés tant s'agissant de la rétrogradation des résultats de recherche sur internet pour les sites contrefaisants que des liens vers les contenus illicites eux-mêmes. Les États-Unis demandent que les moteurs de recherche continuent à mettre à jour et à améliorer leurs outils de rétrogradation et à collaborer avec les ayants droit afin de rendre plus difficile la prolifération de contenus contrefaisants.

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

Les ayants droit et l'administration prônent aux USA la conclusion d'accords volontaires avec le plus grand nombre d'intermédiaires au-delà des seuls acteurs du paiement et de la publicité en ligne tels que les hébergeurs, les registres et les bureaux d'enregistrement, les CDN ainsi que les moteurs de recherche.

L'IMPLICATION DES INTERMÉDIAIRES DE PAIEMENT

Des accords ont été conclus en mai 2011, avec le soutien de l'administration Obama, entre les ayants droit et les intermédiaires de paiement^[13], qui visent aussi bien les contrefaçons de droits d'auteur que de marques. En application de ces accords est née l'initiative

RogueBlock^[14] qui permet de faire cesser la fourniture de moyens de paiement aux sites contrefaisants. Dans ce cadre, une plateforme sécurisée de l'*International AntiCounterfeiting Coalition (IACC)* – dont les membres sont des titulaires de droits de propriété intellectuelle – est destinataire des signalements des ayants droit. À ce jour, l'IACC fait savoir que le programme a permis de toucher plus de 200 000 sites (sur des motifs de contrefaçon de marques ou de droits d'auteur confondus). Depuis 2015, les sites hébergeant des contenus illicitement mis à disposition (*cyberlockers*) sont également visés par les actions entreprises dans le cadre de *RogueBlock*. Ce dispositif ne semble toutefois pas être très utilisé par les titulaires de droits d'auteur, qui préfèrent développer des relations de confiance directement avec les intermédiaires de paiement.

L'IMPLICATION DES ACTEURS DE LA PUBLICITÉ EN LIGNE

En juillet 2013, plusieurs régies publicitaires^[15] ont signé une charte de bonnes pratiques (*Best practices guidelines for ad networks to address piracy and counterfeiting*).

En février 2015, le *Trustworthy Accountability Group (TAG)*^[16] a lancé le *Brand Integrity Program Against Piracy*, qui propose des outils et services permettant d'identifier et de prévenir le risque de diffusion de publicités sur des sites contrefaisants. Plusieurs outils et programmes ont ensuite été régulièrement lancés^[17], le dernier en date étant un livre blanc intitulé « *Winning the Fight Against Ad-Supported Piracy* »^[18], qui vise à donner aux intermédiaires de la publicité en ligne un certain nombre d'outils et de recommandations afin de s'assurer que leurs publicités ne figurent pas sur un site illicite.

Plus récemment, le TAG a signé le MoU européen sur la publicité en ligne et les droits de propriété intellectuelle.

[13] MasterCard, Visa International, Visa Europe, PayPal, MoneyGram, American Express, Discover, PULSE, Diners Club et Western Union.

[14] www.iacc.org/online-initiatives/rogueblock

[15] Media, Adtegrity, AOL, Condé Nast, Google, Microsoft, SpotXchange et Yahoo!.

[16] L'Association of National Advertisers et l'American Association of Advertising Agencies, se sont associées avec l'IAB pour créer le Trustworthy Accountability Group (TAG).

[17] En octobre 2015, un nouveau programme, Verified by TAG, a été mis en place afin de créer une liste d'annonceurs et de supports validés. En juin 2017, le TAG a lancé un outil permettant d'aider ses membres à ne pas diffuser de publicités sur des applications mobiles qui mettent illicitement à disposition des contenus protégés. En octobre 2017, le TAG a publié une étude « *Measuring Digital Advertising Revenue to Infringing Sites* » estimant les revenus des principaux sites dédiés à la contrefaçon à 111 millions de dollars, dont 83 % issus d'annonceurs non-premium. L'étude indique également que si l'industrie ne s'était pas mobilisée, ces services auraient touchés des revenus de 48 % et 61 % supérieurs.

[18] https://cdn2.hubspot.net/hubfs/2848641/TAG_WhitePaper_AntiPiracy_005.pdf

LA PUBLICATION DE LISTES NOIRES

L'administration américaine, via l'*United States Trade Representative* (USTR), une agence gouvernementale qui coordonne la politique commerciale des États-Unis, publie chaque année :

- une liste, prévue par la loi (la *Special 301 List*), qui répertorie les pays qui ne fournissent pas une protection effective des droits de propriété intellectuelle ;
- une liste des marchés qui commettent ou incitent manifestement à la commission d'infractions aux droits de la propriété intellectuelle (le rapport « *Out-of-cycle Review of Notorious Markets* » ou « *Notorious Markets List* »). La liste est constituée en toute transparence à partir des données fournies via un site internet par toute personne désireuse d'y contribuer, qu'importe où elle se situe dans le monde. Alors qu'auparavant la liste visait seulement les marchés hors États-Unis, l'édition 2020 vise des antennes locales d'Amazon, compagnie pourtant basée aux États-Unis. Seuls les services pour lesquels de nombreuses informations concordantes ont été reçues figurent ensuite sur la liste. Les marchés listés sont des services qui ont fait l'objet de mesures de lutte ou qui devraient faire l'objet d'investigations. La volonté première de l'agence gouvernementale est de faire réagir les opérateurs de ces marchés, mais également de mobiliser les gouvernements locaux. La liste autorise des actions de plaidoyer de la même manière que le rapport 301. Il s'agit également d'alerter les consommateurs sur la nécessité de prendre leurs distances vis-à-vis de ces services illicites et des risques qu'ils peuvent encourir en les utilisant. La liste est publiée et actualisée chaque année.

Tous les acteurs prenant part, de manière directe ou indirecte, à la commission d'acte de contrefaçon peuvent être listés.

Le rapport met chaque année en lumière une problématique spécifique, laquelle peut être un défi particulier dans la lutte contre la contrefaçon ou un nouveau mode de piratage tel que le *stream ripping*, qui a ainsi fait l'objet d'un focus dédié dans le rapport de 2018^[19]. Le rapport 2017 de l'USTR^[20] a pour sa part consacré un focus aux « *Illicit Streaming Devices* » ou ISD, vocable spécifique créé par les anglo-saxons pour désigner les

divers terminaux configurés pour faciliter le piratage. Aux États-Unis, 6,5 % des foyers se seraient équipés de tels terminaux, 106 millions d'utilisateurs auraient un abonnement à un service de télévision illicite, cette tendance étant à la hausse. Les rapports suivants continuent de s'inquiéter de l'utilisation de ces terminaux et mentionnent les actions pénales conduites dans le monde contre les réseaux rediffusant illégalement des chaînes de télévision, les revendeurs d'applications ou de boîtiers configurés. Les différents rapports s'intéressent également aux actions menées par les bureaux d'enregistrement de noms de domaine, qui maintiennent leurs efforts pour lutter contre les abus, notamment les enregistrements de noms de domaine associés à des sites contrefaisants. Le rapport met également souvent l'accent sur les revenus tirés du piratage.

Depuis plusieurs années, les rapports de l'USTR mentionnent ainsi le fait que les services listés, en plus de faciliter les infractions aux droits d'auteur, peuvent se révéler dangereux pour les internautes : exploitation de leurs données personnelles, atteintes à leur matériel informatique, plusieurs sources étant citées à l'appui^[21]. Les éléments portés à la connaissance du public sur chacun des services listés impliquent d'ailleurs, pour nombre d'entre eux, un point sur les virus qu'ils sont susceptibles de véhiculer. C'est donc logiquement que le rapport pour l'année 2019^[22] consacre son focus aux virus présents sur les sites et services dédiés au piratage. Ce point avait déjà été abordé au sujet de plusieurs sites, dont l'hébergeur de fichiers localisé en France *1Fichier*, listé depuis plusieurs années par l'USTR. Le rapport indique que le seul moyen d'éviter d'être contaminé par ces virus, présents aussi bien dans les applications que dans les publicités figurant sur les sites de piratage, est de consommer légalement.

Les éditions 2019 et 2020 ont également insisté sur la complexité de l'écosystème du piratage et le rôle déterminant joué par chacun de ces acteurs (les bureaux d'enregistrement de noms de domaine, les fournisseurs de services d'hébergement, les annonceurs et les réseaux de placement publicitaire, les acteurs du paiement, les réseaux sociaux et les moteurs de recherche), lesquels peuvent grandement contribuer à faciliter ou réduire le piratage. Ainsi, pour la première fois, une régie publicitaire, Propeller Ads, a été identifiée en 2019 comme un marché notoire pour son rôle dans le financement des sites de piratage. En 2020, c'est le réseau publicitaire RevenueHits, basé en Israël, qui est

[19] <https://ustr.gov/sites/default/files/2016-Out-of-Cycle-Review-Notorious-Markets.pdf>

[20] <https://ustr.gov/sites/default/files/files/Press/Reports/2017%20Notorious%20Markets%20List%201.11.18.pdf>

[21] Digital Citizens Alliance, « *Enabling Malware* », July 2016:

http://www.digitalcitizensalliance.org/clientuploads/directory/Reports/2017_7The_Gateway_Trojan.pdf

<http://www.pandasecurity.com/mediacenter/src/uploads/2017/02/Pandalabs-2017-Predictions-en.pdf>

https://www.symantec.com/security_response/publications/monthlythreatreport.jsp

[22] https://ustr.gov/sites/default/files/2019_Review_of_Notorious_Markets_for_Counterfeiting_and_Piracy.pdf

listé et présenté comme l'un des réseaux publicitaires les plus populaires parmi les sites pirates, en particulier les plateformes d'hébergement de fichiers, la plupart de ses publicités visant un public européen.

Cette initiative porte ses fruits. Certes la « *Notorious Markets List* » n'a pas ou peu d'impact sur les protagonistes les plus aguerris, mais des opérateurs de marché mineurs ou qui considéraient leurs activi-

tés comme un simple moyen de gagner de l'argent ont cessé leurs activités. Surtout, l'impact le plus important de la liste concerne les services légitimes qui tolèrent ce type d'agissement, et avec lesquels l'administration américaine travaille afin qu'ils concluent des accords. La liste est également utilisée pour engager des discussions avec les intermédiaires de l'écosystème de la contrefaçon tels que les services de paiement.

LES ACTIONS VISANT À RESPONSABILISER LES PLATEFORMES DE PARTAGE DE CONTENUS

Il ressort du rapport du Bureau du droit d'auteur précité que les titulaires de droits ont manifesté le souhait d'avoir une disposition similaire à celle de l'article 17 de la nouvelle directive sur le droit d'auteur. Le Bureau du droit d'auteur considère qu'une telle modification nécessiterait une réforme de fond du régime de responsabilité actuelle, laquelle pourrait limiter la liberté d'expression ainsi qu'avoir des conséquences néfastes sur la concurrence. Il est donc estimé que ces questions nécessiteraient davantage de recherches pour que le Congrès les examine. Comme indiqué précédemment, la première ébauche de réforme du DMCA publiée en décembre 2020 formule différentes pistes de réforme, et propose notamment d'introduire une obligation de « *stay down* » pour les plateformes, sans préciser les moyens à utiliser à cette fin.

Le rapport indique également qu'il faudrait notamment trouver un équilibre entre l'interdiction de faire peser une obligation générale de surveillance sur les opérateurs et un « devoir limité de recherche » sur les services en ligne qui ne correspond ni à la connaissance réelle ni à la surveillance proactive. Le Congrès est ainsi invité à actualiser le texte de loi pour refléter cela, la norme devant être suffisamment flexible pour s'adapter aux différents types et tailles de fournisseurs de services en ligne. En outre, s'agissant des profits tirés des activités illicites, le rapport indique qu'une interprétation actualisée de cette notion pourrait consister à examiner si l'existence de matériel de contenus illicites constitue la raison principale de l'attrait du service pour ses utilisateurs.

Le Bureau du droit d'auteur propose d'examiner les moyens de faciliter de nouvelles initiatives volontaires pour lutter contre les infractions en ligne, ainsi que pour aider à identifier un standard de mesures techniques d'identification qui peuvent être adoptées dans certains secteurs. Il est également suggéré que le *National Institute of Standards and Technology*, une agence gouvernementale, dirige un groupe de travail multipartite à cet effet.

S'agissant du bénéfice des exceptions, le rapport relève que la jurisprudence a statué qu'un titulaire de droits doit tenir compte des cas possibles de *fair use*^[23] (une forme d'équivalent dans la *common law* des exceptions au droit d'auteur) lorsqu'il notifie un contenu qu'il estime illicite. Cette décision a suscité beaucoup de controverses, notamment sur le rôle des outils de détection et de reconnaissance des contenus, et sur leur capacité (ou non) à identifier des cas de *fair use*. Le rapport préconise ainsi que le Congrès surveille l'impact de cette jurisprudence, en particulier pour les ayants droit, et envisage toute clarification qui pourrait s'avérer nécessaire.

[23] *Lenz v. Universal Music Corp.*, 815 F.3d 1145, 1154–55 (9th Cir. 2016), cert.denied sub nom., *Universal Music Corp. v. Lenz*, 137 S. Ct. 2263 (2017).
<http://cdn.ca9.uscourts.gov/datastore/opinions/2015/09/14/13-16106.pdf>

S'agissant des demandes de retrait notifiées aux plateformes par les ayants droit et de la possibilité que ces notifications soient contestées en justice, le Bureau du droit d'auteur recommande :

- que les normes minimales requises pour formuler les demandes de retrait ne soient plus prévues par la loi mais déterminées par voie réglementaire, ce qui permettrait au Bureau de fixer des règles plus souples et d'éviter à la loi de devenir obsolète face aux évolutions techniques ;
- de raccourcir les délais de traitement des litiges portant sur des contenus notifiés par les ayants droit en adoptant un processus de règlement alternatif des litiges, tel que l'arbitrage, comme alternative plus rapide et moins coûteuse aux poursuites engagées devant les tribunaux.

Il faut également relever que le plan d'action publié en 2020 indique que le retrait de certains contenus protégés par le droit d'auteur, tels que les retransmissions de rencontres sportives, doit pouvoir intervenir en quelques minutes pour empêcher un préjudice économique substantiel. Dans ce contexte, il est annoncé qu'il sera essentiel d'examiner et d'adopter de nouvelles technologies, notamment les technologies de reconnaissance de contenus et l'intelligence artificielle, afin d'améliorer l'identification et le retrait rapide de ces contenus.

Enfin, une loi, promulguée en décembre 2020, prévoit qu'un tribunal rattaché au Bureau du droit d'auteur sera chargé de résoudre les conflits portant sur des montants peu importants (« *small claims* »). Les moyens à engager pour saisir ce tribunal seraient bien inférieurs aux montants qu'il faut engager pour saisir un tribunal classique, car se déroulant en dehors des tribunaux fédéraux. Le montant des dommages-intérêts octroyés serait compris entre à peu près 11 000 et 26 000 euros. Ce tribunal pourrait notamment permettre de résoudre les litiges relatifs aux utilisations illicites de photographies et de musiques sur internet, tout comme les litiges en rapport avec des demandes de retrait auprès de plateformes telles que YouTube. Certains craignent par ailleurs qu'il ne soit utilisé pour agir à l'encontre des internautes ayant partagé illicitement des contenus sur internet.

FRANCE

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

65,3 POPULATION^[1]
en millions

83,3 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

4,1 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

75 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



Le dispositif français de lutte contre le piratage s'articule depuis 2009 autour d'outils complémentaires mis en œuvre par une autorité publique dédiée, la Haute autorité pour la diffusion des œuvres et la protection des droits sur internet (Hadopi), et d'un dispositif permettant aux ayants droit du secteur culturel d'obtenir en justice des mesures de blocage et de déréférencement. Des discussions parlementaires autour d'un projet de réforme d'envergure du dispositif de lutte contre le piratage sont actuellement en cours.

Dans le cadre de l'exercice de ses missions, l'Hadopi publie différentes études, et des indicateurs détaillés et une analyse approfondie des usages des internautes en France, reposant à la fois sur des données d'audience fournies par Médiamétrie et des études d'usages menées auprès des internautes, de façon à mesurer avec précision ces usages et leurs différentes composantes. Ces études sont consultables sur son site internet hadopi.fr. À noter que certains écarts peuvent apparaître entre les chiffres publiés par l'Hadopi et ceux proposés plus hauts par MUSO en raison d'approches méthodologiques et de niveaux de détail différents.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

LES ACTIONS VISANT LES INTERNAUTES

LE DISPOSITIF DE RÉPONSE GRADUÉE

LA GENÈSE DE LA RÉPONSE GRADUÉE

La loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet^[4] (dite « Hadopi 1 ») a permis la création du dispositif dit de réponse graduée, dont l'objectif était de fournir une réponse pénale adaptée au phénomène de piratage massif, à l'époque essentiellement cantonné à une technologie donnée, le pair à pair. La création de ce dispositif de pédagogie et de dissuasion s'articule autour de l'obligation du titulaire de l'abonnement internet de veiller à ce que sa connexion ne soit pas utilisée, par lui-même ou par un tiers, pour télécharger ou mettre à disposition sur les réseaux de pair à pair des œuvres protégées par le droit d'auteur ou les droits voisins^[5], désormais sanctionné par une peine dédiée moindre que celle applicable aux faits de contrefaçon^[6].

L'Hadopi est chargée d'envoyer aux abonnés à internet concernés des avertissements lorsqu'elle est saisie de faits susceptibles de constituer un manquement à l'obligation faite à tout abonné de veiller à l'usage licite de son accès à internet. Le juge judiciaire peut prononcer des sanctions, au titre de la contravention

dite de négligence caractérisée^[7] qui punit l'absence de sécurisation de son accès internet par le titulaire de l'abonnement, lorsque celui-ci a été utilisé pour partager illicitement des œuvres.

LES AJUSTEMENTS RÉGLEMENTAIRES POSTÉRIEURS À LA CRÉATION DU DISPOSITIF

Une seule peine de suspension de l'accès à internet a été prononcée en 2013 à l'encontre d'une personne ayant fait défaut devant le tribunal. Cristallisant de nombreuses critiques contre l'institution et le dispositif de réponse graduée, cette peine a finalement été abrogée par un décret du 8 juin 2013. Les abonnés avertis par l'Hadopi dont l'accès continuerait néanmoins d'être utilisé à plusieurs reprises pour commettre des actes de contrefaçon n'encourent donc plus qu'une peine d'amende, prononcée par le juge pénal, pouvant aller jusqu'à 1 500 euros.

À la suite d'une procédure initiée par un fournisseur d'accès à internet, le Conseil d'État a condamné l'État en 2015 à indemniser les fournisseurs d'accès à internet pour les identifications réalisées dans le cadre de la réponse graduée et l'a enjoint à publier un décret fixant les conditions futures de cette compensation.

[4] <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020735432/>

[5] 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. »

[6] L'obligation de sécuriser sa connexion internet a été créée par la loi n° 2006-961 du 1^{er} août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information (dite loi « DADVSI »), qui a transposé en droit français la directive 2001/29/CE du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, mais ce n'est qu'à l'occasion de la création de la procédure de réponse graduée que le législateur a accolé une peine dédiée en cas de manquement.

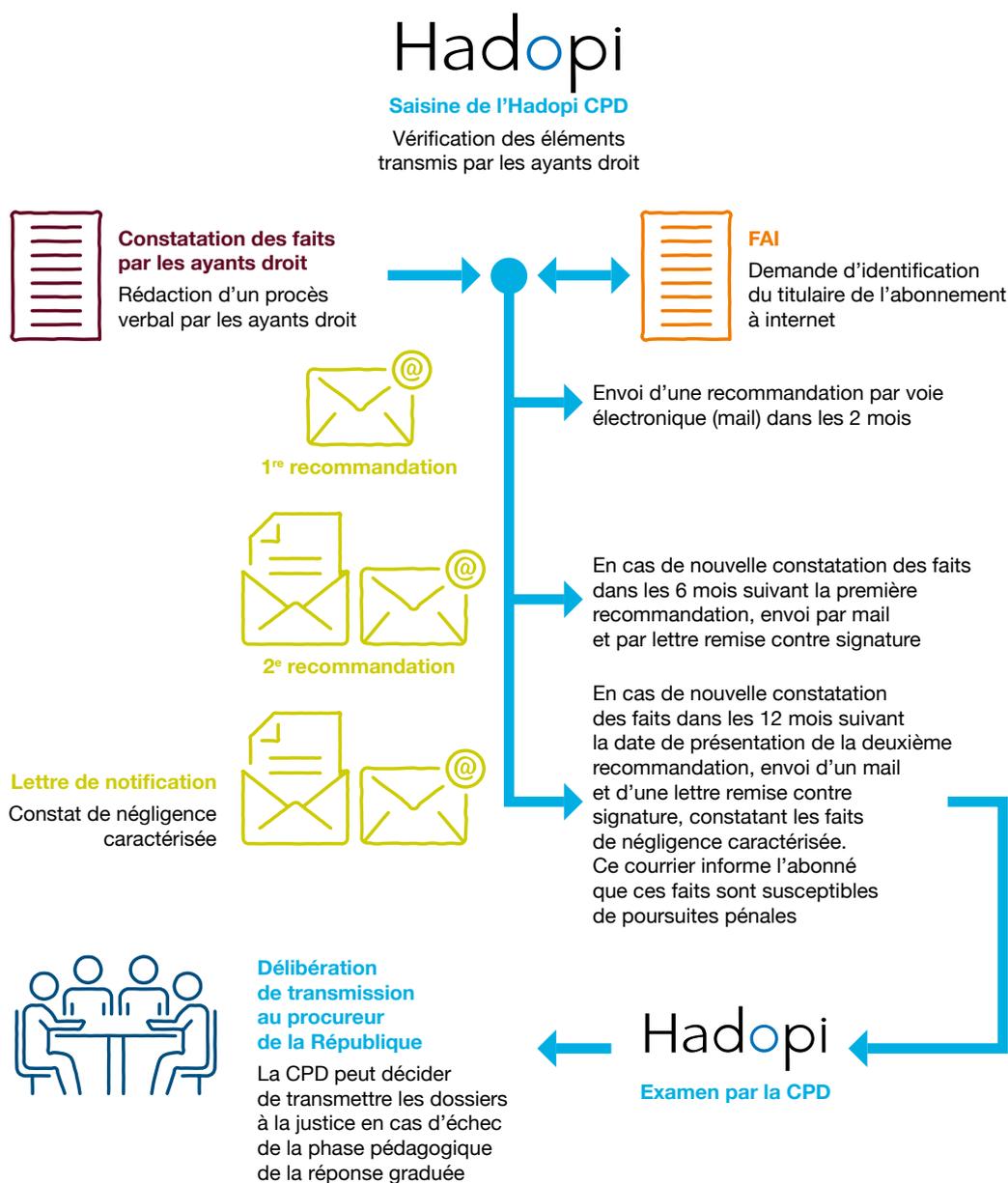
Le projet de loi DADVSI avait déjà prévu de sanctionner par une contravention spécifique les actes de contrefaçon commis au moyen d'un logiciel d'échange de pair à pair. La disposition a toutefois été censurée par le Conseil constitutionnel qui, dans une décision du 27 juillet 2006, a considéré « qu'au regard de l'atteinte portée au droit d'auteur ou aux droits voisins, les personnes qui se livrent, à des fins personnelles, à la reproduction non autorisée ou à la communication au public d'objets protégés au titre de ces droits sont placées dans la même situation, qu'elles utilisent un logiciel d'échange de pair à pair ou d'autres services de communication au public en ligne » (<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT00000460053>). Au lendemain de la promulgation de la loi DADVSI, le partage illicite d'œuvres protégées ne pouvait donc être sanctionné que sur le fondement du délit de contrefaçon (3 ans d'emprisonnement et 300 000 euros d'amende). À la suite de cette décision, la ministre de la Culture et de la Communication lance en 2007 une mission sur la lutte contre le téléchargement illicite et le développement des offres légales d'œuvres musicales, audiovisuelles et cinématographiques. Cette mission confiée à Denis Olivennes aboutit, le 23 novembre 2007, à la conclusion des accords dits « de l'Élysée » entre les ayants droit, les prestataires techniques et les pouvoirs publics, qui entendent « tout à la fois favoriser l'offre légale de contenus sur internet au profit des consommateurs et mettre en œuvre, dans le respect des libertés individuelles, des mesures originales de prévention du piratage ». Les pouvoirs publics s'engagent ainsi à soumettre au Parlement un mécanisme d'avertissement préalable et de sanction visant à dissuader les atteintes aux droits de la propriété intellectuelle sur les réseaux numériques résultant de formes de partage non autorisées mises en œuvre par l'intermédiaire d'une autorité publique dédiée.

[7] Décret n° 2010-695 du 25 juin 2010 instituant une contravention de négligence caractérisée protégeant la propriété littéraire et artistique créant l'article R. 335-5-I du code de la propriété intellectuelle : « 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. [...] »

LA MISE EN ŒUVRE DU DISPOSITIF DE RÉPONSE GRADUÉE

SCHÉMA DE LA RÉPONSE GRADUÉE



Source : Hadopi

En pratique, à l'issue de la phase pédagogique de la procédure, l'Hadopi (via une entité interne dédiée, la Commission de protection des droits, composée de magistrats) décide de transmettre au procureur de la République compétent, en vue d'éventuelles poursuites pénales, les dossiers comportant des réitérations malgré les avertissements.

Les peines contraventionnelles d'amende prononcées sont généralement comprises entre 50 et 1 000 euros. Elles sont assorties ou non de sursis, en fonction de la

situation de la personne condamnée et des éléments présentés à l'audience. L'auteur de l'infraction peut également être condamné à réparer le préjudice subi par les ayants droit à l'origine des saisines de l'Hadopi et dont les œuvres ont été mises en partage. Dans ce cas, le montant des dommages et intérêts est, en général, de l'ordre d'une centaine d'euros par œuvre mise à disposition.

Près de 80 % des suites judiciaires sont des réponses pénales qui se traduisent, à l'égard des titulaires

d'abonnement, par le prononcé de peines d'amende et de mesures alternatives aux poursuites, ces dernières prenant le plus souvent la forme d'un rappel à la loi.

LA CONFORTATION DU DISPOSITIF DE RÉPONSE GRADUÉE

Par une décision du 20 mai 2020^[8], le Conseil constitutionnel s'est prononcé sur la conformité de certaines dispositions du code de la propriété intellectuelle aux droits et libertés garantis par la Constitution. Il a ainsi jugé conformes les dispositions législatives permettant aux membres de la Commission de protection des droits et aux agents assermentés de l'Hadopi d'obtenir des opérateurs de communications électroniques l'identité, l'adresse postale, l'adresse électronique et les coordonnées téléphoniques de l'abonné dont l'accès à internet a été utilisé pour commettre des actes de contrefaçon, rappelant que ces informations limitées aux données d'identification sont recueillies par des agents assermentés soumis au secret professionnel et sont nécessaires à la mise en œuvre de la procédure de réponse graduée. En revanche, ont été censurées les dispositions qui prévoyaient la possibilité pour les membres de la Commission et ses agents assermentés d'obtenir « *tous documents, quel qu'en soit le support, y compris les données conservées et traitées par les opérateurs de communications électroniques* », lesquelles n'étaient du reste pas utilisées en pratique.

Par cette déclaration de conformité, le Conseil constitutionnel a validé le fonctionnement actuel de la procédure de réponse graduée et la poursuite de sa mise en œuvre, conformément au droit au respect de la vie privée et à la protection des données à caractère personnel.

LE BILAN DE LA RÉPONSE GRADUÉE ET LES PISTES DE RÉFORME

Depuis la création de l'Hadopi jusqu'à la fin de l'année 2020, plus de 13 millions de recommandations, toutes phases confondues, ont été envoyées aux titulaires d'abonnement en raison de téléchargements et mises à disposition illicites constatés à partir de leur connexion internet. Ainsi, en 2020, 11 % des Français de 15 ans et plus ont déjà reçu une recommandation, pour 80 % d'entre eux il s'agissait d'une première recommandation, 21 % d'une seconde recommandation, 6 % d'une notification.

L'impact sur les comportements des internautes est significatif : près des deux tiers (63 %) des internautes ayant reçu une recommandation disent avoir diminué leur consommation illicite de biens culturels dématérialisés

et plus d'un tiers d'entre eux (34 %) déclarent s'être tournés vers les offres légales, suite à l'envoi de cette recommandation.

Cela correspond à près de 4 millions de Français qui auraient diminué leur consommation illicite et plus de 2 millions qui se seraient tournés vers les offres légales suite à la réception d'une recommandation de l'Hadopi.

Le volet pédagogique de la procédure est essentiel et porte ses fruits dans des proportions appréciables. Dans plus de 70 % des cas, et à chaque étape de la procédure, aucune réitération des faits n'est constatée : sur 10 personnes averties, 7 prennent des mesures pour éviter tout renouvellement d'actes de piratage.

En cas de persistance des faits et de caractérisation de la négligence, le recours au volet pénal demeure nécessaire. À l'issue de la troisième phase, l'autorité judiciaire peut être saisie par l'Hadopi en vue d'une sanction pénale. Depuis le lancement du dispositif en 2010, près de 7 000 dossiers ont été transmis par l'Hadopi aux procureurs de la République aux fins de poursuites pénales, donnant lieu à un nombre de réponses pénales croissant et de natures variées. Dans le cadre des débats sur le projet de loi relatif à la communication audiovisuelle et à la souveraineté culturelle à l'ère numérique initié en 2019, ainsi qu'à l'occasion de réflexions plus spécifiques visant à renforcer l'efficacité de la procédure de réponse graduée, la question de l'introduction d'un pouvoir de transaction pénale au profit de l'Hadopi a pu être posée. Un tel pouvoir, selon ses défenseurs, serait de nature, en donnant à la réponse pénale un caractère plus certain, à en améliorer l'effet dissuasif et donc à accroître la portée des avertissements adressés aux internautes contrevenants lors de la phase pédagogique de la procédure de réponse graduée.

LA PROMOTION DE L'OFFRE LÉGALE

Le législateur, en créant l'Hadopi, s'est montré attentif à assurer un juste équilibre entre créateurs et usagers des œuvres, et tend, en parallèle de sa mission de lutte contre le piratage, à favoriser le développement d'une offre culturelle diversifiée et accessible.

Le code de la propriété intellectuelle confie ainsi à l'Hadopi une mission d'« *encouragement au développement de l'offre légale* », au titre de laquelle elle est chargée de délivrer un label aux offres légales et d'en publier la liste. L'objectif est double : il s'agit d'une part de renseigner les consommateurs qui peinent souvent

[8] Décision n° 2020-841 qpc du 20 mai 2020 : <https://www.conseil-constitutionnel.fr/decision/2020/2020841QPC.htm>

à juger de la légalité d'une offre en ligne et de les diriger vers ces offres, et d'autre part de valoriser les offres se montrant respectueuses du droit d'auteur.

Au fil du temps, ce label s'est cependant avéré peu attractif avec une baisse du nombre de demandes. Sa faible attractivité peut s'expliquer par l'absence de contrepartie à son attribution et par la complexité de la procédure de labellisation, qui prévoit que la plateforme doit être elle-même initiatrice de la démarche et accepter la publication de son catalogue sur le site de la Haute Autorité pendant un mois. De ce fait, depuis 2013, la Haute Autorité référence également les offres respectueuses des droits de propriété intellectuelle^[9].

Les éléments d'observation pris en compte dans le cadre de ce référencement sont notamment le nombre de demandes de notification et retrait accessibles publiquement, le référencement par d'autres organismes publics, la présence de mentions légales et de conditions générales de vente mettant en avant le respect du droit d'auteur, l'accès à un système de paiement sécurisé pour les offres payantes, l'absence d'environnement présentant une dangerosité (publicité répréhensible, virus, etc.), la revendication par le site lui-même de sa licéité et de l'efficacité de ses systèmes de notification.

Au 31 décembre 2020, l'Hadopi recensait, via son portail de l'offre légale, 423 sites et services légaux répartis en huit catégories, correspondant aux différents types de biens culturels.

Par ailleurs, depuis 2015, le Centre national du cinéma et de l'image animée propose également un moteur de recherche pour les œuvres audiovisuelles^[10].

Enfin, a été mis en place depuis 2014 un service permettant aux internautes de signaler toute œuvre culturelle introuvable en ligne. L'Hadopi répond en orientant les internautes vers des sites licites ou en sensibilisant les ayants droit sur l'indisponibilité de certaines œuvres.

Cette approche novatrice de l'Hadopi a été actée par le projet de réforme, qui devrait supprimer le label et entend adopter une approche souple de la mission du régulateur s'agissant de la promotion de l'offre légale, chargeant celui-ci de prendre « *toute mesure, notamment par l'adoption de recommandations, de guides de bonnes pratiques, de modèles et clauses types ainsi que de codes de conduite* »

et de mettre en place « *des outils visant à renforcer la visibilité et le référencement de l'offre légale auprès du public* ».

LES ACTIONS DE SENSIBILISATION

L'Hadopi a développé de nombreux outils afin de sensibiliser les internautes aux pratiques culturelles responsables : kit à l'intention des professionnels offrant un accès internet^[11], fiches pratiques^[12] et vidéos tutorielles^[13].

L'Hadopi a tout particulièrement axé ses efforts de sensibilisation sur les jeunes publics au regard des récentes études consacrées aux pratiques culturelles des 8-14 ans et aux risques subis par cette population. D'autant plus que les actions de l'Hadopi s'inscrivent dans le respect du code de l'éducation qui prévoit que les élèves soient sensibilisés au respect du droit d'auteur et à la disponibilité des offres légales.

Dans cette optique, elle propose ainsi depuis 2012 des ateliers d'information et de sensibilisation destinés au jeune public et à la communauté éducative. En 2018, l'Hadopi a créé des modules pédagogiques à l'attention des élèves des écoles élémentaires, collèges et lycées qui ont été largement diffusés, notamment grâce à des interventions en classe assurées en collaboration avec l'association Génération Numérique. La conception et la diffusion de ces modules pédagogiques, comme des futurs outils de sensibilisation à destination des publics scolaires, ont fait l'objet de la signature d'une convention en 2019 entre le ministère de l'Éducation nationale et l'Hadopi.

Depuis 2018, plus de 400 interventions ont permis de sensibiliser environ 12 500 élèves de tous niveaux scolaires.

En décembre 2020, l'Hadopi a lancé, en partenariat avec le CNC, une campagne de communication intitulée « *On a tous de bonnes raisons d'arrêter de pirater* »^[14]. Cette campagne est destinée au grand public – notamment les plus jeunes – et valorise l'expérience des utilisateurs des plateformes d'offre légale. En prise avec les usages observés par l'Hadopi, au ton volontairement positif, elle est portée par de jeunes artistes vidéastes.

[9] <https://www.hadopi.fr/en/node/143>

[10] https://www.cnc.fr/cinema/actualites/toute-loffre-legale-francaise-en-deux-clics_134335

[11] <https://www.hadopi.fr/en/node/3634>

[12] <https://www.hadopi.fr/en/node/164>

[13] <https://www.hadopi.fr/en/node/166>

[14] <https://www.hadopi.fr/actualites/campagne-nationale-tous-de-bonnes-raisons-darreter-de-pirater>

En janvier 2021, la Commission nationale de l'informatique et des libertés (CNIL), le Conseil supérieur de l'audiovisuel (CSA), le Défenseur des droits et l'Hadopi ont créé un kit pédagogique, qui regroupe l'ensemble des ressources conçues pour l'éducation du citoyen numérique, à destination des formateurs et des parents qui accompagnent les jeunes en matière de numérique^[15].

Le projet de réforme devait entériner l'approche proactive de l'Hadopi en matière de sensibilisation, chargeant expressément l'autorité publique d'une « mission de prévention et d'information auprès de tous les publics, notamment des plus jeunes, sur les risques et les conséquences du piratage d'œuvres protégées par le droit d'auteur et de contenus sportifs ».

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES MESURES JUDICIAIRES DE BLOCAGE ET DE DÉRÉFÉREMENT

LE DROIT POSITIF

En 2009, le législateur a créé l'article L. 336-2 du code de la propriété intellectuelle, qui permet aux ayants droit d'obtenir en justice « toutes mesures propres à prévenir ou à faire cesser une atteinte au droit d'auteur [...] à l'encontre de toute personne susceptible d'y remédier »^[16].

Sur ce fondement a été prononcé pour la première fois, en novembre 2013^[17], le blocage des noms de domaine d'une galaxie de sites ainsi que le déréférencement par les moteurs de recherche.

Le tribunal n'avait en revanche pas mis à la charge des intermédiaires le coût de ces mesures, poussant les ayants droit de l'audiovisuel à faire appel du jugement sur ce point. Ceux-ci ont eu gain de cause en appel, puis en cassation^[18], et la jurisprudence fait depuis peser les coûts des mesures de cessation sur les intermédiaires.

Si initialement les actions se limitaient aux seuls sites d'une même galaxie, c'est-à-dire des sites pour lesquels on pouvait supposer qu'ils avaient des administrateurs communs ou des miroirs de sites visés par la procédure, elles embrassent désormais une pluralité de sites (et leurs différents avatars), regroupés pour les besoins

de la procédure. De plus, elles peuvent non seulement viser des sites de liens vers des contenus disponibles en streaming et de téléchargement direct, ou encore ceux regroupant des liens pair à pair, voire plus récemment un service d'hébergement de fichiers (*cyberlocker*)^[19]. En 2020, les ayants droit de l'audiovisuel ont obtenu pour la première fois le blocage de services IPTV illicites^[20].

Sur le fond, afin de constater l'atteinte au droit d'auteur ou à un droit voisin, le juge se fonde le plus souvent sur différents critères dont notamment : le nombre de visites mensuelles, le type d'œuvres présentes sur le site (film présent en salle, en ligne, etc.), le nombre d'œuvres accessibles, le pourcentage d'œuvres protégées, ou encore les modalités d'accès à des sites (à la suite d'une recherche sur le moteur Google par exemple). La démonstration du caractère massif des actes de contrefaçon sur ces sites et leur caractère exclusivement dédié à la contrefaçon (développée principalement par les ayants droit de l'audiovisuel) est basée sur une méthode probatoire par échantillonnage afin d'obtenir une approche statistique du pourcentage de contenus illicites sur le site.

Une autre approche probatoire a pu être développée par les ayants droit du secteur de l'édition, ceux-ci ayant notamment mis en avant le fait que la plupart de leur catalogue était mise à disposition par les sites dont ils demandaient le blocage^[21].

[15] <https://hadopi.fr/ressources/kit-pedagogique-du-citoyen-numerique-retrouvez-toutes-les-ressources>

[16] La demande pouvant émaner « 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 » et du CNC.

[17] Tribunal de grande instance de Paris, 28 novembre 2013 : <http://www.hadopi.info/dj/news/ressources/2013.11.29%20TGI%20Paris%2029%20novembre%202013.pdf>

[18] Cour de Cassation, 1^{re} chambre civile, 6 juillet 2017 : <http://www.hadopi.info/dj/news/ressources/2017.07.06%20Cass%206%20juillet%202017%20Allotstreaming.pdf>

[19] Tribunal de grande instance de Paris, 17 octobre 2019, N° RG 19/07748 :

<http://www.hadopi.info/dj/news/ressources/2019.10.17%20TGI%20Paris%2017%20octobre%202019%20RG%2019.07748.pdf>

[20] Tribunal judiciaire de Paris, 17 décembre 2020, N° RG 20/10425.

[21] Tribunal de grande instance de Paris, 7 mars 2019, N° RG 18/14194.

Pour appliquer les injonctions émises par la justice dans un délai de 15 jours et pour une durée de 12 à 18 mois – les ordonnances les plus récentes valant pour 18 mois –, les fournisseurs d'accès à internet mettent en œuvre des mesures de blocage DNS.

Les injonctions à l'encontre des fournisseurs d'accès à internet ne sont pas dynamiques. Elles sont limitées aux seuls domaines ou chemins d'accès identifiés dans les conclusions des ayants droit. Il est cependant possible d'en demander l'actualisation devant le juge des référés pendant le délai restant à courir^[22]. Une nouvelle procédure devra être intentée à l'échéance de l'injonction pour obtenir le renouvellement du blocage. Une certaine forme de dynamisme a cependant été introduite par la jurisprudence. Tout d'abord, le juge a fait droit à la demande de fournisseurs d'accès à internet demandant à être notifiés par les ayants droit des sites bloqués qui seraient devenus inactifs ou qui cesseraient d'être contrefaisants pendant la durée des mesures de blocage prévues par l'injonction, afin d'éviter des frais inutiles^[23]. Plus récemment, les ayants droit ont obtenu de pouvoir à leur tour notifier aux fournisseurs d'accès à internet les sites débloqués qui auraient recommencé leur activité illicite^[24].

S'agissant des moteurs de recherche, une décision de décembre 2017^[25] les a contraints à procéder au déréférencement de l'ensemble des chemins d'accès aux sites litigieux qu'il est en capacité d'identifier techniquement et non uniquement les chemins d'accès précisément visés dans la décision à intervenir. Il résulte toutefois de la jurisprudence récente que les décisions de blocage ne visent désormais plus les moteurs de recherche en même temps que les fournisseurs d'accès à internet, les demandes d'injonctions de déréférencement de sites étant, le cas échéant, formées par les ayants droit dans le cadre de procédures simplifiées et dédiées à cette seule demande.

LE BILAN DES PROCÉDURES DE BLOCAGE ET LE PROJET DE RÉFORME

L'Hadopi a souhaité analyser l'impact des jugements ordonnant des mesures de blocage sur l'accès aux galaxies de sites visées et sur les comportements des internautes les utilisant.

Une étude a ainsi été réalisée et, à la suite des deux décisions de justice du 14 décembre 2018 dans des procédures initiées par les ayants droit de l'audiovisuel

portant sur le blocage de 38 noms de domaine relatifs à 11 galaxies de sites illicites^[26], une analyse de l'audience de ces sites a ainsi été réalisée à partir des données d'audience fournies par Médiamétrie NetRatings, sur une période de trois mois, entre décembre 2018 et février 2019, ainsi qu'une mesure de l'audience des sites sur lesquels se sont reportés les internautes ayant visité les sites concernés par les décisions de justice. Cette analyse a été faite à panel constant, c'est-à-dire en considérant la seule part des internautes ayant visité les sites illicites par les noms de domaine bloqués en application de la décision de justice.

Il ressort tout d'abord que les mesures de blocage de noms de domaine génèrent une baisse brutale de l'audience des galaxies de sites illicites concernés : la part d'audience des galaxies de sites provenant de manière cumulée des 34 noms de domaine étudiés est passée de 3,8 millions de visiteurs uniques en décembre 2018 (avant l'application des décisions de justice) à 1,2 million en février 2019, soit une baisse de 68 %.

Leur audience venant de ces noms de domaine bloqués n'est cependant pas réduite à néant : environ 590 000 internautes ont continué à accéder à la galaxie via les noms de domaine bloqués entre décembre 2018 et février 2019, en contournant les mesures de blocage (*via* le recours à un DNS alternatif, par exemple). Par ailleurs, 612 000 nouveaux internautes ont pu accéder aux galaxies, dans les mêmes conditions (*via* des redirections automatiques par exemple).

Mais au final, 84 % des internautes qui se rendaient sur un des sites *via* un des noms de domaine bloqués par les jugements ne l'utilisaient plus en février 2019.

Cependant, bien que ces 84 % d'internautes n'utilisent plus ces noms de domaine, ils ont continué, pour 57 % d'entre eux, à se rendre sur au moins un autre site illicite après les mesures de déréférencement et blocage. Parmi ces derniers, 22 % d'entre eux continuent à se rendre sur l'une des galaxies de sites visées par les jugements *via* un autre nom de domaine non bloqué.

Enfin, 37 % de ces internautes qui n'ont plus utilisé les noms de domaine bloqués se sont rendus sur un site légal payant, soit 1,2 million d'internautes. En particulier, 7 % de ces internautes sont devenus de nouveaux utilisateurs de l'offre légale payante audiovisuelle, à laquelle ils n'avaient jamais eu recours.

[22] Tribunal de grande instance de Paris, 14 décembre 2018.

[23] Tribunal de grande instance de Paris, 14 décembre 2018, n° RG 18/10597 et n° RG 18/106.

[24] Tribunal judiciaire de Paris, 18 décembre 2020, N° RG 20/10567.

[25] Tribunal de grande instance de Paris, 15 décembre 2017 :

<http://www.hadopi.info/dj/news/ressources/2017.12.15%20TGI%20Paris%2015%20d%3%a9cembre%202017.pdf>

[26] <https://cdn2.nextinpact.com/medias/voirfilm-libertyland-streamcomplet.pdf> et <https://cdn2.nextinpact.com/medias/tgi-paris-14-12-2018.pdf>

Les mesures de blocage illicites présentent une réelle efficacité, la part d'audience des galaxies de sites correspondant aux noms de domaine bloqués voyant leur audience diminuer drastiquement dans les mois suivant les décisions. L'analyse des reports d'audience montre cependant que si une part de leurs utilisateurs se tournent alors vers l'offre légale, une proportion plus importante poursuit sa consommation délictueuse en recourant à des sites illicites appartenant aux galaxies des sites visés par la décision de justice. Il apparaît ainsi que l'efficacité des mesures de blocage serait renforcée par l'actualisation régulière des mesures de blocage afin que celles-ci visent l'ensemble des sites d'une même galaxie.

Il faut en outre constater que les délais pour obtenir des mesures de blocage demeurent relativement longs. En effet, il s'est écoulé en moyenne 97 jours ouvrés entre l'assignation et la décision du juge pour les décisions rendues depuis juillet 2017 ; 85,5 jours pour les renouvellements des mesures de blocage une fois le terme de l'injonction initiale échue et 33 jours pour les 3 demandes d'actualisation des mesures de blocage obtenues en référé pour le temps de l'injonction restant à courir. À ces délais, il faut ajouter le temps nécessaire à la réunion des preuves destinées à prouver l'illicéité des sites en cause. Les ayants droit de l'audiovisuel dressent notamment des procès-verbaux qui permettent de caractériser l'illicéité des contenus présents sur les différents sites concernés ; la démonstration du caractère massif des actes de contrefaçon sur ces sites et leur caractère exclusivement dédié à la contrefaçon est basée sur une méthode probatoire par échantillonnage – développée par l'Association de lutte contre la piraterie audiovisuelle (ALPA) – afin d'obtenir une approche statistique du pourcentage de contenus illicites sur chaque site.

Le projet de réforme propose ainsi de renforcer la portée des mesures prononcées par le juge à l'encontre de sites contrefaisants afin de prendre en compte le phénomène dit de « sites miroirs ». L'autorité publique devait se voir confier le pouvoir, sur saisine des ayants droit, de demander le blocage ou le déréférencement d'un site jugé illicite en application d'une décision initiale du juge. En complément, l'autorité devait élaborer des modèles d'accord type à destination des parties prenantes, aux fins d'exécuter de manière dynamique ladite décision judiciaire.

LA LUTTE CONTRE LE PIRATAGE DE CONTENUS SPORTIFS

Les organisateurs de manifestations sportives en France ne disposent pas, en l'état du droit positif, d'une procédure judiciaire *sui generis* leur permettant d'obtenir des mesures de blocage susceptibles de pouvoir intervenir en direct (à l'occasion de la retransmission d'un match) afin de lutter efficacement contre le piratage de leurs contenus.

Le projet de réforme prévoit de consacrer, dans le code du sport, une procédure spécifique de blocage adaptée aux problématiques spécifiques du piratage sportif.

Le dispositif a pour objectif de permettre aux ayants droit concernés :

- d'obtenir, dans le cadre d'une procédure unique, le prononcé d'une décision dynamique permettant d'étendre l'efficacité des mesures de blocage ou de déréférencement des sites ou services pirates identifiés au jour de la décision à d'autres sites ou services susceptibles d'apparaître pendant la durée de la compétition, étant précisé que les mesures peuvent être mises en œuvre selon un calendrier prévisionnel calqué sur le calendrier officiel de la compétition ;
- de s'appuyer sur un régulateur jouant un rôle de tiers de confiance pour faciliter l'identification des sites ou services pirates, notamment des services miroirs.

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

Sous l'impulsion du ministère de la Culture et de la Communication, les acteurs de la publicité ont signé le 23 mars 2015 une « charte des bonnes pratiques pour le respect du droit d'auteur », suivie du lancement d'un comité de suivi des bonnes pratiques dans les moyens de paiement en ligne pour le respect du droit d'auteur et des droits voisins.

Le projet de réforme prévoit l'établissement, après une procédure contradictoire, d'une liste des sites portant atteinte de manière grave et répétée au droit d'auteur et aux droits voisins. Cette liste a vocation à permettre de sécuriser les actions d'autorégulation de la part de divers intermédiaires, tels que les acteurs de paiement et les acteurs de la publicité, et susceptibles d'assécher les ressources des services illicites (approche dite « *Follow the money* »).

LES ACTIONS VISANT À RESPONSABILISER LES PLATEFORMES DE PARTAGE DE CONTENUS

À la suite de l'adoption de la directive 2019/790 sur le droit d'auteur et les droits voisins dans le marché unique numérique, l'Hadopi a conduit conjointement avec le Conseil supérieur de la propriété littéraire et artistique (CSPLA) et le CNC une mission visant à dresser un état des lieux actualisé des outils de reconnaissance de contenus dont certains sont déjà utilisés par ces plateformes, pour reconnaître les contenus des ayants droit, et en bloquer ou monétiser l'accès.

La mission a ainsi été chargée :

- d'évaluer l'efficacité et la pertinence des outils techniques existants ; il s'agira à la fois d'apprécier leur performance en mesurant leurs éventuelles limites, ainsi que leur finesse, en analysant les risques de retraits injustifiés de contenus ;
- de formuler des recommandations sur l'utilisation de ces technologies dans le cadre de la directive sur le droit d'auteur.

Après près d'une soixantaine d'auditions et plus de 200 personnalités rencontrées par les équipes de l'Hadopi, du CSPLA et du CNC, le rapport^[27] de la mission a procédé, sur la base de tests techniques détaillés, à une évaluation approfondie des technologies pertinentes et des outils de reconnaissance existants. Il conclut à leur réelle efficacité, tout en mettant en évidence des points possibles d'amélioration et en offrant une approche prospective du sujet. Sur la base des dizaines d'auditions conduites en France et à l'étranger, ainsi que d'enquêtes d'opinion quantitatives et qualitatives, le rapport dresse un panorama des perceptions et attentes des acteurs, tant utilisateurs qu'ayants droit ou plateformes.

Le rapport esquisse enfin les premières pistes pour une mise en œuvre à la fois ambitieuse et concertée de cet article 17. Bien qu'ayant initialement fait l'objet de débats virulents, l'article 17 semble en réalité éloigner le risque de filtrage généralisé et vise plutôt à pérenniser et encadrer une situation préexistante en permettant une protection renforcée du droit d'auteur, mais également une meilleure prise en compte des équilibres entre protection et usages.

Dans la continuité de ce rapport, une nouvelle mission conjointe a été lancée en avril 2020, notamment afin d'alimenter les « orientations » de la Commission européenne sur ce sujet et la transposition de la directive sur le droit d'auteur en France. Le rapport de cette mission, publié le 19 janvier 2021^[28], souligne le rôle que devront jouer les outils automatiques de reconnaissance des contenus d'ores et déjà déployés sur les plus importantes plateformes. Il précise les modalités d'intervention de ces outils préventifs indispensables à la protection du droit d'auteur et décrit les conditions de l'équilibre à assurer avec les exceptions à ce droit et avec la liberté d'expression, dont le respect peut et doit être assuré sans paralyser pour autant le fonctionnement des outils automatiques. Le rapport plaide pour une lecture rigoureuse du texte de la directive et donne au régulateur un rôle de garant de l'équilibre à instituer entre les droits des différentes parties prenantes : utilisateurs, titulaires de droit d'auteur et plateformes. Seule une telle lecture, qui fait toute leur place aux outils technologiques disponibles, permettra à la directive de produire tous ses effets avec des contenus légaux plus largement disponibles au bénéfice de chacun.

Les propositions présentées s'inscrivent dans cette logique en développant la transparence des pratiques et la responsabilité de tous les acteurs : inscription dans la loi du bénéfice des exceptions, traitement rapide et efficace des plaintes, définition du rôle du régulateur, transparence des algorithmes mis en œuvre par les plateformes et des règles de gestion de droits appliqués, déclinaison fine de la mise en œuvre de la directive aux différents domaines, y compris l'image et l'écrit...

Par ailleurs, le 3 décembre 2020, a été adoptée une loi habilitant le gouvernement à transposer par ordonnance différentes directives et notamment la directive sur le droit d'auteur et les droits voisins dans le marché unique numérique.

[27] <https://hadopi.fr/ressources/etudes/rapport-cspla-hadopi-cnc-vers-une-application-effective-du-droit-dauteur-sur-les>

[28] <https://www.hadopi.fr/ressources/etudes/rapport-cspla-hadopi-cnc-les-outils-de-reconnaissance-des-contenus>

GRÈCE

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

10,4 POPULATION^[1]
en millions

75,67 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

0,51 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

65 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illicites par mode d'accès en %



La Grèce s'est récemment dotée d'un dispositif de notification et de retrait pouvant se conclure par une injonction de blocage administratif (notamment inspiré du système établi en Italie).

Les mesures ciblant les internautes restent peu développées, la loi précisant expressément que le dispositif anti-piratage n'est pas applicable aux infractions commises par des utilisateurs finaux, quelle que soit la technologie utilisée pour partager ou consulter des œuvres.

LES ACTIONS VISANT LES INTERNAUTES

LES ACTIONS DE SENSIBILISATION

En ce qui concerne les initiatives de sensibilisation, l'*Hellenic Copyright Organisation (OPI)* a élaboré au fil du temps une stratégie globale sur le droit d'auteur et l'éducation grâce à la mise en œuvre de programmes éducatifs s'adressant aux éducateurs et aux élèves de l'enseignement primaire et secondaire. En ce qui concerne l'enseignement primaire, les actions conduites ont obtenu le soutien de l'Union européenne, tandis que le programme a également reçu (et reçoit toujours sur une base annuelle) le soutien du ministère de l'Éducation. Un site dédié a été créé^[4].

Enfin, l'initiative la plus récente dans ce domaine concerne la mise en œuvre du programme financé par l'Union européenne intitulé « *Éduquer les jeunes et les enseignants du secondaire au droit d'auteur en Grèce et à Chypre* ». Ce programme a été sélectionné pour financement par l'EUIPO et est conduit avec Chypre. Il prévoit différentes actions comprenant entre autres, la production de matériel informatif et éducatif sur le droit d'auteur destiné aux jeunes et aux élèves de l'enseignement secondaire, et l'organisation de séminaires éducatifs pour les enseignants du secondaire.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] <https://copyrightschool.gr/index.php/en/>

LA PROMOTION DE L'OFFRE LÉGALE

L'OPI a mis en place en août 2019 un portail qui référence les plateformes proposant légalement des

contenus culturels et sportifs en ligne, dans le cadre du projet européen Agorateka^[5] L'OPI envisage à l'avenir de rediriger les utilisateurs vers ce portail en cas de mesure de blocage à l'encontre d'un site.

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES SERVICES ILLICITES ET LEURS OPÉRATEURS

Une décision a été rendue au pénal par la cour d'appel de Komotini en novembre 2019. Elle a fait l'objet d'une large publicité car c'est la première fois qu'une sanction pénale a été prononcée à l'encontre d'un opérateur de sites contrefaisants. Celui-ci a été reconnu coupable de contrefaçon à échelle commerciale et condamné à cinq ans d'emprisonnement.

En septembre 2019, un réseau de piratage IPTV très important a été démantelé. Dans le cadre de cette action policière, les fournisseurs de Xtream Codes, un logiciel apparemment utilisé par plus de 90 % des fournisseurs d'offres IPTV illégales, ont été arrêtés. Ce logiciel, qui permettait de gérer les comptes clients et de générer pour ces derniers les « playlists M3U » individuelles, était utilisé par un nombre très important de revendeurs d'offres IPTV illégales. Ainsi, à la suite de cette opération de police, une baisse temporaire du trafic global de l'IPTV illégale de 50 % aurait été observée. Cette opération a vu intervenir Eurojust et a impliqué les services de police en Italie (pays où a débuté l'enquête), en Bulgarie, en Grèce, aux Pays-Bas, en Allemagne et en France.

LES MESURES ADMINISTRATIVES DE BLOCAGE

En 2017^[6], une réforme législative a introduit une procédure de blocage administratif des sites illicites confiée à l'OPI. Cette procédure a été mise en place pour pallier l'absence de procédures judiciaires favorables aux ayants droit.

La base légale du blocage administratif résulte de la transposition en droit national de la directive dite

« commerce électronique » qui prévoit la possibilité que le blocage soit mis en place par une autorité publique.

En accord avec cette disposition, le nouveau mécanisme de blocage administratif relève d'un texte spécial en matière de droit d'auteur. L'intervention de l'autorité publique s'opère dès le stade des notifications et retraits, et peut se conclure par une injonction de blocage prononcée par l'autorité à l'encontre des fournisseurs d'accès à internet.

Au sein de l'OPI, c'est plus particulièrement le comité pour la notification des droits d'auteur et des droits voisins qui traite les procédures afférentes au nouveau dispositif. Le comité est composé de trois membres nommés pour trois ans, ayant chacun un suppléant :

- le président de l'OPI (qui préside le comité) ;
- un représentant de l'autorité de régulation grecque des communications électroniques et des postes (secrétaire du comité) ;
- un représentant de l'autorité grecque de protection des données personnelles.

Les ayants droit (y compris les sociétés de gestion collective ou les syndicats de défense professionnelle) peuvent saisir le comité après avoir effectué une demande de retrait restée infructueuse en soumettant un formulaire de demande type fourni par l'OPI accompagné de tous les documents complémentaires requis par le comité.

La procédure devant le comité s'achève de plein droit en cas de saisine de l'autorité judiciaire sur le même sujet.

Le comité procède, dans les dix jours ouvrables à compter de la réception de la saisine, à une étude de sa recevabilité. La saisine peut être déclarée irrecevable notamment

[5] <https://thelegalbay.gr/en/home/>

[6] Law no. 4481 (OFFICIAL GOVERNMENT GAZETTE A 100/ 20.7.2017) *Collective management of copyright and related rights, multi-territorial licensing in musical works for online use and other issues falling within the scope of the Ministry of Culture and Sport*, article 52.

au regard du non-respect du formalisme prévu ou de l'existence d'un contentieux en cours ou d'une décision de justice devenue définitive.

Lorsque la saisine est regardée comme recevable, le comité prend attache avec les administrateurs et/ou les propriétaires des services visés par la saisine. Le comité informe également, selon les cas de figure en cause, en tant que possible, les fournisseurs de services d'hébergement et lorsque le site est hébergé à l'étranger, les fournisseurs d'accès à internet grecs.

Dans le cadre de cette notification aux sites sont mentionnés :

- les contenus litigieux ;
- les dispositions légales qui ont été enfreintes ;
- un résumé des faits et des preuves jointes à la saisine ;
- la mention du contradictoire invitant le service litigieux à présenter toute preuve pertinente prouvant qu'aucune infraction n'a été commise sous cinq jours ;
- et enfin les conditions dans lesquelles la procédure pourra être clôturée par le retrait des contenus litigieux ou par la possibilité de conclusion d'accords volontaires entre les parties.

Après la fin de la période d'objection et en toute hypothèse dans les 40 à 60 jours de la réception de la demande^[7], le comité doit rendre sa décision et la notifier aux parties prenantes. Le comité peut soit constater qu'aucune infraction n'a finalement été commise, soit enjoindre :

- lorsque le service est hébergé en Grèce, aux hébergeurs le retrait des œuvres s'il s'agit d'infractions isolées ou si le comité estime être en présence d'une violation massive, qu'il cesse d'héberger le service ;
- lorsque le service est hébergé hors de Grèce, aux fournisseurs d'accès à internet de bloquer l'accès au service en utilisant les moyens techniques les plus appropriés et efficaces.

Dans tous les cas, la durée du blocage est précisée par le comité.

Les destinataires de la décision doivent se conformer à l'obligation de supprimer ou de bloquer l'accès au contenu dans un délai de trois jours ouvrables à compter de la notification de la décision du comité. En cas de non-respect, ils sont passibles d'amendes sous astreinte imposées par le comité qui peuvent être comprises entre 500 et 1 000 euros par jour, en fonction du sérieux de l'infraction et de sa récurrence.

La décision est susceptible de recours devant les tribunaux administratifs.

Les coûts du blocage sont en principe supportés par les fournisseurs d'accès à internet^[8]. Les ayants droit s'acquittent toutefois auprès de l'OPI de sommes pour les frais afférents aux décisions de blocage administratif, suivant le nombre de noms de domaine à bloquer (de 1 à 50). L'OPI considère que les frais dont doivent s'acquitter les ayants droit pour lancer une procédure sont prévus pour chaque nom de domaine dont le blocage est demandé et non par offre. Ainsi, lorsqu'est demandé le blocage d'une offre comprenant un site principal et ses différents miroirs, les frais seront calculés en fonction du nombre de noms de domaine visés.

Le comité a débuté ses activités en septembre 2018, ses décisions sont publiées^[9]. Les ayants droit de différents secteurs (livre, audiovisuel, musique) ont fait des demandes de blocage auprès de l'OPI. La liste des sites bloqués est publiée sur le site de l'OPI^[10].

L'ACTUALISATION DES MESURES ADMINISTRATIVES DE BLOCAGE

L'écueil du dispositif grec est qu'il ne prévoyait pas de procédure spécifique pour les sites miroirs, de sorte que les ayants droit devaient à nouveau saisir l'OPI dans les mêmes formes que pour la demande initiale de blocage. Dans l'attente d'un amendement, les ayants droit avaient rapidement limité l'engagement de nouvelles procédures.

Une loi de juillet 2020 a permis au comité d'ordonner toute mesure visant à prévenir ou à faire cesser une atteinte à un droit d'auteur ou un droit voisin. Désormais, si à la suite de l'adoption et de l'exécution d'une ou de plusieurs décisions, l'atteinte persiste, le titulaire de droits lésé peut déposer une demande auprès de l'OPI afin de solliciter l'adoption d'une nouvelle décision, ce sans payer de frais supplémentaires.

[7] N.B. : chacun des délais susmentionnés peut être doublé.

[8] <https://www.opi.gr/index.php/en/committee/request-committee>

[9] <https://www.opi.gr/en/current-affairs1/news/9379-07-11-2018-decisions-of-the-committee-for-the-notification-of-copyright-and-related-rights-infringement-on-the-Internet>

[10] https://opi.gr/images/epitropi/edppi_list_v5.pdf

Dans ce cas, le comité informe les administrateurs des services en leur communiquant la demande par tout moyen et en les invitant à soumettre leurs éventuelles observations sous cinq jours. Ensuite, le comité rend sa décision dans un délai de dix jours à compter de l'expiration du délai susmentionné.

À la suite de cet amendement, un organisme de gestion collective administrant des droits sur des œuvres audiovisuelles a déposé deux demandes devant le comité alléguant le contournement de ses décisions. Deux décisions ont été émises à la suite de cette réforme en 2020.

LA LUTTE CONTRE LE PIRATAGE DE CONTENUS SPORTIFS

Le législateur grec a introduit en décembre 2020 la possibilité pour les titulaires de droit de demander des injonctions de blocage en direct pour empêcher la retransmission sur internet non autorisée d'événements culturels et sportifs.

Les conditions préalables qui doivent être cumulativement remplies pour l'ouverture de cette procédure sont les suivantes :

- une violation du droit d'auteur ou des droits voisins des chaînes de télévision à grande échelle doit être imminente sur internet concernant – selon le libellé pertinent – des événements s'adressant à des audiences télévisées nationales ou internationales qui seront transmis au moment même où ils se dérouleront ;
- en outre, une telle violation doit avoir lieu au moyen de certains URL, adresses IP ou noms de domaine qui supportent ou plus précisément qui permettent de visionner le contenu ;
- et il doit y avoir un cas d'urgence pour prévenir un danger immédiat, sérieux et imminent ou un préjudice irréparable pour l'intérêt public ou le titulaire du droit.

Si les conditions préalables susmentionnées sont remplies, l'autorité est habilitée à rendre une décision de blocage temporaire limitée à la durée de l'événement.

Dans cette perspective, les titulaires de droits doivent soumettre leur demande au moins quinze jours avant la transmission prévue de l'événement, tout en étant en mesure d'actualiser cette demande jusqu'à ce que le comité rende sa décision, notamment s'agissant de la liste des services à bloquer.

La décision ordonne aux fournisseurs d'accès à internet de bloquer l'accès au contenu illicite dans un délai allant de six à douze heures à compter de la notification de la décision. La décision du comité doit être rendue vingt-quatre heures au plus tard avant la transmission de l'événement indiqué et être notifiée dans ce délai, par courrier électronique, au demandeur, ainsi qu'aux fournisseurs d'accès et au régulateur des télécommunications.

À l'expiration de ce délai, la décision est en outre notifiée aux opérateurs des services visés, lesquels peuvent faire appel de cette décision devant la cour d'appel administrative d'Athènes dans un délai de dix jours à compter de la notification. Dans le cas où un recours n'a pas été émis ou au contraire est rejeté, la décision ordonnant le blocage ne peut plus être contestée.

Il est en outre prévu, s'il s'avère que les conditions préalables prévues par la loi n'ont pas été remplies, que le demandeur devra indemniser l'opérateur des sites indûment visés par une mesure de blocage. À cet égard, la loi prévoit que le montant d'une telle indemnisation est déterminé en fonction des circonstances de chaque cas d'espèce en tenant également compte du comportement raisonnable ou au contraire de la faute du titulaire du droit.

Un décret doit encore préciser les contours de cette procédure.

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

1 380 POPULATION^[1]
en millions

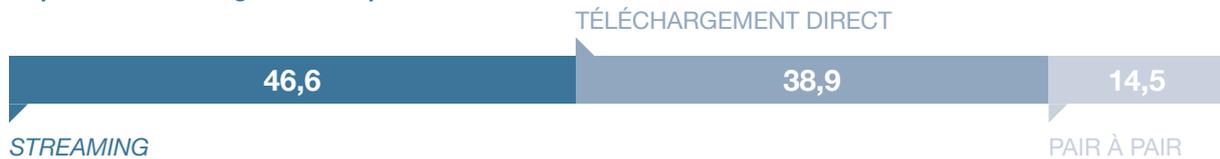
20,1 % TAUX DE PÉNÉTRATION
INTERNET (2018)^[2]

USAGES ILLICITES^[3]

5,4 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

20 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illégitimes par mode d'accès en %



Une étude publiée en septembre 2017 indique que 94 % des utilisateurs d'internet indiens^[4] ont téléchargé illégalement des contenus musicaux ces six derniers mois et ont utilisé Google pour trouver de la musique gratuite – la plupart recherchant expressément des sources illégitimes^[5]. Les services de *stream ripping* illégitimes, très présents en Inde, sont également un problème majeur.

L'industrie du jeu vidéo a fait savoir que l'Inde était le cinquième pays du monde, en 2017, s'agissant du nombre de partages sur les réseaux pair à pair. L'Inde est d'ailleurs le second pays du monde s'agissant des usages illégitimes de jeux vidéo^[6].

En réponse au phénomène de piratage, le gouvernement indien a approuvé en mai 2016 une politique nationale de propriété intellectuelle axée autour de sept objectifs^[7]. Ces derniers comprennent notamment : la sensibilisation aux droits de propriété intellectuelle de la société dans son

ensemble, l'adoption de lois de propriété intellectuelle efficaces, la modernisation et le renforcement de services dédiés de l'administration et des procédures judiciaires.

Ces actions doivent être menées par différents ministères et coordonnées par le ministère du Commerce et de l'Industrie.

Il faut relever que l'Inde étant une république fédérale, la coordination de la lutte contre le piratage, et notamment les actions visant les services contrefaisants, est complexe et peut varier selon les régions.

Si une large part du dispositif anti-piratage à destination des internautes relève d'actions pénales ou d'actions de sensibilisation, des mesures judiciaires à l'égard des sites illégitimes peuvent également être prononcées sur le fondement de la *common law*.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] L'étude « Badvertising Report » de Verisite indique qu'en Inde le piratage via des applications mobiles prend également de plus en plus d'ampleur.

[5] KPMG LAIFC FICCI Report: The 'Digital First' journey :

[http://www.laindiafilmcouncil.org/og-content/uploads/documents/1507100573The %20Digital %20First %20journey_Print.pdf](http://www.laindiafilmcouncil.org/og-content/uploads/documents/1507100573The%20Digital%20First%20journey_Print.pdf)

[6] <https://iipa.org/files/uploads/2018/02/2018SPEC301INDIA.pdf>

[7] Communiqué de presse « Cabinet approves National Intellectual Property Rights Policy » 13 mai 2016, <http://www.pib.nic.in/newsite/PrintRelease.aspx?relid=145338> - Lien vers la vidéo de campagne : https://www.youtube.com/watch?v=-EDT4q_Vis

LES ACTIONS VISANT LES INTERNAUTES

LES ACTIONS DE SENSIBILISATION

La *Cell For Ipr Promotion And Management*, entité rattachée au département de la politique et de la promotion industrielle (DIPP) du ministère du Commerce et de l'Industrie, organise une campagne de sensibilisation, notamment sur les réseaux sociaux (par exemple en utilisant le mot-clé #LetsTalkIP), et des ateliers de sensibilisation aux droits de propriété intellectuelle dans les écoles et les collèges.

En août 2017, la CIPAM et le DIPP ont organisé le premier groupe de travail national dédié à la propriété intellectuelle. L'un des axes principaux de communication était une vidéo réalisée en partenariat entre des ayants droit de l'audiovisuel anglo-saxon (la MPA), l'opérateur des chaînes de télévision Viacom 18's et la chaîne de télévision destinée au jeune public Nickelodeon^[8]. Cette vidéo met en scène des personnages de dessins animés très populaires auprès des enfants qui expliquent que le piratage équivaut à du vol.

Le ministre du Commerce et de l'Industrie a dévoilé une nouvelle campagne de lutte contre le piratage en mai 2018. Cette campagne a mobilisé d'importants moyens et a vu la participation de célèbres acteurs bollywoodiens^[9] à des vidéos disponibles notamment sur YouTube. Une campagne spécifique aux enfants conduite par la CIPAM en partenariat avec l'EUIPO met en scène une grand-mère technophile (IP Nani) qui aide le gouvernement à combattre le piratage avec l'aide de son petit-fils.

La CIPAM collabore également avec le conseil national de la formation à la recherche et à l'enseignement pour élaborer des supports dédiés aux droits de propriété intellectuelle : cette coopération a permis d'introduire les droits de propriété intellectuelle au programme des manuels scolaires des lycéens.

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES SERVICES ILLICITES ET LEURS OPÉRATEURS

En janvier 2017, le ministre du Commerce et de l'Industrie a annoncé la création d'une boîte à outils destinée aux officiers de police sur tout le territoire indien afin de les aider à appréhender les crimes et infractions liés aux droits de propriété intellectuelle. Cette boîte à outils a été développée par la Cellule pour la promotion et la gestion des droits de propriété intellectuelle (CIPAM) en partenariat avec la Fédération des chambres de commerce et d'industrie indiennes et des acteurs privés.

La boîte à outils a vocation à être utilisée dans tous les programmes de formation des officiers et prévoit notamment des explications détaillées sur tous les types

d'infractions, une liste des vérifications pour recevoir les plaintes et conduire les perquisitions et les saisies, ainsi que des conseils pour mener à bien les perquisitions.

La CIPAM a également organisé des programmes de formation pour les officiers de police en collaboration avec des ayants droit, comme la MPA, dans des académies de police locales.

LES MESURES JUDICIAIRES DE BLOCAGE

Les ayants droit peuvent demander en justice le prononcé d'ordonnances dites « *John Doe* »^[10] permettant d'agir à l'encontre des intermédiaires techniques dès lors que l'administrateur du site n'est pas connu.

[8] https://www.youtube.com/watch?v=_JBpNZweibU

[9] Voir par exemple <https://www.youtube.com/watch?v=KcqnmxCNRXE>

[10] Les *John Doe* orders sont issues de la common law.

La procédure telle qu'elle résulte des deux affaires distinctes^[11] traitées par la haute cour de Bombay est la suivante : l'ayant droit doit procéder à une notification publique du jugement afin d'informer les défendeurs et leur laisser un délai de quatre jours pour faire appel de la décision. Le blocage des pages dure 21 jours maximum, l'ayant droit doit saisir à nouveau le juge s'il souhaite prolonger l'effet des injonctions. Sur les pages bloquées, les hébergeurs doivent faire apparaître des mentions indiquant précisément les raisons pour lesquelles les pages sont bloquées, l'adresse de l'ayant droit et l'information selon laquelle toute personne s'estimant lésée peut saisir le juge. Les conditions d'exercice de cette action sont similaires à celles de l'introduction d'une procédure en référé. Ces ordonnances sont régulièrement utilisées par l'industrie du cinéma indien qui est particulièrement vigilante dans les jours qui précèdent la sortie d'un film. Ainsi, en novembre 2018, la haute cour de Madras a ordonné le blocage de 12 564 noms de domaine en lien avec 16 sites, en prévision de la sortie du film indien aux coûts de production le plus élevés à ce jour^[12]. Il faut relever que parmi tous ces noms de domaine, nombre d'entre eux n'avaient pas été enregistrés au moment de la décision.

Une décision d'octobre 2017 de la haute cour de Delhi a quant à elle ordonné, dans le cadre d'une procédure intentée par la *Motion Picture Distributor's Association* (MPDA) au nom de tous les studios, le blocage de deux sites dans leur intégralité, arguant de leur caractère structurellement contrefaisant. Le juge a également accepté que les studios puissent faire évoluer leurs demandes afin d'intégrer les sites de contournement. Suite à cette décision, 78 % des fournisseurs d'accès à internet se sont conformés à la décision du juge et les ayants droit ont constaté une diminution de 89 % du trafic total vers ces sites.

En avril 2019, la haute cour de Delhi a ainsi ordonné^[13] le blocage permanent de certains des plus importants sites de pair à pair et de *streaming*, ainsi que les noms de domaine alternatifs et proxys utilisés. La décision prévoit que les ayants droit pourront transmettre les informations relatives à l'apparition de sites de contournement afin que ceux-ci soient immédiatement bloqués. Le juge a également suggéré aux autorités la possibilité d'envoyer des courriels, de mettre en place des pop-ups ou d'autres types d'avertissement à l'adresse des internautes continuant d'utiliser les sites visés. Il précise

qu'en cas d'échec de ces mesures d'avertissement, l'internaute pourrait devoir payer une amende.

Plus de 13 000 sites sont actuellement bloqués en Inde à la suite de demandes adressées à la haute cour de Calcutta, à la haute cour de Delhi, à la haute cour de Madras et d'une soumission à la *Maharashtra Digital Crime Unit*.

LE PROJET DE RÉFORME

Un nouveau projet de réglementation sur le commerce électronique a été publié début 2019. Celui-ci prévoit la création d'une entité regroupant les parties prenantes afin de permettre d'identifier les sites proposant illicitement des contenus protégés, afin de mettre en œuvre diverses mesures à leur encontre. Les intermédiaires techniques pourraient notamment être tenus de désactiver l'accès à ces services et les moteurs de recherche tenus de les déréférencer.

Le projet pourrait également inviter les plateformes à mettre en place, sur une base volontaire, des mesures pour empêcher la diffusion en ligne de contenus piratés. Il s'agirait pour ces acteurs d'identifier des entités dignes de confiance dont les signalements seraient traités en priorité.

LA LUTTE CONTRE LE PIRATAGE DES CONTENUS SPORTIFS

En juin 2019, la haute cour de Delhi^[14] a rendu une ordonnance en référé, dans le cadre d'une procédure initiée par un groupe détenant les droits des retransmissions radio des matchs de la coupe du monde de cricket, laquelle devait s'achever début juillet 2019. La cour a ordonné le blocage des services retransmettant illégalement la captation audio de ces rencontres. Dans le cadre de l'ordonnance, les moteurs de recherche sont également tenus de supprimer de leurs résultats tout site web/URL qui donne accès à des sites en infraction sur notification du défendeur. À noter que l'injonction vise non seulement les diffusions illicites de la captation audiovisuelle des matchs mais également les retransmissions radio illicites de ces matchs.

[11] *Affaire Balaji Motion Pictures & Anr v Bharat Sanchar Nigam & Ors et Affaire Eros International and Anr v BSNL & Others*.

[12] *High Court of Madras, 28 novembre 2018, Lyca Production Pvt. Ltd v Bahrat Sanchar Nigam Limited & Others*.
<https://torrentfreak.com/images/johndoe20.pdf>

[13] *High Court of Delhi, 10 avril 2019, CS (COMM) 724/2017 & Ors*.

[14] *High Court of Delhi, 03 juin 2019, CS (COMM) 326/2019 & I.A. 8510/2019 & 8508/2019* : <https://torrentfreak.com/images/Channel2-blocking-order-Delhi-High-Court.pdf>

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

Les autorités indiennes se sont inspirées de la PIPCU, l'unité de police anglaise spécialisée dans la lutte contre les atteintes aux droits de propriété intellectuelle, pour créer dans certains États des unités de police dédiées à la cybercriminalité.

L'unité dédiée à la cybercriminalité de l'État du Maharashtra a été créée en 2017. Sur la base du modèle britannique, les sites soupçonnés de se livrer à la contrefaçon sont examinés à la lumière de différents paramètres avant d'être inscrits sur une liste de sites à surveiller.

L'unité met alors en demeure le site inscrit et ses partenaires afin qu'ils cessent leurs activités illicites. Ensuite, des notifications sont adressées aux régies publicitaires pour leur demander de cesser de collaborer avec les sites.

En parallèle, les fournisseurs d'accès à internet ainsi que le *registrar* Nixi (l'organisme en charge de l'enregistrement des noms de domaine locaux en « .in »), reçoivent une plainte écrite de l'unité leur demandant de cesser de fournir leurs services aux sites mis en cause. Les demandes de la police sont fondées sur des dispositions du code de procédure pénale, qui permettent d'engager toute action préventive lorsqu'un crime est suspecté.

Nixi suspend les noms de domaine qui se livrent à des activités dédiées au piratage en vérifiant les informations fournies pour l'enregistrement et notamment la validité des adresses *e-mail* fournies. Ainsi, depuis juin 2017, l'unité a obtenu la suspension de plus de 25 noms de domaine dans le cadre de cette procédure.

Par ailleurs, le nouveau projet de réglementation sur le commerce électronique publié début 2019 prévoit la création d'une entité regroupant les parties prenantes afin de pouvoir lister, après vérification, les sites proposant illicitement des contenus protégés, afin de permettre la mise en œuvre de mesures de type « *Follow the money* » à leur encontre. Dans ce contexte, les ayants droit et les acteurs de la publicité discuteraient d'ailleurs, sous l'égide de la CIPAM, de la signature d'un engagement volontaire.

IRLANDE

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

4,9 POPULATION^[1]
en millions

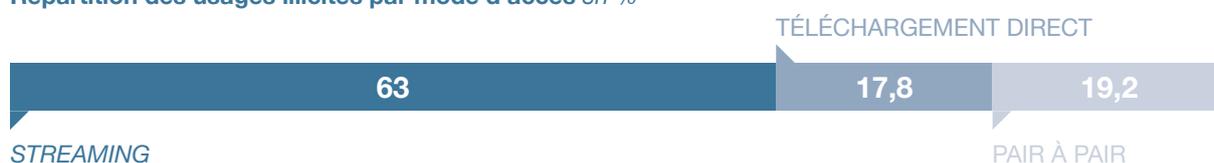
84,5 % TAUX DE PÉNÉTRATION
INTERNET (2018)^[2]

USAGES ILLICITES^[3]

0,28 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

68 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



Le système irlandais de lutte contre le piratage combine un dispositif d'avertissement des internautes et un dispositif judiciaire de blocage. Une des spécificités de ce système réside dans le

fait que ces mesures peuvent être mises en œuvre par différents acteurs, soit en vertu d'un accord volontaire, soit dans le cadre d'une injonction judiciaire.

LES ACTIONS VISANT LES INTERNAUTES

LE DISPOSITIF D'AVERTISSEMENT DES INTERNAUTES

UN MÉCANISME D'AVERTISSEMENT GRADUEL MIS EN ŒUVRE DANS LE CADRE D'UN ACCORD VOLONTAIRE BILATÉRAL

En 2009, un accord a été conclu entre le principal fournisseur d'accès à internet, Eircom (devenu Eir en 2019) et l'*Irish Recorded Music Association* (IRMA), aux termes duquel le fournisseur d'accès à internet s'est engagé à mettre en place un dispositif de réponse graduée.

Le fournisseur d'accès à internet envoie ainsi des *emails* à ses abonnés dont l'adresse IP lui a été transmise par l'IRMA. Après trois avertissements, la sanction encourue, sans intervention du juge, est la coupure de l'accès à internet pour une durée de sept jours. En cas de réitération, cette coupure peut être d'une durée d'un an.

Ce dispositif n'a pas été mis en œuvre de façon continue et a connu des interruptions, compte tenu de certaines incertitudes juridiques en matière de protection des données personnelles, jusqu'à la validation définitive du dispositif en 2013 par la juridiction suprême irlandaise^[4].

En 2019, Eir a continué à mettre en œuvre ce dispositif, avec l'envoi de 5 000 avertissements par mois.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] www.supremecourt.ie/Judgments.nsf/1b0757edc371032e802572ea0061450e/c9861b9cda79509b80257b9d004e9a7a?OpenDocument

L'EXTENSION DE CE MÉCANISME EN APPLICATION D'UNE INJONCTION JUDICIAIRE

Les ayants droit de la musique ont souhaité étendre à d'autres fournisseurs d'accès à internet l'application du dispositif précité mais, faute d'accord volontaire, il n'a été possible d'imposer cette mise en œuvre qu'après la transposition, en 2012, de l'article 8.3 de la directive 2001/29/CE dite DADVSI du 22 mai 2001, lequel permet d'obtenir une injonction contre un intermédiaire technique dont les services sont utilisés pour porter atteinte à un droit d'auteur ou un droit voisin.

Le juge irlandais, saisi par les ayants droit de la musique dans le cadre d'un contentieux les opposant au fournisseur d'accès à internet UPC (depuis devenu Virgin), a laissé un délai aux parties afin qu'elles parviennent à un accord. Passé ce délai, faute d'accord, le juge a posé les grandes lignes du dispositif^[5] :

- lorsqu'un de ses abonnés a été destinataire de trois notifications, le fournisseur d'accès à internet doit en informer les ayants droit ;
- l'ayant droit pourra ensuite saisir le juge pour connaître l'identité de cet internaute et demander à ce que son contrat avec le fournisseur d'accès à internet soit résilié ou à ce que son accès internet soit suspendu (à la différence de l'accord avec Eir, qui n'implique pas l'intervention du juge) ;
- en raison des coûts du dispositif, Virgin Media doit adresser au maximum 2 500 notifications par mois et un délai de 15 mois lui a été octroyé pour mettre en place un système automatisé.

Sky et Vodafone ont été contraints dans des termes similaires de mettre en place un dispositif d'avertissement respectivement par un jugement du 8 octobre 2018 et du 8 avril 2019. Le délai qui est laissé aux fournisseurs d'accès pour mettre en place un système automatisé et le nombre maximal de notifications que ceux-ci peuvent envoyer varient cependant selon le nombre d'abonnés et les spécificités techniques des différents fournisseurs d'accès. Sky doit envoyer un maximum de 1 200 notifications par mois et s'est vu octroyer jusqu'à avril 2019 pour mettre en place un système automatisé. Quant à Vodafone, celui-ci a pu disposer d'un délai de neuf mois pour mettre en place un système automatisé qui lui permettra d'envoyer au maximum 1 800 notifications par mois.

LA PROMOTION DE L'OFFRE LÉGALE

L'*Industry trust for Intellectual Property Awareness Ireland*, un organisme privé qui regroupe des acteurs de l'audiovisuel et promeut la protection des œuvres et de la création, a lancé une plateforme en Irlande^[6] qui vise à sensibiliser à la protection du droit d'auteur et à l'importance de se tourner vers l'offre légale pour encourager la création.

Le groupement, qui a également une branche anglaise, déploie ainsi différentes campagnes de communication et notamment « *Momentsworthpayingfor* » depuis sept ans. Soutenues par l'industrie du cinéma, leurs bandes annonces sont projetées dans les cinémas en Irlande tout au long de l'année^[7].

[5] High Court Commercial, *Sony Music Entertainment (Ireland) Ltd & Ors -v- UPC Communications Ireland Limited* (No. 1), 27 mars 2015 : www.courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/84d0803d3bc9ae1c80257e5100477a3d?OpenDocument
High Court Commercial, *Sony Music Entertainment (Irl) Ltd & Ors -v- UPC Communications Irl Ltd* (No 3), 17 juin 2015.

[6] <http://lovemovies.ie/>

[7] <https://www.industrytrust.co.uk/campaigns/moments/>

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES MESURES JUDICIAIRES DE BLOCAGE

Dans le secteur musical, l'accord conclu entre l'IRMA et le fournisseur d'accès à internet Eircom comporte également des dispositions facilitant l'exécution de mesures de blocage. Sur cette base, il a pu être enjoint à Eircom de bloquer le site « *The Pirate Bay* » et sa galaxie en 2009.

S'agissant des autres fournisseurs d'accès à internet, il n'a été possible de diligenter des procédures visant à obtenir le blocage des sites qu'à partir de 2012, date à laquelle a été transposé l'article 8.3 de la directive DADVSI précitée.

Depuis, plusieurs décisions ont permis d'enjoindre aux fournisseurs d'accès à internet de bloquer notamment les sites « *The Pirate Bay* » en juin 2013^[8] et « *Kickass-Torrents* » en décembre 2013.

Deux ordonnances de blocage ont été rendues récemment :

- le 3 avril 2017, les membres de la MPA ont obtenu le blocage, par les huit principaux fournisseurs d'accès à internet irlandais, de trois sites contrefaisants^[9] ;
- en janvier 2018, huit sites de *streaming* ou de *torrent* violant massivement les droits d'auteur^[10] ont également été bloqués, notamment eu égard à leur forte audience, à la présence de milliers de fichiers contrefaisants et à un « *important motif d'intérêt public* ».

Depuis 2013, les décisions prévoient expressément que les fournisseurs d'accès à internet bloqueront par la suite les sites de contournement permettant d'accéder aux sites bloqués, dans le respect d'un protocole d'accord annexé à l'ordonnance.

En pratique, les ayants droit notifient ainsi régulièrement aux fournisseurs d'accès à internet une liste actualisée avec les nouvelles adresses IP et/ou les nouveaux noms de domaine à partir desquels les contenus des sites bloqués sont accessibles.

LA LUTTE CONTRE LE PIRATAGE DES CONTENUS SPORTIFS

En se fondant sur la jurisprudence développée au Royaume-Uni, le 15 juillet 2019^[11], pour la première fois, une injonction de blocage IP dynamique en temps réel, limitée à la durée des matchs, a été rendue par la haute cour pour bloquer l'accès aux contenus sportifs de la *Premier League* jusqu'au 30 juin 2020, afin de couvrir la saison 2019/2020 de football. La *Premier League* peut demander le renouvellement de cette injonction devant le juge. En septembre 2020, l'UEFA a obtenu une injonction similaire pour la saison 2020/2021^[12], obtenant l'autorisation d'obliger plusieurs fournisseurs d'accès à internet locaux à bloquer l'accès aux flux de matchs piratés.

[8] High Court Commercial, 12 juin 2013, *EMI Records (Ireland) Limited Sony Music and Entertainment (Ireland) Limited Universal Music Ireland Limited and Warner Music Ireland Limited - v - UPC Communications Ireland Limited, Vodafone Ireland Limited Imagine Telecommunications Limited Digiweb Limited Hutchinson 3G Ireland Limited and by order of the Court Telefonica Ireland Limited*.

[9] High Court commercial, 3 Avril 2017, *Motion Picture Association v Eircom, Sky, Ireland, Vodafone, Magnet Networks, Three Ireland, Three Ireland Services*.

[10] High Court commercial, 15 janvier 2018, *Motion Picture Association -v-Eircom, Sky, Ireland, Vodafone Ireland, Virgin Media Ireland, Three Ireland, Digiweb, Imagine Telecommunications, Magnet Networks*.

[11] High Court Commercial, 15 juillet 2019, *the Football Association Premier League Limited v eircom limited trading as eir , sky ireland limited , sky subscribers services limited , virgin media ireland limited , vodafone ireland limited*.

[12] High Court Commercial, 29 septembre 2020, *Union des Associations Européennes de Football v eircom limited t/a eir, sky ireland limited, sky subscribers services limited, virgin media ireland limited and vodafone ireland limited*
[https://www.bailii.org/cgi-bin/format.cgi?doc=/ie/cases/IEHC/2020/2020IEHC488.html&query=\(uefa\)](https://www.bailii.org/cgi-bin/format.cgi?doc=/ie/cases/IEHC/2020/2020IEHC488.html&query=(uefa))

ITALIE

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

60,5 POPULATION^[1]
en millions

74,39 % TAUX DE PÉNÉTRATION
INTERNET (2018)^[2]

USAGES ILLICITES^[3]

1,9 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

42 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



Le dispositif italien se concentre principalement sur la lutte contre les services illícites. En revanche, aucun dispositif ne vise spécifiquement les inter-

nantes, bien qu'une première action à leur encontre ait été initiée en 2020.

LES ACTIONS VISANT LES INTERNAUTES

La police douanière et financière (*la Guardia di Finanza*) dispose de compétences d'investigation, de contrôle et de répression des violations commises sur internet *Guardia*. En février 2020, l'action de la *Guardia di Finanza* s'est dirigée vers les particuliers qui utilisaient des abonnements à des bouquets de chaînes proposés illícitement. 223 personnes ont été identifiées et risquent une condamnation à 8 ans de réclusion et jusqu'à 25 000 euros d'amende^[4].

Parallèlement, des mesures sont mises en œuvre afin d'améliorer la visibilité de l'offre légale : un portail de l'offre légale recensant les différentes plateformes des principaux secteurs culturels numériques a été mis en place par l'association des industries culturelles italiennes (*Confindustria cultura italia*)^[5].

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] Article 171 octies de la loi 633/41 sur le droit d'auteur.

[5] www.mappadeicontenuti.it

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

Le *decreto legislativo* n° 70/2003 transposant la directive dite « commerce électronique » prévoit que l'autorité publique, tout comme l'autorité judiciaire, peut prescrire aux hébergeurs et aux fournisseurs d'accès internet toutes mesures propres à prévenir ou à faire cesser un dommage occasionné par la mise à disposition d'un contenu non autorisé par un service de communication au public en ligne^[6].

Coexistent alors deux procédures pouvant conduire au blocage de sites : une procédure administrative mise en œuvre par une autorité indépendante, l'*Autorità per le Garanzie nelle Comunicazioni* (AGCOM), et une procédure judiciaire. Des actions au pénal sont par ailleurs diligentées à la suite d'investigations conduites par la police.

LES ACTIONS CONTRE LES SITES ILLICITES ET LEURS OPÉRATEURS

La première approche mise en œuvre par la police douanière et financière a vocation à permettre, à partir des investigations opérées par des acteurs locaux de la publicité en ligne, de remonter jusqu'aux responsables des sites et de les identifier. Dans ce cadre, la *Guardia di Finanza* a mené une opération appelée « *Operation Pirate* », qui a abouti à l'identification des responsables d'un groupe de distribution de copies illicites de films et des séries. Une seconde approche dite « *Follow the hosting* » permet d'identifier la véritable localisation des sites. Certains sites, en utilisant des techniques d'anonymisation, apparaissent comme établis à l'étranger alors même qu'ils sont gérés à partir du sol italien.

En septembre 2019, les douaniers italiens de la *Guardia di Finanza* ont annoncé avoir démantelé un réseau proposant illicitement des offres IPTV.

L'enquête, dirigée par le parquet de Naples, a permis l'arrestation de 23 personnes ainsi que la mise au jour et la désactivation de la plateforme d'IPTV illégale Xstream Codes qui revendiquait plus de 5 000 clients pour plus de 18 000 serveurs vendus et plus de 50 millions d'utilisateurs.

En décembre 2020, cette même *Guardia di Finanza* a mené une opération coordonnée par le parquet de Milan qui a abouti à la « saisie préventive » d'une plateforme IPTV par laquelle les utilisateurs accédaient à des contenus télévisés sans autorisation. Cette action faisait suite aux dépôts de plaintes d'ayants droit d'événements sportifs auprès des autorités.

LES MESURES ADMINISTRATIVES DE BLOCAGE

PRÉSENTATION DE L'AUTORITÉ

Une autorité indépendante créée en 1997, l'*Autorità per le Garanzie nelle Comunicazioni* (AGCOM), exerce des fonctions de réglementation et de contrôle dans le secteur des communications électroniques, de l'audiovisuel et de l'édition.

L'AGCOM est une autorité « convergente » qui a vu depuis 2000 son rôle s'accroître au fur et à mesure en matière de protection du droit d'auteur dans les secteurs où elle exerce des fonctions de garant et de régulateur (audiovisuel, services de média à la demande et communications électroniques).

L'AGCOM est ainsi chargée de la définition et de la mise en œuvre de la lutte contre les sites massivement contrefaisants. À ce titre, elle a adopté le 12 décembre 2013 un règlement de protection du droit d'auteur sur les réseaux de communication électroniques, qui est entré en vigueur le 31 mars 2014.

La procédure devant l'AGCOM s'achève en cas de saisine de l'autorité judiciaire sur le même sujet : elle lui transmet alors les éléments en sa possession.

LES PROCÉDURES DE RETRAIT DES ŒUVRES OU DE BLOCAGE ADMINISTRATIF

L'AGCOM peut être saisie par les ayants droit pour obtenir le retrait de contenus mis à disposition sur internet sans autorisation.

L'AGCOM informe le site de sa saisine et l'invite à procéder volontairement au retrait du contenu et à faire valoir ses éventuelles observations dans un délai

[6] L'autorité judiciaire ou administrative ayant des fonctions de contrôle peut exiger y compris en voie d'urgence du prestataire qu'il mette un terme à une violation.

de cinq jours. L'AGCOM informe également du début de la procédure les fournisseurs d'accès internet et les hébergeurs (à savoir les intermédiaires cités par la directive « commerce électronique »).

En cas d'absence de coopération du site, l'AGCOM a trente-cinq jours pour statuer sur la demande des ayants droit.

Le règlement de protection du droit d'auteur sur les réseaux de communication électroniques prévoit dans les hypothèses de « violations massives » une procédure abrégée de 12 jours.

Différents éléments sont pris en compte pour déterminer la gravité et l'ampleur de l'atteinte et notamment la quantité d'œuvres disponibles sur le site concerné (une violation est considérée comme massive dès lors que sur un site sont présentes une trentaine d'œuvres illégales), la promotion ou l'incitation à la consommation de contenus illicites, la présence d'allégations mensongères quant à la légalité des services fournis.

Le collège de l'AGCOM peut soit conclure au classement de la demande, soit constater l'atteinte. Dans le respect du principe de proportionnalité, l'AGCOM prononce alors des injonctions à l'encontre :

- des hébergeurs lorsque le site mis en cause est hébergé sur un serveur présent sur le territoire italien. Le collège peut leur ordonner de retirer les œuvres en cause ou en interdire l'accès en cas de violation massive ;
- des fournisseurs d'accès à internet, si le serveur hébergeant les œuvres est hors du territoire national. Le collège peut ordonner aux fournisseurs d'accès internet de procéder au blocage DNS ou IP d'un site entier. En pratique, seules des décisions de blocage DNS sont prononcées. La charge financière des opérations de blocage incombe aux fournisseurs d'accès.

Lorsque le collège prononce une injonction de retrait des œuvres ou de blocage du site, il peut ordonner que les requêtes des internautes relatives aux pages ou au site bloqué soient redirigées automatiquement vers un message de l'AGCOM sur les mesures qu'elle a ordonnées.

Le règlement relatif aux compétences de l'autorité publique prévoyait la possibilité pour l'AGCOM de prononcer des sanctions administratives en cas de non-respect de ses décisions, lesquelles peuvent d'ailleurs être contestées devant l'autorité judiciaire. Toutefois, par décision du 15 juillet 2019^[7], le Conseil d'État italien a considéré qu'en l'absence de dispositions législatives l'y autorisant expressément, l'AGCOM n'était pas autorisée à émettre de sanctions en cas de non-respect de ses injonctions de blocage^[8]. Un décret du 19 juillet 2020 dit « *Decreto Rilancio* » a ainsi prévu la possibilité pour l'AGCOM de prononcer des amendes administratives en cas de non-respect de ses décisions et a par ailleurs prévu la possibilité pour l'AGCOM d'ordonner des mesures de retrait des œuvres à des intermédiaires tels que notamment les services de messagerie. L'AGCOM a lancé une consultation afin d'adapter le règlement en conséquence.

S'agissant des services visés par les décisions de l'AGCOM, la reconnaissance d'un droit voisin sur les retransmissions sportives rend l'AGCOM compétente pour ordonner des mesures de blocage à l'égard des services proposant du *live streaming*.

Les injonctions de blocage peuvent viser également les sites illicites de *stream ripping*. L'AGCOM a ainsi prononcé des injonctions de blocage visant 16 sites de *stream ripping*. Dans une décision du 2 août 2019^[9], le tribunal de Latium a ainsi confirmé l'injonction de blocage du site de *stream ripping* Yout prononcée par l'AGCOM.

En janvier 2019, l'AGCOM a également ordonné le blocage du service d'hébergement de fichiers français *1Fichier*.

Enfin, en avril 2020, l'AGCOM a été saisie par la Fédération italienne de éditeurs de journaux (FIEG) afin d'obtenir de la plateforme de messagerie instantanée Telegram le retrait de plusieurs éditions des journaux et la suspension de l'accès à la plateforme. Après un échange avec la plateforme, cette dernière a, en accord avec l'AGCOM, procédé volontairement à la suppression de sept des huit chaînes de diffusion signalées par la FIEG.

[7] Consiglio di Stato, sez VI, 15 juillet 2019 n° 4993.

[8] Cette décision intervient après une longue bataille judiciaire commencée en 2014 dans le cadre d'un recours pour excès de pouvoir introduit par plusieurs associations de consommateurs.

[9] Cour du Latium, 2 août 2019, n° 09060/2019

<http://www.hadopi.info/dj/news/ressources/English%20TRANSLATION%20order%20n.%205304-2019.docx>

L'EXTENSION DES POUVOIRS DE L'AGCOM AUX ATTEINTES MANIFESTES ET L'ACTUALISATION DES MESURES DE BLOCAGE

L'AGCOM a adopté le 16 octobre 2018 un règlement qui détaille la mise en œuvre concrète de ses injonctions et les mesures nécessaires afin d'empêcher la réitération des violations déjà constatées.

LES MESURES D'URGENCE

Lorsqu'il existe un risque de préjudice imminent, l'autorité peut soit ordonner en urgence aux hébergeurs de retirer les œuvres en cause, soit ordonner une mesure de blocage.

Ces mesures doivent être adoptées dans un délai de trois jours suivant la saisine des ayants droit.

Lorsque la personne ayant mis le contenu à disposition et/ou le gestionnaire du site internet est joignable, l'injonction lui est également notifiée et il dispose de cinq jours pour s'opposer à la décision.

En cas de recours, le collège de l'Autorité délibère dans un délai de sept jours.

LES HYPOTHÈSES DE RÉITÉRATION

S'agissant des réitérations de violations constatées et ayant fait l'objet d'une injonction de l'AGCOM, il est prévu que suite à la saisine des ayants droit, l'autorité procède à la vérification de la réitération. Dans le document de consultation préalable à l'adoption du règlement cité ci-avant, l'AGCOM a fourni une description de la méthode qu'elle utilise pour évaluer la réitération :

- en cas de réitération d'une violation ayant fait l'objet d'une injonction aux hébergeurs pour obtenir le retrait des œuvres : l'AGCOM évalue la correspondance effective entre les nouvelles œuvres et celles précédemment retirées ;
- en cas de réitération d'une violation ayant fait l'objet d'une injonction de blocage à l'encontre d'un fournisseur d'accès à internet : l'AGCOM analyse les similitudes entre les noms de domaine, l'identité de l'adresse IP et la structure des sites.

Si la violation précédente avait déjà donné lieu à une injonction aux hébergeurs, l'AGCOM prononce une sanction à leur encontre et informe la police judiciaire. Si la violation précédente avait donné lieu à une injonction à l'encontre des fournisseurs d'accès internet, l'autorité transmet aux fournisseurs d'accès à internet un fichier listant les nouveaux services à bloquer.

LES MESURES JUDICIAIRES DE BLOCAGE

Le système italien prévoit une procédure devant le juge, qui rend caduque toute procédure devant l'AGCOM.

Dans ce cadre, la police douanière et financière (*Guardia di Finanza*) précitée peut soumettre des affaires à l'autorité judiciaire qui peut adopter des mesures de blocage à l'encontre des sites.

Depuis 2016, l'action de la *Guardia Di Finanza* s'est largement développée, si bien que plusieurs sites contre-faisants ont été bloqués.

Sur le plan judiciaire, la jurisprudence italienne en matière de piratage s'est considérablement étoffée.

En juillet 2017, le tribunal de Milan, saisi par le groupe éditorial Mondadori, avait ordonné aux principaux fournisseurs d'accès internet italiens de bloquer l'accès au site internet « dasolo.org » ainsi qu'aux sites ayant un nom de domaine similaire. Suite au transfert des contenus illicites sur un site internet ayant un nom de domaine totalement différent, à savoir « italiashare.info », le tribunal de Milan nouvellement saisi a jugé recevables les demandes du groupe Mondadori et a ordonné la mise en place par les fournisseurs d'accès à internet de mises à jour des mesures de blocage. Ceux-ci devront ainsi bloquer l'accès aux contenus illicites sur simple demande des ayants droit, y compris lorsqu'il s'agit d'un site qui, indépendamment du nom de domaine, conduit aux mêmes violations constatées dans la décision initiale.

S'agissant des sites communément appelés miroirs, dans une décision du 12 avril 2018, le tribunal de Milan a considéré que l'obligation pour les fournisseurs d'accès à internet d'empêcher l'accès aux services déjà qualifiés par un juge comme illégaux sur simple signalement des ayants droit et sans besoin d'une nouvelle décision de justice, est compatible avec l'interdiction prévue par l'article 15 de la directive « commerce électronique » de soumettre les prestataires à une « obligation générale de surveiller les informations qu'ils transmettent ou stockent [ou] à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites ».

L'IMPLICATION DES FOURNISSEURS DE DNS ALTERNATIFS

L'AGCOM a conclu un accord volontaire concernant le service DNS de CISCO en 2019. Aux termes de celui-ci, CISCO s'est engagé à bloquer, pour les internautes utilisant son service depuis l'Italie, les sites visés par une ordonnance de blocage prononcée par l'AGCOM et destinée aux seuls fournisseurs d'accès internet locaux.

L'IMPLICATION DES RÉSEAUX DE DIFFUSION DE CONTENUS

Dans le cadre d'une procédure intentée contre Cloudflare par *Reti Televisive Italiane s.p.a.* (RTI), le tribunal des entreprises de Rome a, par une décision de juin 2019^[10], confirmé en appel que certaines des activités de Cloudflare s'apparentent à des services d'hébergement par opposition à une simple mise en cache, ce qui inclut notamment la fonction par laquelle Cloudflare copie une partie des sites sur son serveur, afin de les rendre accessibles en cas de problèmes techniques avec les fournisseurs d'hébergement des sites.

La décision pose également que Cloudflare avait connaissance de l'existence des activités illicites de ses clients et n'avait par conséquent pas droit au bénéfice du régime de responsabilité limitée prévu pour les intermédiaires techniques. La poursuite délibérée de la fourniture de services par lesquels des infractions au droit d'auteur sont commises, malgré la connaissance de ces activités, peut en effet équivaloir à contribuer à une activité illicite et, par conséquent, empêcher le fournisseur de services de pouvoir bénéficier du régime de responsabilité prévu pour les services d'hébergement diligents. Il a en outre été jugé que Cloudflare ne peut exiger de formalités particulières en ce qui concerne le format des notifications, si ce n'est une information suffisamment détaillée quant à l'infraction constatée.

Cloudflare a ainsi été condamné à payer à RTI 1 000 euros pour chaque jour où il aurait constaté que l'ordonnance a été violée. En revanche, s'agissant de ses autres activités, Cloudflare est qualifié de service de mise en cache pour la plupart de ses activités, par conséquent, l'applicabilité de cette décision à d'autres CDN pourrait être limitée.

En mars 2020, Cloudflare a ensuite été enjoint de mettre en œuvre des mesures de blocage géographique sur le territoire italien de 22 services illicites. En octobre 2020, une injonction dynamique a enjoint plusieurs intermédiaires techniques, dont Cloudflare, de prendre des mesures à l'encontre des noms de domaine actuels et futurs d'un service IPTV illicite visant spécifiquement le public italien, dans le cadre d'une procédure initiée par la ligue de football Serie A et Sky Italy. En défense, Cloudflare avait avancé qu'il ne faisait qu'optimiser le trafic vers le service illicite mais cet argument n'a pas été retenu par le tribunal.

Il faut enfin relever qu'en 2020, Cloudflare a par ailleurs conclu un accord volontaire avec l'autorité publique locale, l'AGCOM, permettant à celle-ci d'avoir connaissance de l'adresse IP et donc de l'hébergeur réel d'un service illicite ou, si le site est hébergé par Cloudflare, lui garantissant que sa notification de l'AGCOM est transmise à l'opérateur du service pour action.

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

L'observation des publicités présentes sur les sites bloqués par l'AGCOM lui permet de relever le but lucratif de l'activité illicite. L'AGCOM a constaté la présence de diverses marques sur les sites illicites visés à savoir de grands constructeurs automobiles, des plateformes de paiement et de paris et même des laboratoires pharmaceutiques.

L'AGCOM a souscrit au projet OMPI visant à créer une base de données centralisée listant des services illicites aux fins de mise en œuvre de l'approche dite « *Follow the money* ».

[10] CloudFlare - CloudFlare Inc. and Reti Televisive Italiane s.p.a. (RTI) R.G.26942/2019, juillet 2019, <http://www.hadopi.info/dj/news/ressources/Italy%20-%20Cloudflare%20Judgment%20Court%20of%20Rome%20July%202019%20.docx>

LES ACTIONS VISANT À RESPONSABILISER LES PLATEFORMES DE PARTAGE DE CONTENUS

Dans une décision du 15 février 2019, le tribunal de Rome a rappelé que les hébergeurs de contenus (en l'espèce Facebook) sont dans l'obligation, dès lors qu'il a été porté à leur connaissance qu'un contenu a été illicitement mis en ligne par un utilisateur, de retirer ou d'empêcher l'accès audit contenu. La Cour suprême italienne a ajouté que les hébergeurs doivent également empêcher la réapparition du contenu illicite sur leur plateforme.

JAPON

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

126,5 POPULATION^[1]
en millions

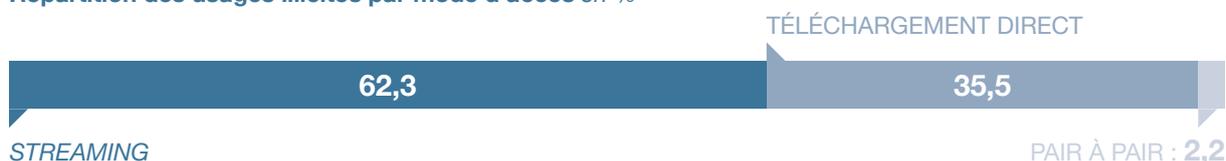
92,7 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

2,4 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

21 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



Le Japon déploie des mesures répressives ciblées à l'égard des internautes. Des mesures de blocage ont pu en outre être mises en œuvre volontairement

par les fournisseurs d'accès à internet en lien avec le gouvernement.

LES ACTIONS VISANT LES INTERNAUTES

LE MÉCANISME D'AVERTISSEMENT DES INTERNAUTES

Un groupement privé, le *Consortium against Copyright Infringement via File-Sharing Software* (CCIF) regroupant des ayants droit et les principaux fournisseurs d'accès à internet, assure la mise en œuvre d'un mécanisme d'avertissement des internautes depuis 2010. Les ayants droit transmettent aux fournisseurs d'accès à internet leurs constats lorsqu'ils détectent des actes de mise à disposition illícites de fichiers protégés. Le fournisseur d'accès à internet se charge ensuite d'adresser à l'internaute un *e-mail* d'avertissement lui demandant de supprimer le fichier mis en partage illégalement. *In fine*, l'internaute qui continue de partager des œuvres peut être arrêté à la suite d'investigations par la police.

LES ACTIONS PÉNALES VISANT LES INTERNAUTES

Au Japon, des sanctions pénales punissent depuis 2012 les internautes qui téléchargent des vidéos ou des morceaux de musique illícitement. Une nouvelle législation, entrée en vigueur le 1^{er} janvier 2021, a étendu ce dispositif aux œuvres littéraires (mangas, magazines, etc.). Celle-ci perpétue la logique de la législation antérieure, avec des sanctions sévères mais accompagnées de garanties permettant d'épargner les téléchargeurs occasionnels, notamment par la nécessité d'une preuve d'une intention malveillante, telle que le téléchargement répétitif et continu.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

LES ACTIONS DE SENSIBILISATION

Le secteur de la musique a créé un label dit « *L mark* » pour aider les internautes à reconnaître les offres légales.

Par ailleurs, un projet *Manga-anime guardians anti-piracy project* a été lancé en juillet 2014 pour lutter contre le piratage des mangas par le ministère de l'Économie, du Commerce et de l'Industrie japonais (METI), l'association de distribution des contenus japonais à l'étranger (CODA) et les acteurs du secteur du manga.

En mars 2018, une campagne de sensibilisation du grand public et des enfants a été lancée en collaboration avec les gouvernements chinois et coréen. Cette campagne avait vocation à sensibiliser la population sur la nécessité de protéger les œuvres audiovisuelles et les personnages populaires issus de mangas et dessins animés. Des posters et des vidéos sont diffusés sur les plateformes comme YouTube et ont vocation à être diffusés aux établissements scolaires. Une nouvelle vidéo autour du personnage Hello Kitty a été diffusée dans le cadre de la réforme du droit d'auteur adoptée en juin 2020^[4].

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES SERVICES ILLICITES ET LEURS OPÉRATEURS

La réforme entrée en vigueur début 2021 prévoit une sanction pénale pour les opérateurs de sites de liens et les fournisseurs d'applications si le site/l'application conduit de manière proactive les utilisateurs à un contenu illicite et est principalement utilisé pour l'exploitation de ce contenu illicite.

S'agissant des contrefacteurs qui mettent en ligne des œuvres sur internet, ceux-ci relevaient déjà du pénal.

Par exemple, en septembre 2019, la police japonaise a arrêté l'opérateur du site Mangamura. Ce site était une des sources les plus populaires de mangas illicites et il a cessé ses activités lorsque le gouvernement japonais a proposé en avril 2018 que les fournisseurs d'accès à internet mettent en œuvre volontairement des mesures de blocage.

LES MESURES DE BLOCAGE

Le blocage de sites au Japon reste une mesure complexe à obtenir.

Le 13 avril 2018, le gouvernement japonais a exhorté les fournisseurs d'accès à internet à mettre en œuvre des mesures de blocage des sites illicites portant atteinte aux droits d'auteur et plus particulièrement aux industries du manga et des dessins animés. Il en a appelé à la coopération des fournisseurs d'accès à internet, lesquels collaborent déjà depuis 2011 avec les autorités pour couper l'accès aux sites internet à caractère pédopornographiques.

Les fournisseurs d'accès à internet japonais ont ainsi volontairement accepté de recourir à des mesures de blocage du type DNS pour bloquer trois des principaux sites visés par le gouvernement et se sont engagés à empêcher l'accès à d'autres sites sur demande du gouvernement. Selon le gouvernement, il s'agit de mesures de blocage d'urgence fondées sur un principe du code pénal japonais qui permet d'agir directement pour « *prévenir un danger immédiat* »^[5].

[4] <https://www.youtube.com/watch?v=-NkJsxVNSIY&feature=youtu.be>

[5] Article 37 du code pénal japonais définit la prévention d'un danger immédiat comme l'« acte accompli de manière inévitable pour empêcher un danger actuel pour la vie, l'intégrité corporelle, la liberté ou la propriété de soi-même ou de toute autre personne. Il n'est pas susceptible de poursuites lorsque le préjudice causé par un tel acte n'excède pas le préjudice qu'il a permis d'éviter ; toutefois, lorsqu'un tel acte cause un préjudice excessif, il peut conduire à une réduction de peine ou à une dispense de la sanction à la lumière des circonstances ».

Ces mesures font cependant l'objet d'importants débats au regard de la Constitution japonaise^[6] et du *Telecommunications Business Act* et les détracteurs de ces mesures estiment que le blocage des sites – malgré leur caractère illicite – serait illégal.

Un client de l'un des principaux fournisseurs d'accès à internet japonais a ainsi attaqué ce dernier en justice afin qu'il cesse ses opérations de blocage au motif qu'elles violeraient le secret des communications ainsi que son contrat d'abonnement qui ne stipule pas que le fournisseur d'accès à internet ait le droit d'interrompre arbitrairement les communications de ses abonnés.

L'IMPLICATION DES MOTEURS DE RECHERCHE

En juillet 2019, Google et les représentants des ayants droit au Japon ont signé un accord devant encadrer des discussions sur le référencement des sites illicites, dans le cadre duquel les parties se sont engagées à échanger sur la lutte contre le piratage sous l'égide de l'agence des Affaires culturelles. En amont de ces travaux, Google et la CODA travaillaient déjà sur le déréférencement des pages d'accueil des sites illicites des résultats du moteur de recherche.

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

En février 2018, neuf organisations d'ayants droit et trois organismes publicitaires ont – avec le soutien du gouvernement japonais – élaboré une liste non publique de sites contrefaisants de manière à assécher une partie de leurs revenus. Cette liste est destinée aux régies publicitaires signataires et permet de supprimer les publicités des annonceurs traditionnels sur ces sites. La liste est mise à jour trimestriellement. Le 9 avril 2020, elle comptait 33 URL.

Par la suite, en suivant les propositions de l'*Intellectual Property Strategy Headquarter* (composé de tous les ministres du gouvernement et des experts en droit de la propriété intellectuelle), la CODA et les trois associations représentant l'industrie de la publicité, ont signé un accord dans le but de réduire le placement de publicités sur les sites contrefaisants en juillet 2019. Cette initiative a été initiée avec le soutien du ministère de l'Économie, du Commerce et de l'Industrie (METI) et renforce l'approche susmentionnée.

Le Japon a rejoint récemment le dispositif de l'OMPI dit « *WIPO ALERT* » qui vise à donner une portée internationale aux approches de démonétisation.

[6] L'article 21 de la Constitution japonaise dispose « la liberté de rassemblement et d'association tout comme la liberté d'expression, de la presse et de toutes autres formes d'expression sont garanties [...] il ne doit y avoir aucune censure, et le secret des moyens de communication ne doit pas être enfreint ».

LITUANIE

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

2,7 POPULATION^[1]
en millions

81,6 % TAUX DE PÉNÉTRATION
INTERNET (2018)^[2]

USAGES ILLICITES^[3]

0,3 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

133 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



Selon une étude de l'EUIPO, la Lituanie est un des pays européens qui a le taux de piratage le plus important^[4]. Selon cette étude, si l'internaute moyen dans l'Union européenne a accédé à des contenus piratés 9,7 fois par mois en 2018, l'internaute lituanien y a accédé 26 fois par mois.

Pour faire face au piratage massif, la Lituanie s'est récemment dotée d'une procédure de blocage administratif. Depuis le 1^{er} avril 2019, la commission de la radio et la télévision (ci-après la commission), une autorité publique en charge de la régulation des diffuseurs de radio et télévision, s'est vu dotée par une loi d'août 2018 d'une nouvelle mission lui permettant d'enjoindre les fournisseurs d'accès à internet de bloquer les sites contrefaisants.

LES ACTIONS VISANT LES INTERNAUTES

Le ministère de la Culture de la république de Lituanie, en collaboration avec l'EUIPO, a créé un portail de référencement de l'offre légale, qui fait partie intégrante du projet Agorateka^[5].

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] https://torrentfreak.com/images/online_copyright_infringement_in_eu_en.pdf

[5] <https://naudoklegaliai.lt/na/en>

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES MESURES ADMINISTRATIVES DE BLOCAGE

La procédure mise en œuvre depuis une loi de 2018 par la commission de la radio et la télévision (ci-après la commission) prévoit que, dans le cadre de leur saisine, les ayants droit sont tenus de tenter de démontrer avoir tenté de mettre fin à la diffusion des contenus protégés *via* :

- une demande écrite, y compris par courrier électronique, à l'administrateur du site internet où le contenu protégé par le droit d'auteur a été rendu illégalement accessible au public, lui demandant de supprimer définitivement ce contenu et de garantir qu'il ne réapparaisse pas ;
- une demande écrite, y compris par courrier électronique, à l'hébergeur du service où le contenu protégé par le droit d'auteur a été rendu illégalement accessible au public, lui demandant de supprimer définitivement le contenu protégé et de garantir que ce contenu n'est pas rendu illégalement accessible au public sur le site internet de manière répétée.

Si le contenu n'a pas été supprimé dans un délai de cinq jours ouvrables à compter de la demande, les ayants droit peuvent ensuite saisir la commission. Le demandeur n'a pas à s'acquitter de ces démarches lorsqu'il demande le blocage d'un site miroir.

Le demandeur peut aussi justifier qu'il ne dispose d'aucune information lui permettant de contacter la/les personne(s) spécifiée(s) et qu'obtenir ces informations n'est pas possible sans encourir des frais déraisonnablement élevés.

Le président de la commission doit ensuite apprécier la recevabilité de la saisine. Le refus de traiter la demande n'exclut pas la possibilité pour le demandeur d'adresser la même demande ultérieurement à la commission, si les circonstances qui ont empêché le traitement de la demande ont été éliminées ou ont cessé d'exister.

Le demandeur est informé de la décision prise par la commission au plus tard dans les sept jours ouvrables à compter de la réception de la demande du demandeur. La décision de la commission de refuser de traiter la demande est motivée et précise les motifs de ce refus.

La demande jugée recevable est ensuite instruite et la décision de la commission est prise dans les 14 jours ouvrables à compter de la date de réception de la demande et des documents la justifiant.

Les critères pris en considération pour déterminer si un site est illégal sont les suivants :

- le *ratio* des contenus illicites présents sur le site ;
- le site a été créé et est utilisé pour diffuser des contenus illicites ;
- si le site diffuse uniquement des contenus protégés par le droit d'auteur ou s'il met également à disposition d'autres types de contenus ;
- si les utilisateurs sont directement ou indirectement incités à promouvoir, télécharger, reproduire ou à utiliser de toute autre manière les contenus illicites ;
- des mesures spécifiques sont mises en œuvre pour supprimer les contenus illicites ;
- l'audience du site ;
- si le site a une activité lucrative ;
- le contenu protégé par le droit d'auteur dont le demandeur demande le retrait est accessible sur des sites de l'offre légale.

Si les critères sont remplis, la commission enjoint aux fournisseurs d'accès à internet de mettre en œuvre des mesures de blocage DNS. Les décisions de la commission doivent alors être approuvées par la cour administrative régionale de Vilnius. Toutes les décisions sont publiées sur le site de la commission.

Le demandeur peut faire appel de la décision adoptée par la commission devant le tribunal administratif régional de Vilnius.

En 2019, la commission a rendu 16 décisions de blocage^[6]. À la suite de ses décisions, la commission effectue un suivi quant à la réapparition de sites dits miroirs. Elle a ainsi procédé en 2019 au blocage de cinq sites miroirs.

LES MESURES JUDICAIRES DE BLOCAGE

Les ayants droit peuvent obtenir le blocage de sites illégaux devant le juge judiciaire. La première décision de blocage a été rendue par la Cour suprême de Lituanie. Cette décision, datée du 4 juillet 2019^[7], a enjoint aux fournisseurs d'accès à internet de bloquer, à leurs frais, l'accès au site de partage de contenus *linkomanija.net*.

L'IMPLICATION DES MOTEURS DE RECHERCHE ET DES FOURNISSEURS DE SERVICES DNS ALTERNATIFS

Des échanges ont eu lieu entre des représentants de la commission et Google en 2019 afin d'envisager la suppression des résultats du moteur de recherche des sites bloqués mais également des sites dits miroirs des sites bloqués du service de DNS alternatif de Google. Les représentants de Google ont répondu positivement à la première requête de la commission.

[6] Rapport d'activité 2019 de la commission de la radio et la télévision :

https://www.rtk.lt/uploads/documents/files/Annual%20reports/LRTK%202019%20m%20veiklos%20ataskaita_EN_JD_rev2.pdf

[7] Cour Suprême de Lituanie, 4 juillet 2019, Vilnius, civil case n° e3k-3-236-969/2019,

<http://www.hadopi.info/dj/news/ressources/4%20LIT%20190604%20Supreme%20Court,%20Linkomanija.net,%204%20July%202019%20EN.docx>

MEXIQUE

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

128,9 POPULATION^[1]
en millions

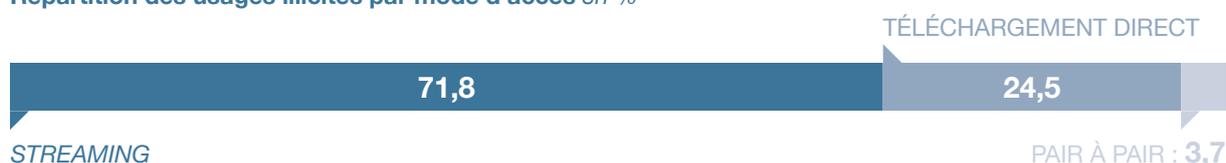
70,1 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

2,7 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

30 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illicites par mode d'accès en %



Si Spotify a nommé le Mexique « capitale du *streaming* » fin 2018, le piratage y est cependant une pratique répandue.

Le Mexique devrait engager une série de réformes destinées à lui permettre d'accentuer le degré de

protection accordé aux œuvres sur internet, notamment à la suite de l'accord tripartite conclu par le Mexique avec les États-Unis et le Canada (dénommé USMCA, pour *U.S.-Mexico-Canada Agreement*) et ratifié par le Mexique fin 2019.

LES ACTIONS VISANT LES INTERNAUTES

La loi mexicaine sur les télécommunications interdit aux fournisseurs d'accès à internet de divulguer les informations personnelles de leurs abonnés aux ayants droit afin que ceux-ci initient une action civile à leur égard – cette loi les soumettant cependant à un devoir de coopération dès lors qu'ils ont reçu une injonction émanant de toute autorité compétente.

Les fournisseurs d'accès à internet se sont de plus en plus montrés réticents à insérer dans leur contrat d'abonnement une clause permettant la résiliation du contrat en cas d'atteinte commise par l'abonné aux droits de propriété intellectuelle, sur le modèle de ce qui est prévu dans la loi américaine.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES SERVICES ILLICITES ET LEURS OPÉRATEURS

Le procureur général de la République est en charge de l'application des mesures pénales au niveau fédéral. Il est toutefois difficile pour les ayants droit d'engager des actions au pénal contre les opérateurs de sites contrefaisants car le code pénal mexicain exige de prouver un « avantage économique direct » pour le contrevenant.

LES MESURES ADMINISTRATIVES DE BLOCAGE

Depuis 2013, des injonctions de blocage administratives peuvent être prononcées par l'Institut mexicain de la propriété industrielle (IMPI), qui est notamment responsable de l'enregistrement des droits d'auteur et dispose d'un pouvoir de médiation entre ayants droit et utilisateurs. La première injonction a été prononcée en 2014 à l'égard d'un site contrefaisant, assortie d'une amende à l'encontre de l'administrateur du site. Un tribunal a par la suite confirmé l'action et l'autorité de l'IMPI.

En 2015, l'IMPI a agi contre le site *mymusic.com*, sur saisine de l'Association mexicaine des producteurs de phonogrammes et de la Société mexicaine des auteurs et compositeurs. Cette affaire a été transmise aux autorités judiciaires lorsque deux fournisseurs d'accès à internet ne se sont pas conformés à l'injonction de l'IMPI. Le tribunal a levé l'injonction, ce qu'a confirmé la Cour suprême, au motif que la mesure était disproportionnée au regard de la présence, au sein du site litigieux, de contenus ne contrevenant pas au droit d'auteur.

Une réforme en cours d'adoption devrait également permettre à l'IMPI de notifier les opérateurs de sites illicites, qu'ils soient localisés au Mexique ou à l'étranger, par courrier électronique, dans les hypothèses où une infraction au droit d'auteur est commise par un moyen de communication électronique. Pour l'instant, le droit mexicain oblige l'IMPI à effectuer ces notifications à leur adresse physique, ce qui s'avère souvent impossible.

L'IMPLICATION DES INTERMÉDIAIRES TECHNIQUES

En l'absence de régime spécifique de responsabilité des intermédiaires techniques, en novembre 2009, 37 organisations représentant le secteur de la création, les titulaires de droit et les sociétés de gestion collective ont créé la Coalition pour l'accès légal à la culture (CLAC), destinée à promouvoir et défendre les droits d'auteur et les droits voisins menacés par le piratage physique et en ligne, en collaboration avec différentes entités gouvernementales et autorités fédérales. L'un des principaux objectifs de cette coalition était de développer la coopération avec les fournisseurs d'accès à internet. Plus de dix ans après sa création, la coalition n'est cependant toujours pas parvenue à trouver un accord avec les intermédiaires techniques et en particulier les fournisseurs d'accès à internet, et un dispositif de blocage administratif a été créé en parallèle. En revanche, certains ayants droit parviennent à obtenir des retraits de contenus auprès de prestataires locaux, voire la coopération du registre local, mais il apparaît que seule une loi permettra de mettre en place une coopération réelle de l'ensemble des intermédiaires techniques.

NOUVELLE-ZÉLANDE

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

4,8 POPULATION^[1]
en millions

90,8 % TAUX DE PÉNÉTRATION
INTERNET (2017)^[2]

USAGES ILLICITES^[3]

0,43 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

98 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



La Nouvelle-Zélande s'est dotée en 2011 d'un mécanisme de type réponse graduée en trois étapes, aujourd'hui abandonné. S'agissant de la lutte contre les services contrefaisants, alors que les ayants droit déplorent ne pas avoir dans leur *corpus* juridique de dispositif qui permette expressément de demander aux intermédiaires le blocage

de sites, le gouvernement néo-zélandais a lancé une consultation sur la loi régissant le droit d'auteur et les droits voisins de novembre 2018 à avril 2019, portant notamment sur la lutte contre le piratage. Des tables rondes destinées à favoriser le débat public ont parallèlement été organisées.

LES ACTIONS VISANT LES INTERNAUTES

LE DISPOSITIF D'AVERTISSEMENT DES INTERNAUTES

La Nouvelle-Zélande s'était dotée en 2011 d'un dispositif législatif de lutte contre le partage illégal de fichiers sur les réseaux pair à pair.

La procédure prévoyait que les ayants droit pouvaient saisir les fournisseurs d'accès à internet de notifications faisant état de violations des droits d'auteur. Ceux-ci devaient adresser aux internautes concernés une notification. Après trois notifications adressées, les ayants droit pouvaient introduire une action en justice pour obtenir réparation.

La sanction susceptible d'être infligée par le tribunal pouvait aller jusqu'à 15 000 dollars néo-zélandais (soit 9 760 euros environ).

En pratique, seul le secteur de la musique a fait usage du dispositif, le secteur audiovisuel ayant notamment estimé que celui-ci coûtait trop cher (25 dollars néo-zélandais par notification, soit environ 16 euros). La *Recording Industry Association of New Zealand* (RIANZ), aujourd'hui devenue *Recorded Music NZ*, a fait envoyer des notifications de 2011 à mi-2016.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

15 500 notifications ont été envoyées par les ayants droit de la musique, 51 internautes poursuivis en justice, pour 21 affaires finalement jugées.

Les ayants droit ont choisi de cesser d'utiliser le mécanisme de réponse graduée principalement au regard de ses coûts trop importants et du fait du déclin des pratiques de pair à pair.

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES SERVICES ILLICITES ET LEURS OPÉRATEURS

S'agissant des actions répressives contre les services illicites, le principal fournisseur de télévision par abonnement en Nouvelle-Zélande, Sky Network Television, a réussi à empêcher, dans deux procédures distinctes, la publicité et la vente en Nouvelle-Zélande de boîtiers configurés à des fins de piratage permettant d'accéder illicitement à des services de télévision par abonnement. Cet objectif a été n'atteint non pas tant au regard du droit d'auteur qu'en invoquant l'illégalité des allégations commerciales des vendeurs en vertu de la législation sur la protection des consommateurs.

LES MESURES DE BLOCAGE

Un projet de réforme visant à lutter contre les sites contrefaisants est actuellement à l'étude par le gouvernement néo-zélandais.

PAYS-BAS

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

17,1 POPULATION^[1]
en millions

93,3 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

1 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

60 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illégitimes par mode d'accès en %



Aux Pays-Bas, l'action anti-piratage est essentiellement conduite par les ayants droit, *via* une fondation, (*Stichting*) BREIN, l'association de lutte anti-piratage locale regroupant les ayants droit de tous les secteurs de l'industrie culturelle (créateurs et producteurs).

La BREIN conduit des actions tant à l'égard des internautes qui mettent illégalement à disposition des

contenus que des services eux-mêmes et, lorsque que cela est nécessaire, des actions impliquant les intermédiaires sont également engagées. Les actions conduites par la BREIN sont retracées dans le rapport annuel^[4] de la BREIN.

Par ailleurs, la directive droit d'auteur dans le marché unique numérique du 17 avril 2019 a été transposée par une loi de décembre 2020.

LES ACTIONS VISANT LES INTERNAUTES

Aux Pays-Bas, les ayants droit ont essentiellement mis en place une approche indemnitaire qui vise à transiger avec les internautes qui mettent à disposition de nombreux contenus.

LE DISPOSITIF DE MISE EN DEMEURE INDEMNITAIRE

La BREIN conduit des actions à l'égard des internautes qui mettent beaucoup d'œuvres à disposition,

par différents moyens (groupes Facebook, chaînes YouTube, *cyberlockers*, Usenet et logiciels de pair à pair...). S'agissant plus spécifiquement des réseaux pair à pair, la BREIN s'est dotée d'un logiciel dédié qui permet d'identifier les adresses IP des *primo-uploaders* sur les réseaux pair à pair.

L'objectif est alors de parvenir à des accords transactionnels avec les contrefacteurs ou, à défaut, d'engager des poursuites. La conclusion de transactions pour les actes de contrefaçon passés est subordonnée par ailleurs à l'engagement, sous astreinte, de ne pas

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] Rapport annuel 2019 de la BREIN : <https://stichtingbrein.nl/english-brein-review-2018/>

porter atteinte au droit d'auteur à l'avenir. Dans le cadre de ces transactions, l'*uploader* peut par exemple être conduit à publier ou envoyer des messages de type « *La mise à disposition et le téléchargement non autorisés sont illicites et coûtent beaucoup d'argent à l'industrie créative* ».

La BREIN négocie ces transactions directement avec les internautes. Les sommes demandées dépendent de l'étendue de l'infraction commise et de la situation personnelle de l'internaute. En 2019, la BREIN a conclu 29 transactions portant engagement de cessation et d'abstention des activités illicites assortis de clauses de pénalité et du paiement d'une indemnisation d'un montant moyen de plusieurs milliers d'euros par cas.

Certains cas sont cependant portés en justice. Ainsi, en 2019, une juridiction d'Utrecht a condamné un des plus importants *uploaders* néerlandais et a enjoint celui-ci à donner toutes les informations concernant son activité et les personnes impliquées sous peine de devoir payer une amende de 150 000 euros.

Certains ayants droit (dont le distributeur de films *Dutch FilmWork* – « DFW ») souhaiteraient par ailleurs envoyer des demandes d'indemnisation à l'ensemble des internautes. Fin 2017, l'autorité en charge de la protection des données personnelles a autorisé la collecte de données personnelles aux fins d'envoyer des demandes de compensation financière. DFW a cependant été débouté en première instance et en appel lors d'une procédure engagée à l'encontre d'internautes. Les juges ont estimé que la protection des données personnelles des titulaires de comptes devait prévaloir dans la mesure où les demandes de DFW n'étaient pas claires et où une seule atteinte au droit d'auteur était en cause^[5]. DFW a formé un pourvoi devant la Cour suprême néerlandaise fin 2019. Cette décision de justice ne concerne pas la BREIN qui ne traite que les cas des contrefacteurs ayant porté atteinte au droit d'auteur à plusieurs reprises.

LE DISPOSITIF D'AVERTISSEMENT DES INTERNAUTES

En décembre 2020, la BREIN a lancé une campagne visant à changer le comportement des *uploaders* de contenus sur *BitTorrent*, consistant en l'envoi d'avertissements éducatifs aux seuls utilisateurs de *BitTorrent* mettant de nombreux contenus à disposition et/ou mettant à disposition des contenus de façon prolongée. Cette campagne a vocation à durer six mois, en ciblant

un maximum de 1 000 adresses IP par mois. Au-delà de cette période, la BREIN envisage des mesures coercitives contre les utilisateurs dont l'adresse aura été relevée au moins trois fois, en priorisant ceux qui ont partagé des contenus s'adressant spécifiquement au marché néerlandais.

Un logiciel dédié est utilisé par les ayants droit aux fins de détection des internautes ciblés par la campagne. Un certain nombre de critères permettront ensuite de sélectionner les destinataires des avertissements : il faudra notamment que le contenu partagé soit la propriété d'un membre de la BREIN, que l'adresse IP appartienne à un fournisseur d'accès néerlandais et enfin que cette dernière ait été relevée au moins deux fois dans une période de quatre semaines, avec un intervalle d'au moins sept heures.

S'agissant des modalités de traitement des demandes d'identification des adresses IP par les fournisseurs d'accès à internet, la réglementation néerlandaise ne prévoit aucune compensation financière visant à indemniser les opérateurs au titre de ces prestations d'identification. Des fournisseurs d'accès à internet exigeraient toujours une décision de justice leur enjoignant de fournir les données d'identification aux ayants droit. La question qui reste en suspens concerne donc la participation des différents fournisseurs d'accès à internet au dispositif.

LES ACTIONS DE SENSIBILISATION

Aux Pays-Bas, les titulaires de droits fournissent du matériel éducatif aux écoles, avec une subvention du ministère de la Culture, des Sciences et de l'Éducation ainsi que de l'EUIPO. Deux sites dédiés^[6] comportant des vidéos explicatives sur le droit d'auteur notamment ont ainsi été créés.

LA PROMOTION DE L'OFFRE LÉGALE

L'industrie cinématographique a lancé en février 2017, après la création d'un portail référençant les plateformes de l'offre légale, un moteur de recherche de l'offre légale par œuvre qui vise les internautes qui cherchent une œuvre audiovisuelle en particulier. L'originalité de cet outil est qu'il vise aussi les internautes qui cherchent une œuvre illégalement mise à disposition. En effet, la description des œuvres comporte des mots-clés comme « *torrent* » ou « *téléchargement illégal* » pour

[5] <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHARL:2019:9352>

[6] www.auteursrecht.nl et <https://www.auteursrechtvoorjou.nl/>

que les internautes qui utilisent ces mots-clés puissent être redirigés sur l'offre légale. Ensuite, pour chaque œuvre audiovisuelle, dans la description, un message est disponible pour dissuader les internautes de se

tourner vers l'offre illégale de type « *Ne téléchargez pas illégalement. Dirigez-vous vers une offre légale sûre et rapide* ».

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES SERVICES ILLICITES ET LEURS OPÉRATEURS

La BREIN a notamment initié une série d'actions contre les vendeurs de boîtiers équipés d'un lecteur audiovisuel multimédia préconfigurés à des fins de piratage. Dans ce cadre, la CJUE, saisie d'une question préjudicielle, a considéré que la commercialisation de tels boîtiers ainsi configurés constituait un acte de communication au public qui doit être préalablement autorisé^[7] sauf à constituer une violation du droit d'auteur.

À la suite de cette décision, la BREIN a obtenu que plus de 300 acteurs de cet écosystème illicite cessent leurs activités. Ce chiffre inclut les vendeurs d'abonnements IPTV illégaux avec et sans décodeurs. Des injonctions ont été obtenues contre des sociétés qui ont continué leurs activités, estimant que la fourniture d'un lien aux utilisateurs finaux leur permettant d'accéder à des contenus illégaux est en elle-même un acte illégal de communication au public. 23 vendeurs d'abonnements illégaux à l'IPTV ont de plus été arrêtés en 2019.

Par ailleurs, Eurojust et Europol ont coordonné l'exécution d'une demande d'aide judiciaire de la police fiscale italienne et, sur cette base, la police néerlandaise a désactivé chez un important fournisseur d'hébergement néerlandais 93 serveurs en lien avec le service d'IPTV illicite Xstream Codes, ce qui a notamment permis le démantèlement de ce service en septembre 2019.

LES MESURES JUDICIAIRES DE BLOCAGE

En 2015, la Cour suprême néerlandaise avait posé une question préjudicielle^[8] à la Cour de justice de l'Union européenne pour savoir si le site « *The Pirate Bay* », qui est un site de liens *torrent*, porte lui-même atteinte au droit d'auteur et, dans le cas contraire, si le blocage du site est tout de même possible.

La Cour^[9] a jugé le 14 juin 2017 que « *la fourniture et la gestion d'une plateforme de partage en ligne d'œuvres protégées telle que « The Pirate Bay » peut constituer une violation du droit d'auteur* » et qu'il est possible de mettre en cause le site « *The Pirate Bay* » pour les liens *BitTorrent* qui y sont référencés.

La BREIN a obtenu en justice des premières mesures de blocage à la suite de cette décision^[10]. Après une décennie de litiges, le 2 juin 2020, la cour d'appel d'Amsterdam^[11] a ainsi ordonné à deux des principaux fournisseurs d'accès à internet de bloquer l'accès aux noms de domaine et adresse IP permettant d'accéder à « *The Pirate Bay* ». Lorsqu'un site est bloqué, un message de redirection vers l'offre légale est mis en place.

Une décision d'octobre 2020 est venue compléter celle de juin, ordonnant cette fois aux fournisseurs d'accès à internet de bloquer les proxys et sites miroirs.

[7] CJUE, 26 avril 2017, *Stichting Brein c/ Jack Frederik Wullems dite « Filmspeler »*, C-527/15.

[8] Cour suprême des Pays-Bas, 13 novembre 2015, *le Hoge Raad der Nederlanden, Stichting Brein contre Ziggo BV, XS4All Internet BV*.

[9] CJUE, 14 juin 2017, C-610/15 - *Stichting Brein/Ziggo BV, XS4All Internet BV dite « The Pirate Bay »*.

[10] Une première décision de septembre 2017 a ordonné ces mesures à l'égard des deux principaux fournisseurs d'accès internet puis une décision de janvier 2018 a ordonné la même mesure à l'égard d'autres fournisseurs d'accès à internet.

[11] Cour d'appel d'Amsterdam, 2 juin 2020, 200.243.005/01 *ZIGGO B.V., and XS4ALL INTERNET B.V., vs STICHTING BREIN [BREIN FOUNDATION]*, - <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHAMS:2020:1421&showbutton=true>

L'IMPLICATION DES FOURNISSEURS DE SERVICES D'HÉBERGEMENT

En 2019, la BREIN a notamment fait fermer 564 sites ou services, principalement avec la coopération de fournisseurs d'hébergement néerlandais, et a fait fermer 12 groupes Facebook sur lequel étaient partagées des œuvres protégées par le droit d'auteur.

En octobre 2019, la BREIN, en collaboration avec la MPA et l'ACE, a obtenu en justice que cinq intermédiaires techniques domiciliés ou ayant des serveurs aux Pays-Bas déconnectent les serveurs utilisés par le service *Moonwalk*, ce qui a conduit à sa fermeture. *Moonwalk* était un *Content Delivery Network* qui mettait à disposition une infrastructure technique de stockage et de diffusion de contenus audiovisuels ainsi que des services annexes. Cette infrastructure servait de base à de nombreux sites tiers par l'intermédiaire desquels les utilisateurs pouvaient accéder aux œuvres piratées. *Moonwalk* fournissait ainsi les ressources et les contenus illicites à environ 80 % des sites russes connus de *streaming* illégal, et conserve les preuves en lien avec ce service^[12].

L'infrastructure internet néerlandaise est utilisée par de nombreux services illégaux rentables dans le monde entier. Bien que les fournisseurs néerlandais coopèrent généralement bien pour supprimer les sites et les flux en direct, les services illégaux persistent. C'est pourquoi la BREIN estime nécessaire d'identifier les personnes impliquées afin qu'elles soient tenues pour responsables. Dans la pratique, cependant, les fournisseurs néerlandais qui hébergent des services illégaux ne disposent pas des données d'identité correctes de leurs clients ou ont des clients qui revendent leurs services d'hébergement et qui, à leur tour, ne disposent pas d'informations permettant d'identifier le véritable contrevenant. Cela permet en fait aux services illégaux d'utiliser l'infrastructure néerlandaise de manière anonyme et en toute impunité. C'est pourquoi la BREIN promeut la nécessité pour les in-

termédiaires techniques néerlandais de vérifier l'identité de leurs clients et d'exiger contractuellement la même chose de leurs clients qui revendent leurs services. La BREIN promeut également cette exigence au niveau européen. En 2020, la BREIN a ainsi intenté, en collaboration avec la MPA, des actions contre trois intermédiaires techniques pour qu'ils adoptent la doctrine dite « *Know your customer* » et qu'ils soient disposés à transmettre les informations relatives à l'identité de leurs clients aux ayants droit, notamment en cas de violation de la propriété intellectuelle, et exigent la même chose de leurs revendeurs.

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

La BREIN collabore avec les intermédiaires de paiement et des acteurs de la publicité en ligne afin de leur demander de cesser de fournir leurs services aux sites contrefaisants.

LA LUTTE CONTRE LE PIRATAGE DE CONTENUS SPORTIFS

En janvier 2018, la *Premier League* anglaise a obtenu devant la cour de La Haye que l'hébergeur néerlandais Ecatel cesse de fournir le service facilitant le visionnage illicite de ses matchs sous 30 minutes après la notification de la *Premier League*. La mesure devait être temporaire et limitée à la durée des rencontres. Cette décision faisait suite à de nombreuses demandes de retrait ignorées par l'hébergeur et s'appuie sur les droits de propriété intellectuelle de la *Premier League* sur les diffusions. La portée pratique de cette mesure est cependant à nuancer dans la mesure où Ecatel n'existait plus au moment du jugement, mais le principe de la décision constitue toutefois une victoire significative pour les ayants droit.

[12] <https://stichtingbrein.nl/brein-serves-ex-parte-order-on-dutch-hosting-providers-for-80-of-russian-streaming-sites/>

PÉROU

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

33 POPULATION^[1]
en millions

60 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

1 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

49 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



Des millions d'utilisateurs péruviens consomment de manière illicite des biens culturels chaque mois^[4]. Lors du sommet dédié à la lutte contre le piratage qui s'est tenu à Lima en octobre 2017, les *leaders* de l'industrie ont estimé que ces usages illicites au Pérou engendrent des pertes s'élevant à plus de 150 millions de dollars, soit plus de 131,7 millions d'euros.

Face à ce phénomène, les instances péruviennes ont réagi pour procéder à la fermeture de sites établis au Pérou et à l'arrestation de leurs administrateurs. Des actions administratives impliquant les intermédiaires sont également mises en œuvre par l'Institut national de défense de la concurrence et de la protection de la propriété intellectuelle

(INDECOPI)^[5], l'autorité publique locale rattachée aux services du Premier ministre qui est chargée de la lutte contre le piratage.

Un projet de loi destiné à renforcer la protection des droits de propriété intellectuelle, qui créera notamment un programme de récompenses visant à obtenir des informations sur l'identité des principaux responsables d'actes de piratage, a été soumis à consultation en janvier 2020. Il comporte quatre axes principaux : la création d'un programme national de sensibilisation pour les publics scolaires, la promotion de l'offre légale, le durcissement des sanctions encourues ainsi que la promotion d'une approche collaborative à l'égard des intermédiaires du piratage.

LES ACTIONS VISANT LES INTERNAUTES

L'INDECOPI fait partie de la commission de lutte contre la criminalité et le piratage, une commission permanente multisectorielle présidée par le ministère de la Production. Cette commission est un organe de coor-

dination qui réunit l'INDECOPI, le pouvoir judiciaire, le ministère public, la police nationale et les douanes. Les accords adoptés ont un caractère contraignant pour tous les secteurs et organismes publics et privés qui,

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] Source : Étude menée en janvier 2016 « South America Television Piracy Landscape For Alianza Contra La Piratería de Televisión Paga ».

[5] Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.

par l'intermédiaire de leurs représentants, composent la commission. Les activités de la commission comprennent des groupes de travail thématiques multisectoriels, dont le but est de mettre en place des mécanismes de coordination qui permettront à terme de décourager et de réprimer la contrefaçon et le piratage dans le cadre d'une alliance avec le secteur privé. Des groupes de travail ont été mis en place pour faciliter une meilleure coordination entre les autorités publiques et le secteur privé, dont notamment un groupe dédié à la lutte contre le piratage de contenus audiovisuels.

LES ACTIONS DE SENSIBILISATION

L'INDECOPi conduit des actions de sensibilisation. Un programme intitulé « *Je respecte la propriété intellectuelle et je refuse la contrebande* » est actuellement en phase d'expérimentation dans les lycées afin d'encourager la future génération d'actifs à respecter la propriété intellectuelle, et générer une culture de respect. Le projet de loi actuellement à l'étude prévoit notamment la création d'un programme national de sensibilisation pour les publics scolaires. La politique nationale en matière de propriété intellectuelle en cours de discussion devrait également comprendre un volet sur les raisons qui poussent le grand public à consommer illégalement, dans l'objectif de lutter contre ces comportements.

Chaque année, l'INDECOPi mène diverses activités de formation, dans le cadre de réunions physiques et en ligne, à l'intention des procureurs, des juges, de la police nationale, des autorités douanières et de toute autre autorité dont la compétence est liée à la protection de la propriété intellectuelle, dans le but de développer, renforcer ou améliorer leurs capacités techniques.

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES SERVICES ILLICITES ET LEURS OPÉRATEURS

Un bureau spécial du procureur est en charge de lutter contre les atteintes aux droits de propriété intellectuelle.

En 2017, un ayant droit a déposé une plainte au motif que trois sites internet mettaient à disposition du public des films et des émissions télévisées sans son autorisation. Le 8 septembre 2017, le juge a autorisé la perquisition aux domiciles et sur les lieux de travail des suspects et leur arrestation. Le bureau du procureur a mené l'enquête avec la division des crimes liés à la haute technologie. Le mandat couvrait également la confiscation des biens matériels et des noms de domaine.

Le site a immédiatement été fermé. Concomitamment, des bannières informatives ont été publiées sur les sites, indiquant que le nom de domaine était suspendu par ordre de la seconde cour pénale de Lima dédiée à la propriété intellectuelle et du bureau spécial du procureur pour les crimes liés à la propriété intellectuelle.

Cette décision est une première au Pérou et constitue un précédent en matière pénale : le juge a reconnu que la mise à disposition du public de contenus protégés sans l'autorisation du titulaire de droit est illicite et les revenus publicitaires de ces sites suffisent à démontrer le caractère intentionnel.

LES MESURES ADMINISTRATIVES DE BLOCAGE

La législation péruvienne permet aux titulaires du droit d'engager des procédures administratives devant l'INDECOPi, qui peut notamment prendre diverses injonctions contre les intermédiaires techniques. Le délai moyen pour l'adoption des mesures de blocage est de cinq jours ouvrables.

L'IMPLICATION DES BUREAUX D'ENREGISTREMENT ET DES REGISTRES

Dans le cadre de la législation précitée, qui permet à l'INDECOPi d'enjoindre aux fournisseurs d'accès à internet de bloquer des sites, l'INDECOPi peut également enjoindre aux bureaux d'enregistrement et aux registres. Au cours de l'année 2019, grâce au travail coordonné entre l'INDECOPi et le pouvoir judiciaire, 18 sites enfreignant les droits d'auteur sur la musique et les films ont ainsi été désactivés.

Récemment, l'INDECOPi a enjoint à GoDaddy – l'un des principaux bureaux d'enregistrement de noms de domaine du monde, basé aux États-Unis – de suspendre les noms de domaine de sites contrefaisants, et le bureau a mis en œuvre la demande de l'INDECOPi.

L'INDECOPi cherche par ailleurs à conclure un accord avec le bureau d'enregistrement précité GoDaddy, afin de donner un cadre à la collaboration informelle qui s'est déjà nouée entre les deux entités, dans le but que l'INDECOPi puisse demander la suspension de noms de domaine enregistrés aux États-Unis mais visant le public péruvien.

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

Un accord est par ailleurs en cours de négociation avec l'écosystème publicitaire dont l'objectif est de mettre en œuvre une démarche de type « *Follow the money* ». L'INDECOPi a en outre adhéré au dispositif « *WIPO ALERT* » qui vise à implémenter l'approche dite « *Follow the money* » au niveau international.

LA LUTTE CONTRE LE PIRATAGE DE CONTENUS SPORTIFS

Le 15 avril 2019, l'INDECOPi et la Ligue nationale de football professionnel (*La Liga*) d'Espagne^[6] ont signé un accord de coopération pour lutter contre le piratage dans le domaine du sport. *La Liga* a accordé à l'INDECOPi une licence d'utilisation du logiciel Lumière, spécialisé dans la détection des émissions sportives illégales. La ligue de football espagnole a en effet développé pour son application officielle pour smartphones des outils permettant d'accéder au micro et aux données de géolocalisation de l'utilisateur. Dès lors que ce dernier consent à l'activation de ces fonctions, l'application – qui n'est activée que lorsque *La Liga* retransmet un match – géolocalise les sons pour vérifier notamment si le match est diffusé chez un diffuseur agréé. Les sons ainsi récupérés par l'application sont automatiquement convertis dans un code binaire, rendant impossible la reconstitution des enregistrements.

En 2018, l'INDECOPi a enjoint aux fournisseurs d'accès à internet de bloquer le site de retransmission en direct de contenus sportifs *Rojadirecta* à la suite d'une demande de Fox Sports Latin America. L'INDECOPi a pris en compte, pour prononcer son injonction, différents facteurs, dont le fait que le site porte atteinte au droit d'auteur en fournissant consciemment des liens vers différents événements sportifs, nonobstant la question de savoir si le contenu était transmis à partir du site ou non. Deux autres sites de *streaming* en direct de contenus sportifs ont également été bloqués par la suite.

[6] <https://repositorio.indecopi.gob.pe/bitstream/handle/11724/6761/NP%20190415%20Convenio%20INDECOPi%20%20-%20LaLiga.pdf?sequence=1&isAllowed=y>

PORTUGAL

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

10,2 POPULATION^[1]
en millions

75,4 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

0,6 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

72 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



Au Portugal, un dispositif de blocage des sites illícites est mis en œuvre dans le cadre d'un *memorandum* (MoU) conclu en juillet 2015 entre l'Inspection générale des affaires culturelles^[4] (IGAC, entité rattachée au ministère de la Culture), l'Association portugaise des opérateurs de télécommunications (APRITEL), les ayants droit regroupés au sein du MAPINET (association anti-piratage plurisectorielle), la direction générale de la consommation, des représentants du secteur de la publicité et l'entité portugaise gérant les noms de domaine sous l'extension locale (« .pt »). Depuis début 2019, un *addendum* à ce MoU

permet également le blocage DNS temporaire des retransmissions sportives. En outre, des injonctions judiciaires de blocage IP temporaire en temps réel applicables pour une saison entière ont été prononcées au second semestre 2019.

Enfin, il faut relever que, comme dans d'autres pays européens, la transposition de la directive 2019/790 sur le droit d'auteur dans le marché unique numérique pourrait être au Portugal l'occasion de réformer le dispositif public de lutte contre le piratage.

LES ACTIONS VISANT LES INTERNAUTES

Le MoU précité prévoyait en outre la création et l'administration d'un agrégateur de l'offre légale.^[5] La création de cette plateforme s'est inscrite dans le cadre du projet de l'EUIPO d'agrégateur européen de l'offre légale (Agorateka).

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] L'IGAC est l'entité spécialisée dans la protection du droit d'auteur et des droits voisins sous le contrôle du ministère de la Culture. Ils ont aussi pour mission notamment d'enregistrer les œuvres et de superviser les sociétés de gestion collectives.

[5] www.ofertaslegais.pt/na

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES MESURES ADMINISTRATIVES DE BLOCAGE

La législation portugaise transposant la directive 2000/31/CE du 8 juin 2000 dite « commerce électronique » prévoit que l'autorité publique peut constater une atteinte au droit d'auteur, dans le cadre d'un règlement provisoire des différends, et enjoindre les fournisseurs d'accès à internet de bloquer un site. Toutefois, le recours au juge s'imposait^[6] pour rendre ces mesures exécutoires.

Afin de faciliter les mesures de blocage, les fournisseurs d'accès à internet, qui sont souvent également ayants droit au Portugal, ont accepté de négocier un accord aux fins de mettre en place des mesures de blocage sous le contrôle de l'autorité publique. La procédure mise en place par le MoU prévoit cinq étapes :

- à titre liminaire, le MAPINET notifie les contenus illégaux à la plateforme et demande leur retrait. À ce stade, les services visés par le MoU sont ceux dédiés à la communication au public d'œuvres protégées. Les services illégaux de *stream ripping* ne sont pas visés par le MoU ;
 - c'est seulement en l'absence de réponse ou en cas de réponse négative que le MAPINET réunit des éléments visant à attester que le site est contrefaisant et saisit l'IGAC. Le MoU prévoit que pour chaque site faisant l'objet d'une transmission à l'IGAC, les ayants droit doivent démontrer soit que plus de 500 œuvres protégées sont disponibles sur le site, soit que plus de 2/3 de contenus hébergés sont contrefaisants ;
 - une fois saisie, l'IGAC effectue un contrôle rapide de chaque site par échantillonnage et, dans l'hypothèse où le site se révèle être massivement contrefaisant, demande aux fournisseurs d'accès à internet de procéder au blocage DNS du site ;
 - les fournisseurs d'accès à internet disposent de quinze jours pour procéder au blocage. Ils supportent les coûts du blocage bien que le MoU prévoit une possibilité de partage des frais. Ils diffusent un message indiquant que le site a été bloqué par l'IGAC ;
- l'IGAC doit ensuite transmettre les dossiers concernant les services bloqués au procureur, le droit portugais comportant un équivalent à l'article 40 du code de procédure pénale français imposant aux autorités publiques de dénoncer les crimes et délits dont ils ont connaissance. En pratique, les services pour lesquels il sera réellement possible d'engager une procédure pénale au Portugal au regard de la localisation des administrateurs de ces sites lui sont spécifiquement signalés.

Les mesures de blocage sont en vigueur pendant une durée d'un an. À l'expiration de ce délai, les ayants droit doivent faire une nouvelle demande de blocage. L'actualisation des demandes de blocage avant ce délai reste donc compliquée.

Un des enjeux pour les fournisseurs d'accès à internet dans la conclusion du MoU était non pas tant de limiter le nombre de sites à bloquer mais de rationaliser le traitement des demandes de blocage pour en minimiser l'impact en termes de traitement et éviter la création d'une équipe dédiée.

C'est donc au regard de cette considération que le MoU prévoit que les ayants droit doivent centraliser leur demande *via* le MAPINET et transmettre les demandes de blocage au maximum deux fois par mois (en début de mois et le 15 du mois). Ces demandes doivent concerner au minimum 50 nouveaux sites. En pratique, les ayants droit ne transmettent des demandes qu'une fois par mois, pour au moins 50 sites.

L'ACTUALISATION DES MESURES ADMINISTRATIVES DE BLOCAGE

Il n'existe pas de procédure spécifique pour obtenir le blocage d'un service de contournement mais la procédure classique de blocage étant relativement rapide, ceux-ci peuvent être soumis à l'IGAC à l'occasion de la chaque saisine mensuelle du MAPINET. Les mêmes éléments de preuve que pour les services d'origine sont fournis à l'IGAC par les ayants droit.

[6] DL n. ° 7/2004, de 07 de Janeiro, COMÉRCIO ELECTRÓNICO NO MERCADO INTERNO E TRATAMENTO DE DADOS PESSOAIS, art. 18.

LA LUTTE CONTRE LE PIRATAGE DE CONTENUS SPORTIFS

Depuis janvier 2019, les contenus sportifs font également l'objet de mesures de blocage DNS dans le cadre d'un accord dédié.

Cet accord intitulé « *Procédure technique pour les événements diffusés en direct* » a été signé par l'IGAC, les fournisseurs d'accès à internet et les ayants droit.

Il a permis la mise en place d'un dispositif qui permet le blocage temporaire de services proposant des liens vers des contenus sportifs diffusés de manière non autorisée par des plateformes tierces.

En complément de ce dispositif, chaque mois, le MAPINET demande le blocage administratif pérenne, dans le cadre du premier MoU, des sites bloqués de façon temporaire.

Le nombre de sites qui peuvent être bloqués temporairement est limité à 50 pour une période de 15 minutes. Les demandes de blocage ne peuvent intervenir qu'aux heures suivantes : du lundi au vendredi, de 17h30 à 22h45 et les samedis, dimanches et jours fériés, de 11h15 à 13h30 et de 15h30 à 22h. À l'usage, il s'est avéré que plus le temps passe, moins le nombre de noms de domaine bloqués dans le cadre de la procédure « *live* » est important.

Une plateforme dédiée a été créée afin de permettre le fonctionnement du dispositif prévu par la procédure technique. Le prestataire des ayants droit (ou ces derniers) rentre dans la plateforme l'URL de la page d'un site de liens *via* lequel est accessible la rencontre sportive et joint des captures d'écran de cette page attestant de la diffusion en direct.

Ces preuves sont revues par l'association de lutte contre le piratage puis par l'autorité publique, qui ordonne le blocage. Le blocage est ensuite mis en œuvre automatiquement sur les réseaux des fournisseurs d'accès à internet *via* la plateforme. La mesure de blocage, d'une durée de 2,5 heures, est mise en œuvre par les fournisseurs d'accès à internet dans un délai d'une quinzaine de minutes.

Les sites à bloquer sont détectés en amont grâce au fait que ceux-ci annoncent souvent les diffusions à venir, dans des délais variables, et commencent parfois à rediffuser le flux de la chaîne qui va diffuser le match avant que celui-ci ne débute. La plateforme intègre de plus une « liste noire » (sites ayant déjà fait l'objet de mesures de blocage) et une « liste blanche » (Facebook...) de sites à ne pas bloquer.

L'écosystème a toutefois déjà évolué au Portugal avec une croissance des offres IPTV illicites et un important contournement des mesures de blocage DNS par les internautes. Dans ce contexte, Nos Telecom, un des principaux opérateurs de télécommunications portugais et copropriétaire de la chaîne sportive Sport TV, a obtenu en justice à la suite de procédures initiées en mars et en octobre 2019, deux injonctions de blocage IP temporaire en temps réel. Les mesures de blocage, comme cela est précisé dans la première injonction, ne visent que les retransmissions des rencontres impliquant les quatre principales équipes de football portugaises diffusées par Sport TV. Seuls les fournisseurs d'accès à internet distribuant la chaîne ont dans un premier temps été attirés en justice. La seconde injonction a permis que l'extension pour la saison 2019/2020 soit prononcée.

ROYAUME-UNI

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

67,9 POPULATION^[1]
en millions

94,8 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

3,3 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

51 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illicites par mode d'accès en %



Le Royaume-Uni dispose de nombreux outils de lutte contre le piratage, souvent innovants, et est souvent présenté comme un modèle en matière de lutte contre le piratage, ce qui tient notamment au fait que les fournisseurs d'accès à internet, qui sont souvent également des ayants droit, travaillent de concert avec les ayants droit.

Le Royaume-Uni est très actif en matière de sensibilisation des internautes, diverses campagnes ayant été menées à ce titre, dont une campagne d'envoi de *mails* pédagogiques.

S'agissant de la lutte contre les services contrefaisants, le Royaume-Uni tâche d'actionner l'ensemble des leviers : mise en œuvre de l'approche dite « *Follow the money* », accords entre ayants droit et moteurs de recherche sous l'égide du gouvernement, injonctions dynamiques de blocage prononcées par le juge et, dernièrement, injonctions dites de *live blocking* venant notamment répondre à l'invasion massive de boîtiers configurés pour faciliter le piratage, et plus particulièrement le visionnage illégal sur internet de chaînes de télévision payantes et de retransmissions sportives.

LES ACTIONS VISANT LES INTERNAUTES

LE DISPOSITIF D'AVERTISSEMENT DES INTERNAUTES

Le gouvernement, via l'*Intellectual Property Office* (IPO), une agence de l'état rattachée au ministère des Affaires, de l'Énergie et des Stratégies industrielles, et chargée de l'enregistrement des droits de propriété industrielle et de la stratégie en matière de propriété intellectuelle, soutient l'initiative privée *Creative Content UK*, qui résulte d'un

accord volontaire entre les ayants droit et les fournisseurs d'accès internet pour une durée (initiale) de trois ans et qui a notamment mis en œuvre un mécanisme d'envoi de *mails* aux internautes dépourvu de sanction (*Voluntary Copyright Alert Programme*) de début 2017 à mi-2019.

Chaque fournisseur d'accès à internet déterminait lui-même le contenu détaillé des *mails*, une trame leur étant proposée par les ayants droit. Un avertissement pouvait

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

viser plusieurs faits et les *mails* contenaient des liens qui renvoyaient d'une part vers les saisines, mentionnant notamment les œuvres concernées, et d'autre part vers un site comportant, entre autres, des conseils sur les moyens de sécuriser son *Wi-Fi*.

Ce programme d'envoi de mails aurait eu des échos positifs, notamment par la presse, et reçu une large couverture médiatique. Le coût de ce dispositif et sa répartition entre les fournisseurs d'accès à internet et les ayants droit sont restés confidentiels.

Il a cependant été décidé de mettre fin au programme de notification, pour des raisons qui n'ont pas été rendues publiques, et l'envoi de *mails* a cessé mi-2019.

LE DISPOSITIF DE MISE EN DEMEURE INDEMNITAIRE

Les ayants droit peuvent saisir le juge^[4] pour obtenir l'identité d'un internaute qui a partagé illicitement des contenus culturels et dont l'adresse IP a été identifiée sur les réseaux pair à pair. Une fois les coordonnées de l'internaute obtenues, les ayants droit peuvent lui envoyer un courrier demandant le paiement de sommes d'argent. À défaut, il est indiqué que l'internaute pourra être poursuivi.

En pratique, ce dispositif est essentiellement utilisé par les ayants droit du secteur de la pornographie.

En 2012, une décision dite « *Golden Eye* », du nom d'une société de production d'œuvres pornographiques, a permis d'encadrer cette pratique et prévoit notamment que^[5] :

- la lettre de l'ayant doit faire apparaître que malgré l'injonction pour dévoiler l'identité d'un internaute celui-ci n'est pas encore regardé comme un contre-facteur ;
- le délai de réponse doit être raisonnable.

LE DURCISSEMENT DES PEINES ENCOURUES EN CAS DE CONTREFAÇON DE DROITS D'AUTEUR EN LIGNE

Le *Digital Economy Act 2017* entré en vigueur en octobre 2017 a modifié la peine maximale d'emprisonnement en cas de contrefaçon de contenus protégés par le droit d'auteur commise en ligne, et l'a soumise à la connaissance, avérée ou supposée, des pertes que subirait l'auteur. La peine est passée de deux à dix ans de prison, s'alignant ainsi sur ce qui était prévu pour la contrefaçon réalisée dans le monde physique. L'alignement des peines encourues en matière de contrefaçon était discuté depuis 2014^[6].

LES ACTIONS DE SENSIBILISATION

Dans le cadre de l'initiative *Creative Content UK*, des campagnes de sensibilisation sont mises en œuvre depuis novembre 2015.

Les actions menées ont pris différentes formes, notamment une campagne publicitaire appelée *Get It Right from a Genuine Site* qui s'est matérialisée, entre autres, par des publicités diffusées à la télévision et un site internet^[7], qui comporte une liste de sites dits « sincères » et des films d'animation sensibilisant à l'offre légale à destination du jeune public. En décembre 2016, un internaute sur quatre avait été touché par la campagne *Get It Right from a Genuine Site*. Parmi cette population, 17,5 % des gens ont indiqué que cela avait modifié leur perception du piratage. Toutefois, l'étude annuelle réalisée par Kantar Media pour l'IPO^[8] fait état d'un niveau stable d'internautes ayant consommé un contenu illégalement ces derniers mois (25 %).

En 2016, également à l'initiative de *Creative Content UK*, des ressources pédagogiques ont été mises à dispositions des enseignants, centrées autour de la question de savoir qui subviendrait aux besoins d'un acteur (à titre d'exemple) si tous les spectateurs d'un film recourraient au piratage.

[4] Selon un dispositif de common law intitulé *Norwich Pharmacal Order*.

[5] High court of justice, 26 mars 2012, *Golden Eye* : www.baillii.org/ew/cases/EWHC/Ch/2012/723.html

[6] Martin Brassell FRSA, Dr Ian Goodyer, Inngot Limited, « Penalty fair? Study of criminal sanctions for copyright infringement available under the CDPA 1988 », Intellectual Property Office, février 2015.

[7] www.getitrightfromagenuinesite.org

[8] <https://www.gov.uk/government/publications/online-copyright-infringement-tracker-survey-8th-wave>

En janvier 2018, une nouvelle campagne de sensibilisation de la jeunesse, financée par l'IPO et l'industrie de la musique, a été lancée. Elle consiste en une série de dessins animés, intitulée « *Nancy and the Meerkats* »^[9], tirée d'émissions de radio du même nom.

Le 28 mars 2018, le gouvernement britannique a annoncé la conclusion d'un « *Creative Industries Sector Deal* » avec le *Creative Industries Council*^[10], dont l'objet est d'investir dans les entreprises culturelles et créatives. Le rapport « *Industrial Strategy: Creative Industries Sector Deal* », qui présente les objectifs poursuivis, indique que le gouvernement financera la campagne « *Get it Right* » à hauteur de 2 millions de livres (environ 2 270 000 €) sur trois ans.

L'objectif de ces actions de sensibilisation est de changer les comportements à divers égards : orienter les consommateurs vers l'offre légale, et notamment l'offre payante ; changer la perception des atteintes au droit d'auteur sur internet, et notamment le fait qu'elles sont considérées comme acceptables et sans risque ; et enfin informer sur le fonctionnement de l'industrie créative.

La campagne « *Get It Right from a Genuine Site* » a ainsi joué sur la connexion émotionnelle entre les jeunes et les contenus qu'ils affectionnent et essaie de faire passer le message suivant : si vous aimez ce contenu, vous devriez récompenser ceux qui l'ont créé et les efforts qu'ils ont fournis en vous tournant vers l'offre légale. Les messages insistent sur le temps, l'investissement, et la force créative que les auteurs insufflent à leurs œuvres. La campagne a tâché de mettre en avant non pas tant les stars des œuvres mais les collaborateurs « de l'ombre » qui permettent également à ces œuvres d'exister. Les publicités diffusées ne sont pas culpabilisantes ou menaçantes, il s'agit plutôt de guider le consommateur vers un changement d'état d'esprit qui pourra l'amener à faire le choix de l'offre légale. Pour ce faire, la campagne utilise des vidéos diffusées sur de multiples canaux : spots publicitaires et vidéos sur YouTube et une publicité diffusée à la télévision, en particulier lors de matchs de football. L'objectif de cette campagne était de donner une image positive de la

consommation légale, de rendre les contenus issus de sources illicites moins désirables et de faire réfléchir la population sur son comportement. Enfin, elle a créé un climat favorable au lancement de la campagne d'envoi de *mails*, qui n'a d'ailleurs guère suscité de polémique.

Par ailleurs, en partenariat avec l'IPO et des acteurs de l'industrie, l'organisation à but non lucratif « *CrimeStoppers* » a lancé fin 2017 / début 2018 une campagne de sensibilisation sur l'utilisation des terminaux configurés pour accéder illégalement à des contenus, et notamment des programmes TV en direct^[11]. Cette campagne est constituée de quatre vidéos, disponibles sur YouTube, sensibilisant le public aux dangers de ces pratiques (risque d'être infecté par un *malware* ou de se faire voler son identité ; risques pour les jeunes publics), et l'encourageant à rapporter les vendeurs de boîtiers préconfigurés.

Au titre de sa stratégie pour lutter contre la contrefaçon en ligne, le gouvernement britannique envisage notamment de partager davantage les données de la lutte contre le piratage entre parties prenantes et autorités publiques, en s'assurant notamment de la publication des jugements, afin d'évaluer leur impact.

Le gouvernement britannique est en outre d'avis que pour développer des solutions au problème de la violation des droits de propriété intellectuelle, il faut comprendre ce qui motive les consommateurs à les enfreindre. Depuis 2014, l'IPO a ainsi financé des recherches régulières sur le comportement et les attitudes des consommateurs sur internet *via* la conduite d'une étude annuelle sur les indicateurs du piratage appelée *Online Copyright Infringement (OCI) Tracker*. Cette étude, dont la neuvième édition a été publiée en février 2020^[12], montre que le niveau global d'infraction est constant, environ 25 % des consommateurs utilisant une source illégale. L'enquête, réalisée en 2019, montre que là où des quantités substantielles de contenus sont disponibles légalement (*via* des services d'abonnement en *streaming*), la probabilité et le besoin perçu d'infraction sont notablement inférieurs.

[9] Les épisodes sont disponibles sur le site *Cracking ideas*, créé en novembre 2016 par l'IPO :

https://crackingideas.com/third_party/Nancy+and+the+Meerkats

[10] Le *Creative Industries Council* a pour vocation de représenter les industries créatives, et de favoriser leur croissance. Il est composé de membres issus de ces dernières : télévision, jeu vidéo, mode, musique, art, édition, et cinéma.

<https://www.gov.uk/government/groups/creative-industries-council>

[11] L'IPO a elle aussi mené une campagne de sensibilisation dont le but est de présenter une terminologie relative à cette nouvelle forme de contrefaçon ; il est notamment possible d'y trouver les termes « *illicit streaming device* », en référence à tous matériels informatiques permettant d'accéder illégalement à du contenu contrefaisant.

[12] <https://www.gov.uk/government/publications/online-copyright-infringement-tracker-survey-9th-wave>

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES SERVICES ILLICITES ET LEURS OPÉRATEURS

Une nouvelle forme de piratage connaît une expansion importante ces dernières années et est devenue l'une des priorités principales des parties prenantes de la lutte contre le piratage, et notamment de l'unité de la police de Londres dédiée à la lutte contre la contrefaçon : la vente et l'utilisation de boîtiers dotés d'applications permettant d'accéder à des contenus mis illicitement à disposition sur des sites et/ou à des programmes télévisés non accessibles sans abonnement.

Selon la police, la *Federation Against Copyright Theft* (FACT - la FACT est un organisme professionnel créé dans le but de protéger les droits de propriété intellectuelle de ses membres) et l'IPO, les boîtiers préconfigurés, notamment pour accéder gratuitement à des chaînes de télévision payantes, sont très populaires au Royaume-Uni. Le rapport de la FACT « *Cracking Down on Digital Piracy* »^[13] estime à un million le nombre de boîtiers préconfigurés vendus au Royaume-Uni les deux dernières années.

Des arrestations de vendeurs de ce type de boîtiers ont régulièrement lieu à travers des actions coordonnées de la FACT, de la police et de l'IPO. Ces arrestations puis condamnations, relayées dans la presse, ont pour but de lancer des messages forts aux personnes susceptibles de penser que ce type de boîtier est légal et d'endiguer ce phénomène. Les sanctions peuvent aller du paiement d'une amende de plusieurs dizaines de milliers d'euros à des peines de prison. Trois personnes ayant vendu des boîtiers permettant d'accéder aux matchs de football de la *Premier League* ont ainsi été condamnés à 17 ans de prison, en mars 2019. Ils auraient vendu plus de 1 000 abonnements, notamment à des pubs, clubs et foyers.

L'action des parties prenantes ne se limite d'ailleurs pas seulement aux revendeurs de ces boîtiers, mais aussi aux personnes retransmettant sans autorisation du contenu payant, ou à celles développant des applications illicites dédiées au piratage^[14].

LES MESURES JUDICIAIRES DE BLOCAGE

Au Royaume-Uni, depuis 2011, de nombreuses décisions de blocage de sites ont été prononcées par le juge à l'encontre des fournisseurs d'accès à internet. En matière de droit d'auteur, les décisions de blocage mettent jusqu'à présent à la charge des fournisseurs d'accès à internet les frais de mise en œuvre du blocage, les ayants droit prenant à leur charge les frais de procédure et la réunion des preuves de l'illicéité des sites.

Aux fins d'assurer l'effectivité de ces décisions, celles-ci prévoient que les fournisseurs d'accès et les ayants droit pourront ensuite s'accorder sur l'actualisation des sites visés par ces injonctions de blocage, sans repasser devant le juge.

Toutefois, une étude réalisée par l'*Open Rights Group* et publiée en juin 2018 montre :

- que certains des sites bloqués à la suite d'injonctions judiciaires ne devraient plus l'être, par exemple, parce qu'ils n'abritent plus de contenus illicites ;
- que la liste des sites bloqués diverge d'un fournisseur d'accès à internet à l'autre, nuisant à une bonne vision de l'écosystème. Les fournisseurs d'accès à internet n'actualiseraient pas leur liste de la même manière. Selon cet organisme, une solution pour améliorer la situation pourrait consister à demander aux tribunaux de tenir à ce que les fournisseurs d'accès à internet publient des listes actualisées de tous les sites bloqués^[15]. Aujourd'hui, aucune liste des sites bloqués n'est publiée, notamment parce que les parties prenantes constatent déjà une recrudescence des contournements des blocages par les internautes.

[13] <https://www.fact-uk.org.uk/files/2017/09/Cracking-Down-on-Digital-Piracy-Report-Sept-2017.pdf>

[14] Ainsi, la chaîne de télévision Sky a par exemple poursuivi certains de ses clients pour avoir transmis son contenu par streaming : un client a été condamné à payer 16 000 £ en frais de justice et des dommages-intérêts, tandis que deux autres, des propriétaires de pubs dénués de la licence commerciale nécessaire à la diffusion du contenu de la chaîne Sky à leur clientèle, ont été condamnés à 20 000 £ de dommages-intérêts. De la même manière, à la suite de menaces exercées par la FAPL, la société de droit anglais ACE TV, qui proposait des abonnements IPTV premium, a cessé son activité au mois d'avril 2018. La FAPL lui ayant réclamé un paiement transactionnel de 600 000 £, la société a été mise en procédure de liquidation judiciaire. Elle a par ailleurs transféré les données personnelles de ses clients à la FAPL.

[15] <https://torrentfreak.com/uk-pirate-site-blocks-opaque-poorly-administered-180603/>

LES MESURES ADMINISTRATIVES DE BLOCAGE

Le rapport gouvernemental « *Industrial Strategy : Creative Industries Sector Deal* » avait annoncé qu'une réflexion serait conduite courant 2019 sur l'effectivité du dispositif de blocage existant, et l'éventuelle introduction d'un dispositif de blocage administratif. L'IPO a ainsi évalué l'efficacité du système actuellement mis en œuvre pour bloquer les sites illicites. Les parties prenantes lui ont indiqué qu'elles estimaient le système existant efficace et ne considéraient pas qu'il y avait une réelle nécessité d'introduire un système de blocage administratif. De plus, l'IPO estime que le système a fait l'objet d'améliorations constantes et qu'il est adéquatement équipé pour faire face aux futurs défis du blocage des contenus contrefaisants.

LA LUTTE CONTRE LE PIRATAGE DE CONTENUS SPORTIFS

La *Football Association Premier League* (FAPL), qui est l'entité qui administre la *Premier League*, le principal championnat de football professionnel pour les clubs anglais, a obtenu dès 2013^[16] une injonction de blocage d'un site de *live streaming*.

En mars 2017^[17], elle a obtenu la première décision dite de *live blocking* requérant des principaux fournisseurs d'accès à internet britanniques qu'ils bloquent en direct les serveurs retransmettant illégalement des enregistrements de matchs de football.

L'injonction était limitée dans le temps à une période correspondant aux deux derniers mois de la saison 2016-2017 de la FAPL et s'étendant du 17 mars au 22 mai 2017. Les mesures de blocage ordonnées par le juge dans cette décision avaient vocation à constituer une phase de test, d'où leur durée limitée, devant permettre d'évaluer l'efficacité du dispositif et d'en cerner les risques.

Le juge a autorisé la mise en œuvre du dispositif demandé par la FAPL car il a estimé que les serveurs dont la FAPL demandait le blocage temporaire réalisaient une communication au public anglais non autorisée. Le fait que les serveurs s'adressent en particulier au public anglais a été démontré avec l'appui des fournisseurs d'accès internet, certains ayant réalisé des observations de leur réseau démontrant qu'un volume important du trafic vers les serveurs en cause était issu d'abonnés locaux. Ils ont également constaté que le trafic était significativement plus important au moment des matchs de la FAPL ou encore à l'occasion d'autres événements sportifs.

Une décision de juillet 2017, couvrant cette fois l'intégralité de la saison 2017-2018, a précisé le dispositif, posant qu'à chaque date à laquelle un match est prévu, les fournisseurs d'accès devront bloquer les serveurs qui auront communiqué illicitement des matchs en *live* au cours de cette période ou retransmis illicitement le flux d'une chaîne sur laquelle un match de la FAPL sera diffusé. À la fin de chaque période, la FAPL devra notifier aux fournisseurs d'accès à internet la fin du blocage afin que celui-ci prenne fin dans les meilleurs délais. Les injonctions ont ensuite été renouvelées pour les saisons à venir^[18].

Dans un communiqué du 25 juillet 2017, la FAPL a déclaré avoir bloqué plus de 5 000 adresses IP qui retransmettaient illégalement des contenus sportifs^[19]. Les premiers blocages ont également entraîné une grande confusion parmi les fournisseurs des services bloqués^[20], certains suggérant aux usagers d'utiliser des VPN.

En décembre 2017, l'Union des associations européennes de football (UEFA) a obtenu à son tour une injonction similaire couvrant la période du 13 février 2018 au 26 mai 2018^[21], laquelle a été étendue en juillet 2018^[22].

Ces injonctions ne sont dorénavant plus limitées au football car en septembre 2018, le juge a accordé à Matchroom la possibilité, pendant deux ans, de demander le blocage de services rediffusant illicitement

[16] *The Football Association Premier League Ltd v. British Sky Broadcasting Limited & Ors* [2013] EWHC 2058 (Ch), 16 juillet 2013 : [http://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2013/2058.html&query=\(premier\)+AND+\(league\)](http://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2013/2058.html&query=(premier)+AND+(league))

[17] *The Football Association Premier League Ltd v. British Telecommunications Plc & Ors* [2017] EWHC 480 (Ch), 13 mars 2017 : [http://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2017/480.html&query=\(football\)+AND+\(association\)+AND+\(premier\)+AND+\(league\)](http://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2017/480.html&query=(football)+AND+(association)+AND+(premier)+AND+(league))

[18] *The Football Association Premier League Ltd v. British Telecommunications Plc & Ors* [2018] EWHC 1828 (Ch), 18 juillet 2018 : <http://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2018/1828.html&query=football+association+premier+league>

[19] *English Premier League*, « Premier League awarded High Court Blocking Order », 25 juillet 2017.

[20] <https://torrentfreak.com/new-premier-league-blocking-disrupts-pirate-iptv-providers-170814/>

[21] *Union des Associations Européennes de Football v. v. British Telecommunications Plc & Ors* [2017] EWHC 3414 (Ch), 21 décembre 2017 : <http://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2017/3414.html&query=union+des+associations+europ+%E9ennes+de+football>

[22] *Union des Associations Européennes de Football v. v. British Telecommunications Plc & Ors* [2018] EWHC 1900 (Ch), 24 juillet 2018 : <http://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2018/1900.html&query=union+des+associations+europ+%E9ennes+de+football>

des matchs de boxe au Royaume-Uni^[23]. Les termes de cette injonction sont cependant différents compte tenu du fait que l'injonction a une durée de vie très longue et que les créneaux de diffusion des rencontres ne sont pas autant fixés à l'avance que pour une diffusion d'une saison de football. Dans ce contexte, le demandeur doit notifier au moins quatre semaines à l'avance aux fournisseurs d'accès à internet qu'un match sera diffusé sur tel créneau horaire. L'injonction en faveur de Matchroom a été renouvelée fin 2020 jusqu'en 2022^[24], permettant à Matchroom et à ses agents de bloquer les adresses IP des serveurs lorsqu'ils sont utilisés pour transmettre des images de Matchroom lors d'événements ou pendant une « période de pré-surveillance » précédant immédiatement ces événements.

Les fournisseurs d'accès à internet ne se sont pas opposés à ces procédures et les ont au contraire soutenues, sans doute parce que la plupart sont eux-mêmes des licenciés de la FAPL. La décision de juillet 2017 précise par ailleurs que les fournisseurs d'accès à internet ne peuvent qu'être tenus de faire leurs meilleurs efforts pour bloquer les services notifiés, selon la configuration de leur réseau et leurs ressources. Ceux-ci peuvent également réaliser des manipulations sur leur réseau qui vont les empêcher de mettre en œuvre les mesures de blocage mais ils doivent en avertir l'ayant droit dans les meilleurs délais et faire en sorte que ces manipulations aient une durée raisonnable.

LES DROITS DES ORGANISATIONS SPORTIVES EN CAUSE

La FAPL est active depuis longtemps dans la défense de ses droits face au piratage^[25]. Au fil du temps, elle fait évoluer les éléments devant lui permettre de revendiquer des droits de propriété intellectuelle sur les retransmissions des matchs qu'elle organise. Ainsi, la FAPL met en avant ses droits de propriété intellectuelle sur :

- les matchs captés par leurs licenciés^[26] (*Clean Live Feed*) dans la mesure où ils incluent un *replay* des actions les plus marquantes ;
- le flux destiné à l'international, dans la mesure où il s'agit du flux capté par le licencié national mais qu'il est enregistré avant d'être retransmis ;
- les graphiques et les logos qui sont incorporés dans le flux international.

L'UEFA quant à elle, dans des actions du même type au Royaume-Uni, revendique des droits d'auteur sur les retransmissions télévisuelles des matchs en se fondant sur les *replays* ainsi que les logos et musiques qui sont incorporés à la captation.

Une des difficultés pour le blocage de ce type de sites est par ailleurs que les droits sont détenus par une pluralité d'acteurs. C'est pourquoi, afin de donner plus de poids à leur action, la *Premier League* a notamment fait état dans cette procédure du soutien d'autres ayants droit^[27]. La procédure initiée par l'UEFA a de son côté été soutenue de la même façon par la FAPL ainsi que par *Formula One World Championship Ltd*.

LES MODALITÉS D'ACTUALISATION HEBDOMADAIRES DE L'INJONCTION CADRE DE LIVE BLOCKING

En vertu de l'injonction cadre ordonnée par le juge, la FAPL et son prestataire^[28] détectent chaque semaine les serveurs qui diffusent les contenus sportifs *via* différentes sources (réseaux sociaux, *playlists* illicites, applications de *live streaming*, boîtiers configurés...). Les adresses IP des serveurs sont ensuite transmises aux fournisseurs d'accès à internet pour que ceux-ci mettent en place les mesures de blocage IP.

[23] *Matchroom Boxing Limited v. British Telecommunications Plc & Ors* [2018] EWHC 2443 (Ch), 20 septembre 2018 : <https://www.bailii.org/ew/cases/EWHC/Ch/2018/2443.html>

[24] *Matchroom Boxing Limited v. British Telecommunications Plc & Ors* [2020] EWHC 2868 (Ch), 21 octobre 2020 : <https://www.bailii.org/ew/cases/EWHC/Ch/2020/2868.html>

[25] CJUE, C 403/08 et C 429/08, *Football Association Premier League Ltd, NetMed Hellas SA, Multichoice Hellas SA contre QC Leisure, et autres*, 4 octobre 2011.

La CJUE a été saisie de questions préjudicielles à la suite de procédures intentées par la FAPL : d'une part contre des acteurs ayant fourni des matériels et cartes de décodeurs permettant la réception au Royaume-Uni des matchs de Premier League diffusés par des radiodiffuseurs étrangers (en l'espèce, un radiodiffuseur grec) ; et d'autre part contre des café-restaurants ayant projeté des matchs de la Premier League à leurs clients via un dispositif de décodage permettant la réception des matchs diffusés par des radiodiffuseurs étrangers.

[26] Un diffuseur est chargé à chaque match de capturer le flux au niveau national.

[27] La procédure de mars 2017 ayant donné lieu à la première décision de *live blocking* a ainsi été soutenue par les acteurs suivants : i) *British Broadcasting Corporation and BBC Worldwide Ltd*; ii) *DFL Deutsche Fußball Liga GmbH*; iii) *Liga Nacional de Fútbol Profesional*; iv) *The Football Association Ltd*; v) *The Scottish Premier League Ltd*; vi) *The Football League Ltd*; vii) *England and Wales Cricket Board Ltd*; viii) *PGA European Tour*; ix) *The Professional Darts Corporation Ltd*; and x) *Rugby Football Union*.

Friend MTS : <https://www.friendmts.com/about-us/customers/>

[28] Friend MTS : <https://www.friendmts.com/about-us/customers/>

Les fournisseurs d'accès à internet bloquent les serveurs de la liste au moment du match, sachant que la liste des serveurs à bloquer peut en outre être actualisée en temps réel, de façon manuelle si nécessaire. Certains fournisseurs d'accès ont toutefois développé un système qui permet une automatisation du blocage. En pratique, la communication des serveurs à bloquer s'effectue via une plateforme sécurisée avec au moins deux actualisations par date de match.

Les décisions ne comportent aucune disposition sur le partage des coûts, qui demeure donc confidentiel.

Certaines garanties tendent à assurer la proportionnalité du dispositif tel que le fait que les hébergeurs des serveurs soient notifiés des blocages prévus, notamment afin de permettre aux tiers affectés par les mesures de blocage de saisir la cour^[29]. Dans les dix jours ouvrables à la suite de la mise en œuvre de la décision susvisée, les fournisseurs d'accès à internet doivent informer par voie électronique leurs abonnés que l'accès à un nombre de serveurs associés à la diffusion illicite de matchs a été bloqué par décision de justice et que des mesures similaires vont intervenir pour la saison à venir. Les internautes sont également informés de l'identité de la partie qui a obtenu la décision et du fait qu'ils peuvent saisir le juge.

L'IMPLICATION DES MOTEURS DE RECHERCHE ET L'EXTENSION À D'AUTRES INTERMÉDIAIRES

Après plus de deux années de discussion, un accord a été conclu le 9 février 2017, sous l'égide de l'IPO, avec les moteurs de recherche^[30] et les ayants droit^[31]. L'accord est un code de conduite, reposant sur la base de volontariat, juridiquement non contraignant.

Les engagements pris par les moteurs portent à ce stade sur le sous-référencement des offres illégales dans les résultats des moteurs de recherche dans leur version britannique (ex. : google.co.uk) et qui devra être mis en œuvre d'ici juin 2017. Les sites considérés comme illicites ne sont pas supprimés de l'index de recherche,

mais le positionnement de leurs pages dans les résultats de recherche est pénalisé.

La caractérisation des sites illicites relève des échanges d'informations entre les moteurs de recherche et les ayants droit.

Les parties prenantes se sont mises d'accord notamment sur des objectifs chiffrés (en pourcentage) à atteindre par les moteurs. Ces objectifs devraient concerner les recherches effectuées avec des mots-clés neutres par des consommateurs qui ne cherchent pas spécifiquement des offres illicites.

Le sur-référencement de l'offre légale ou la présentation de l'offre légale dans une rubrique dédiée sont exclus tant ils soulèvent des questions juridiques notamment liées au droit de la concurrence.

En contrepartie des engagements pris par les moteurs, les ayants droit^[32] vont faire en sorte que l'offre légale soit mieux référencée par les moteurs de recherche en optimisant leur stratégie de référencement d'une part (*Search Engine Optimization*), et en améliorant le référencement de l'offre légale pour une œuvre donnée d'autre part.

Les résultats obtenus à la suite de la signature de l'accord ont été estimés satisfaisants bien que certains ajustements doivent encore être réalisés pour rendre le dispositif plus efficace^[33]. L'IPO travaille ainsi avec les parties prenantes sur les moyens de résoudre le problème des nouveaux noms de domaine, le moyen d'intégrer un surpoids aux notifications concernant des œuvres diffusées en salles et l'articulation du *search* et d'*autocomplete*.

Le suivi du respect de ces accords est effectué trimestriellement par un prestataire. Le gouvernement a publié fin mars 2018 un rapport intitulé « *Industrial Strategy - Creative Industries Sector Deal*^[34] », qui prévoit d'étendre l'approche adoptée avec les moteurs de recherche en organisant plusieurs tables rondes avec les ayants droit afin d'engager des discussions avec les réseaux sociaux et les plateformes UGC, les acteurs de la publicité en ligne et enfin les places de marché.

[29] Les notifications doivent comporter : l'information que l'adresse a été bloquée à la suite d'une décision judiciaire d'un juge au Royaume-Uni, l'identité de la partie qui a obtenu l'injonction, un lien vers la décision de justice et une information sur le fait que les opérateurs affectés par cette décision de blocage peuvent saisir la cour.

[30] Google, Microsoft (Bing) et Yahoo pour les moteurs de recherche.

[31] La British Phonographic Industry (BPI) pour la musique et la Motion Picture Association (MPA) pour l'audiovisuel.

[32] En effet, iTunes et Netflix par exemple n'auraient pas toujours cette stratégie et n'apparaîtraient pas dans les résultats des moteurs. Ils préféreraient privilégier une recherche dans leurs applications, sans que l'internaute passe par les moteurs.

[33] Par exemple, un des problèmes tient aux différences par secteur s'agissant du nombre de notifications envoyées (le secteur musical est très actif par rapport au livre, notamment au regard du nombre d'œuvres dans un album) et obtient plus aisément un sous-référencement. Les changements de nom de domaine ou de sous-domaine sont également un problème car ils remettent les compteurs à zéro et le nouveau site met un moment à être déclassé.

[34] <https://www.gov.uk/government/publications/creative-industries-sector-deal>

Les sujets abordés sont les suivants : améliorer l'efficacité des notifications de contenus illicites aux plateformes (*Notice and Take down*) ; inciter les sites illicites à mettre un terme à leurs pratiques et réduire les coûts supportés par les ayants droit pour la protection de leurs droits.

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

En septembre 2013, la police de Londres a créé une unité dédiée aux infractions en matière de propriété intellectuelle : la *Police Intellectual Property Crime Unit* (PIPCU) qui lutte contre les atteintes aux droits de propriété intellectuelle (droits d'auteur mais également marques sur des biens matériels ou des biens numériques à l'exception des médicaments) et plus particulièrement les atteintes commises sur internet.

L'unité est subventionnée par l'IPO^[35] et les ayants droit apportent leur concours humain comme financier (et plus particulièrement la FACT – qui représente essentiellement les ayants droit de l'audiovisuel). La police peut être assistée dans la conduite de ses opérations par les enquêteurs spécialisés des ayants droit.

Des accords ont été conclus entre la PIPCU, les ayants droit^[36] et des acteurs de la publicité en ligne^[37], en vue de l'établissement d'un portail en ligne qui comprend une liste de sites massivement contrefaisants (*Infringing Website List*) et de la conduite d'actions à leur égard (*Operation Creative*). La MPA a rejoint cette opération.

Aux termes de cet accord, les ayants droit saisissent la police en lui transmettant les éléments établissant que ce site est massivement contrefaisant. L'élément principal utilisé par les ayants droit pour déterminer si un site est massivement contrefaisant ou non est une méthode statistique qui permet d'établir le pourcentage de contenus illicites qu'on peut y trouver. Il doit être supérieur à 50 % (*mainly infringing*). Les ayants droit informent également la PIPCU, quand ils en ont connaissance, qu'un site a fait l'objet d'une décision de blocage en Europe.

Dans un objectif de traitement efficace des dossiers des sites litigieux, un portail dédié a été créé, au sein duquel les ayants droit ou leurs représentants peuvent signaler un service et mettre à disposition les preuves de son activité illicite et notamment les informations sur le service de paiement utilisé, le cas échéant, et l'hébergeur. Si le site fait appel au prestataire Cloudflare (qui masque l'identité de l'hébergeur réel du site), le secteur privé devra tâcher en amont d'identifier l'hébergeur réel du site. Le portail est ainsi destiné à recueillir tout élément pouvant servir de preuve pour ouvrir une procédure pénale.

La PIPCU examine ensuite ces éléments, conduit ses propres investigations et décide ou non de mener une opération visant ce site. Les critères retenus par la police sont confidentiels. La police se rapproche du site et lui demande de régulariser ses activités sous 14 jours ou, à défaut, de les cesser. À défaut de réponse du site, celui-ci est alors inscrit sur l'*Infringing Website List*. Aucune intervention du juge n'est nécessaire.

La liste contient plus de 1 000 sites contrefaisants et est disponible sur une interface automatisée, accessible aux plus de 250 partenaires de l'opération. La liste comporte essentiellement des sites de liens (dont les revenus sont essentiellement issus de la publicité) et quelques sites hébergeant les contenus (*cyberlockers*). Cette liste pourrait à terme être utilisée dans le cadre de la base centralisée de l'OMPI destinée à mettre en œuvre l'approche dite « *Follow the money* » au niveau mondial.

Un prestataire de la PIPCU (*Pathmatics*) surveille les sites avec un logiciel dédié (*AdRoutes*) pour remonter la chaîne des acteurs de la publicité impliqués dans la diffusion de publicités sur chacun d'entre eux. Lorsque qu'il s'agit d'acteurs qui ne sont pas partenaires, elle leur indique qu'ils pourraient être considérés comme complices d'atteinte au droit de la propriété intellectuelle^[38].

[35] 2,56 millions de livres ont été versés à la police de Londres en 2013 lors de sa création puis 3 millions supplémentaires en 2014, devant permettre le fonctionnement de l'unité jusqu'à mi-2017. Un nouveau financement de 3,32 millions de livres doit permettre son fonctionnement jusqu'en 2019.

[36] La Federation Against Copyright Theft, la British Recorded Music Industry, l'International Federation of the Phonographic Industry (IFPI) et la Publishers Association.

[37] L'Internet Advertising Bureau local (IAB), l'Incorporated Society of British Advertisers et l'Institute of Practitioners in Advertising.

[38] En janvier 2017, la PIPCU a rendu visite à huit acteurs de la publicité en ligne (annonceurs, agences publicitaires, intermédiaires de la publicité). La PIPCU met en avant le succès de ce mécanisme, les publicités résiduelles concernant le secteur de la pornographie et/ou du jeu.

La PIPCU s'est rapprochée de l'autorité chargée d'accorder des licences aux acteurs du jeu/pari (la *Gambling commission*). Celle-ci a indiqué aux titulaires de licence qu'ils pourraient se voir retirer leur autorisation d'exercer s'ils diffusaient des publicités sur des sites illicites^[39]. Une baisse significative (87 % sur la période s'étendant de juin 2016 à juin 2017) de publicités des titulaires de licence est constatée par la police sur les sites illicites.

La PIPCU travaille également sur des aspects plus strictement financiers : elle collabore avec les ayants droit pour d'une part identifier les comptes bancaires des opérateurs de sites illicites qui sont destinataires des paiements des sommes issues des revenus de la publicité en ligne et, d'autre part, empêcher les *cyberlockers* de proposer illégalement des abonnements pour accéder à des contenus en *streaming* ou en téléchargement direct.

La PIPCU travaille également avec les intermédiaires techniques afin de complexifier les activités des services illicites. L'inscription d'un site sur la liste conduit ainsi à l'envoi d'un courrier au bureau d'enregistrement du nom de domaine ou à l'organisme en charge de la gestion de l'extension sous laquelle le nom de domaine a été enregistré pour demander la suspension du nom de domaine. Cette approche rencontre un succès mitigé auprès des acteurs situés hors du Royaume-Uni

(cas les plus fréquents). La PIPCU déplore à cet égard que le caractère international de la contrefaçon sur internet pose des problèmes de juridiction qui rendent plus complexes les actions contre les criminels au-delà des frontières du Royaume-Uni. Elle recherche cependant les intermédiaires en lien avec chaque service et identifie les actions possibles. Des coopérations ont ainsi été nouées avec certains acteurs locaux et à l'international. Le registre des extensions locales « .uk » et « .london » (Nominet) ne requiert ainsi aucune injonction judiciaire lorsque la police de Londres demande la saisie de noms de domaine. Les bureaux d'enregistrement locaux ont également été informés des risques encourus lorsqu'ils sont en affaire avec des services illicites. Dans la suite du Règlement général sur la protection des données (RGPD), qui impose de ne plus rendre publiques les informations sur l'identité des titulaires des noms de domaine, la PIPCU s'est également rapprochée des registres étrangers gérant des extensions locales et de plusieurs bureaux d'enregistrement. S'agissant des hébergeurs, la PIPCU ne demande pas le retrait de contenus donnés mais se positionne en aval de l'action des ayants droit pour solliciter la suspension de sites dans leur intégralité. La PIPCU a ainsi obtenu de Cloudflare, à la suite des difficultés rencontrées par les ayants droit à cet égard, que le service mette à disposition une adresse dédiée *via* laquelle elle peut lui notifier des sites en masse et obtenir les informations quant à leur hébergeur.

[39] *Gambling commission, Licence conditions and codes of practice, janvier 2018 : article 16.1.1 – Licence condition : responsible placement of digital adverts (all licences): » 1) Licensees must: a) ensure that they do not place digital advertisements on websites providing unauthorized access to copyrighted content ».*

RUSSIE

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

145,9 POPULATION^[1]
en millions

82,6 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

8,3 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

69 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illégitimes par mode d'accès en %



La Russie s'implique fortement dans la lutte contre le piratage, et dispose d'une autorité publique, le *Roskomnadzor* (service fédéral de supervision des communications, des technologies de l'information et des médias de masse), qui joue un rôle central dans la lutte contre le piratage. La politique

publique de lutte contre la contrefaçon de droits d'auteur sur internet en Russie repose essentiellement sur un dispositif de retrait des contenus portant atteinte au droit d'auteur pouvant conduire à leur blocage. Ce dispositif est régulièrement modifié afin de le rendre toujours plus efficace.

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES SERVICES ILLICITES ET LEURS OPÉRATEURS

En octobre 2019, la BREIN, en collaboration avec la MPA et l'ACE, a obtenu en justice que cinq intermédiaires techniques domiciliés ou ayant des serveurs aux Pays-Bas déconnectent les serveurs utilisés par le service *Moonwalk*, ce qui a conduit à sa fermeture. *Moonwalk* était un *Content Delivery Network* (CDN) qui mettait à disposition une infrastructure technique de stockage et de diffusion de contenus audiovisuels ainsi que des services annexes. Cette infrastructure servait de base à de nombreux sites tiers par l'intermédiaire desquels les utilisateurs pouvaient accéder aux œuvres

piratées. *Moonwalk* fournissait ainsi les ressources et les contenus illégitimes à environ 80 % des sites russes connus de *streaming* illégitime^[4].

LES MESURES ADMINISTRATIVES DE BLOCAGE

Le dispositif mis en place en Russie prévoit que les ayants droit, en cas d'échec des discussions avec les sites suite à une demande de notification et retrait, disposent d'une procédure accélérée afin que soient ordonnées des mesures de blocage.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] <https://stichtingbrein.nl/brein-serves-ex-parte-order-on-dutch-hosting-providers-for-80-of-russian-streaming-sites/>

La procédure est la suivante : l'ayant droit saisit la cour de Moscou, seul tribunal compétent en Russie en la matière qui, après constatation de la violation, notifie sa décision au *Roskomnadzor*, lequel est en charge de l'exécution de la décision.

Avant d'exécuter la décision, le *Roskomnadzor* contacte le site, lequel dispose alors d'un délai de trois jours pour mettre fin à la violation constatée. Passé ce délai, en l'absence de retrait du contenu litigieux ou de cessation de l'activité illicite, le *Roskomnadzor* peut demander aux intermédiaires techniques et notamment aux fournisseurs d'accès à internet, de mettre en œuvre la mesure destinée à empêcher l'accès au contenu ou au site litigieux.

À défaut d'obtempérer, les intermédiaires encourent une amende d'un montant de 30 000 roubles (environ 500 euros). Afin d'exécuter rapidement les mesures de blocage, une « interconnexion » permettant la circulation sécurisée et facilitée des informations a été mise en place entre le régulateur et les fournisseurs d'accès à internet. L'autorité publique est chargée de maintenir à jour la liste des ressources illicites dans ce système d'information (*Federal state information system* - FGIS) et les intermédiaires techniques supportent les coûts du blocage.

Les mesures de blocage à l'encontre des sites massivement contrefaisants ou encore qui promeuvent de façon répétée des services contrefaisants peuvent être prononcées pour une durée indéterminée.

En 2019, des sites illicites de *stream ripping* ont été bloqués pour la première fois en Russie (Flvto.biz, conv.com et Flv2mp3.by). L'hébergeur de fichiers ou *cyberlocker Rapidgator* a également été bloqué en avril 2019 après de nombreuses tentatives d'appel infructueuses.

Il faut relever qu'en juin 2020, la Cour européenne des droits de l'homme a rendu une décision concernant plusieurs mesures de blocage mises en œuvre en Russie^[5]. Cette décision condamne la Russie sur le fondement de l'article 10 de la Convention européenne des droits de l'homme qui garantit la liberté d'expression et l'article 13 sur le droit à un recours effectif. La décision concerne différentes affaires en Russie – aucune n'ayant cependant trait au piratage. Elle a pointé qu'il était impératif d'assurer la nécessité et la proportionnalité des mesures de blocage mises en œuvre, en particulier lorsqu'un blocage IP pérenne est mis en place, lequel doit donc impliquer en amont

des vérifications afin de ne pas bloquer les autres sites hébergés sur la même adresse IP que celle du site à bloquer. Le manque de transparence des mesures de blocage mises en œuvre et l'absence d'information des opérateurs des services affectés sont également mis en avant pour démontrer les manquements de la Russie dans ces affaires.

L'ACTUALISATION DES MESURES ADMINISTRATIVES DE BLOCAGE

Une loi, adoptée le 1^{er} juillet 2017, a introduit une procédure administrative accélérée qui ne nécessite pas de repasser devant la cour de Moscou pour obtenir le blocage des sites de contournement.

Les ayants droit saisissent le ministère des Télécommunications et de la Communication qui rend sous 24 heures, en s'appuyant sur un collège de trois experts au minimum, une décision reconnaissant le caractère « miroir » du site. La décision est transmise au responsable du site ainsi qu'au *Roskomnadzor*.

Le *Roskomnadzor* notifie à son tour la décision du ministère à l'hébergeur et enjoint sous 24 heures aux fournisseurs d'accès à internet de bloquer le service et, le cas échéant, aux moteurs de recherche de déréférencer le nom de domaine du site en cause.

LE DISPOSITIF DE LUTTE CONTRE LES APPLICATIONS PERMETTANT LA COMMUNICATION AU PUBLIC DE CONTENUS CONTREFAISANTS

En octobre 2020, est entrée en vigueur une législation qui permet aux ayants droit d'obtenir que des mesures soient prises à l'encontre des applications facilitant l'accès aux contenus illicites^[6]. Après avoir reçu une plainte d'un ayant droit, le *Roskomnadzor* dispose de 72 heures pour déterminer où l'application est disponible (sur un magasin d'application officiel tel que Google Play ou l'App Store d'Apple et/ou sur un site tiers). Le *Roskomnadzor* envoie alors un avis d'infraction à la plateforme l'informant de la violation.

Celle-ci a alors 24 heures après la réception de la plainte pour en informer le propriétaire de l'application, lequel disposera à son tour de 24 heures pour empêcher la mise à disposition des contenus visés.

[5] https://www.echr.coe.int/Documents/FS_Access_Internet_ENG.pdf

[6] <http://translate.google.com/translate?hl=fr&sl=auto&tl=fr&u=http%3A%2F%2Fpublication.pravo.gov.ru%2FDocument%2FText%2F0001202006080030>

À défaut, la responsabilité d'empêcher les infractions en cours retombe alors sur les plateformes de distribution d'applications elles-mêmes, les obligeant à cesser de distribuer l'application. Si celles-ci ne s'exécutent pas, le *Roskomnadzor* peut alors enjoindre aux fournisseurs d'accès à internet locaux de bloquer les plateformes de distribution. En toutes hypothèses, les injonctions du régulateur doivent être validées par la cour de Moscou.

Une première ordonnance a ainsi été rendue sur le fondement de cette loi en décembre 2020, enjoignant à Google de bloquer l'accès à une application.

L'IMPLICATION DES SERVICES D'ANONYMISATION

Une loi adoptée le 29 juillet 2017 intègre les services d'anonymisation dans le dispositif de lutte contre le piratage, ceux-ci pouvant désormais faire l'objet de mesures de blocage et de déréférencement s'ils ne respectent pas les nouvelles obligations qui leur incombent. Le nouveau texte prévoit ainsi que les opérateurs de services de VPN ou autres systèmes d'anonymisation doivent faire connaître leur identité auprès des autorités, donner les clés de chiffrement pour permettre le déchiffrement des messages cryptés. Ils doivent également se connecter au dispositif technique du *Roskomnadzor* qui liste les sites bloqués afin d'empêcher à leur tour l'accès à ces sites. Face au refus de plusieurs services de VPN de bloquer les sites listés, le *Roskomnadzor* a annoncé en mars 2019 que ces derniers feraient prochainement l'objet de mesures de blocage en Russie.

L'application de messagerie cryptée Telegram a ainsi fait l'objet d'une mesure de blocage. Le service utilisant cependant les infrastructures d'Amazon et de Google, des millions d'adresses IP des deux sociétés ont été bloquées également, conduisant à un important sur-blocage.

L'IMPLICATION DES MOTEURS DE RECHERCHE

En novembre 2018, les ayants droit, des plateformes et des moteurs de recherche locaux tels que Yandex, Mail.ru et Rambler ont signé un accord de coopération les obligeant à prendre des mesures à l'égard des URL figurant sur une base de données centralisée, créée par le *Roskomnadzor*. Toutes les cinq minutes, les opérateurs des plateformes de recherche doivent interroger la base de données pour obtenir des mises à jour. Ils sont alors tenus de supprimer les URL obtenues de leurs résultats en Russie dans un délai de 6 heures. En cas de conflit entre les signataires, l'accord prévoit une procédure de médiation, avec l'aide du *Roskomnadzor*. Cet accord de coopération, qui devait initialement être en vigueur jusqu'au 1^{er} septembre 2019 puis formalisé par un texte de loi, a finalement été renouvelé jusqu'en août 2021.

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

La loi russe prévoit enfin que les services en ligne qui proposent des publicités doivent également se connecter à la liste des sites illicites afin de cesser de promouvoir des services bloqués ou de fournir des liens vers ces services.

La Russie a rejoint en septembre 2020 le projet de l'OMPI dit « *WIPO ALERT SYSTEM* » qui vise à donner une portée internationale aux dispositifs locaux de démonétisation. Après quatre mois d'adhésion, la Russie a saisi 1 768 adresses de domaine de sites ayant fait l'objet de mesures locales de blocage dans cette base de données.

SINGAPOUR

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

5,9 POPULATION^[1]
en millions

89 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

0,8 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

150 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illégitimes par mode d'accès en %



Depuis 2014, le dispositif de lutte contre le piratage à Singapour se concentre principalement sur la possibilité pour le juge d'ordonner des mesures de blocage aux fournisseurs d'accès à internet.

La disposition légale permettant que de telles mesures soient ordonnées est aujourd'hui également utilisée pour lutter contre de nouvelles formes de piratage telles que l'IPTV illégale.

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

En juillet 2014, un amendement^[4] à la loi sur le droit d'auteur a introduit la possibilité pour les juges d'ordonner aux fournisseurs d'accès à internet de bloquer des services dont l'objet principal est de porter manifestement atteinte au droit d'auteur. L'ayant droit doit au préalable avoir envoyé une notification à l'administrateur du site visé ou avoir effectué des efforts raisonnables pour le contacter. C'est donc seulement en l'absence de réponse de l'opérateur du site visé que l'ayant droit peut agir aux fins de voir ordonnées des mesures de blocage.

La loi prévoit un faisceau de critères pour déterminer si un site porte effectivement atteinte aux droits d'auteur et doit en conséquence être bloqué :

- si l'objectif principal du site est de commettre ou de faciliter la violation du droit d'auteur ;

- si le site met à disposition des contenus ou des répertoires, des index ou des catégories de liens vers des contenus pour faciliter la violation des droits d'auteur ;
- si l'opérateur du site démontre un mépris général du droit d'auteur ;
- si le site a déjà fait l'objet de mesures de blocage dans un autre pays pour cause de violation du droit d'auteur ou en lien avec une telle violation ;
- si le site contient des guides ou des instructions pour contourner des mesures, ou des décisions de justice visant à empêcher l'accès à des sites illégaux ;
- l'audience du site.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] <https://sso.agc.gov.sg/Acts-Supp/22-2014/Published/20141202?DocDate=20141202>

Les premières décisions de blocage de sites sur ce fondement ont été prononcées en 2016. Fin 2018, la haute cour de Singapour^[5] a ordonné pour la première fois le blocage dynamique de 153 noms de domaine considérés comme manifestement illicites. Les fournisseurs d'accès à internet devront ainsi sur simple notification des ayants droit visant à démontrer que le nom de domaine initial a par exemple été redirigé, bloquer les sites dits miroirs des sites visés dans le jugement.

L'APPLICATION DES MESURES DE BLOCAGE POUR LUTTER CONTRE LES ABONNEMENTS À DES BOUQUETS DE CHÂÎNES TÉLÉVISÉES

Singapour est confrontée à un important piratage par le biais de boîtiers configurés. Les ayants droit n'hésitent pas à utiliser la procédure judiciaire de blocage pour lutter contre cette forme de piratage qui permet aux consommateurs d'accéder à des contenus audiovisuels et sportifs, le texte de loi permettant le prononcé de mesures de blocage étant assez large en visant « *les espaces en ligne manifestement illicites* ».

Suite à une procédure intentée par Singtel, opérateur de télécommunications et fournisseur de services de télévision payants, diverses entités du groupe Fox, qui distribue plusieurs chaînes payantes, et la *Football Association Premier League* anglaise, en 2018, la haute cour de Singapour a prononcé une injonction dynamique de blocage ordonnant aux fournisseurs d'accès à internet de bloquer les noms de domaine de serveurs qui sont utilisés par les services diffusant les bouquets de chaînes illégalement (ces serveurs d'authentification permettent aux services illicites de vérifier que l'utilisateur qui veut accéder à l'offre est bien le titulaire d'un abonnement valide).

Un rapport de janvier 2019 du ministère de la Justice indique que le gouvernement souhaite introduire une loi qui permettrait de sanctionner pénalement et civilement ceux qui fabriquent, importent pour vendre, distribuer commercialement ou vendre du matériel qui peut être utilisé pour accéder à du contenu audiovisuel provenant d'une source illégale.

[5] *The High Court of the Republic of Singapore, Disney Enterprise Inc, v M1 LTD, 19 septembre 2018, https://www.supremecourt.gov.sg/docs/default-source/module-document/judgement/os95_18-disney-enterprises-inc-v-m1-limited-pdf.pdf*

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

10,1 POPULATION^[1]
en millions

94,5 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

0,75 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

79 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



Si la Suède est le berceau, tant d'un des acteurs majeurs de l'offre légale de musique en ligne (Spotify) que de l'un des principaux sites de liens *Torrent*, « *The Pirate Bay* », lequel fait l'objet de décisions de blocage dans de nombreux pays, le dispositif

de lutte contre le piratage de contenus culturels en ligne se concentre principalement sur les actions impliquant les intermédiaires à l'égard des sites, bien que des dispositifs dédiés sont mis en place à l'égard des internautes.

LES ACTIONS VISANT LES INTERNAUTES

LE DISPOSITIF DE MISE EN DEMEURE INDEMNITAIRE

Les ayants droit peuvent saisir le juge pour obtenir l'identité d'un internaute qui a partagé illicitement des contenus culturels sur les réseaux pair à pair et dont l'adresse IP a été identifiée. Une fois les coordonnées de l'internaute obtenues auprès du fournisseur d'accès à internet en vertu de la décision de justice, les ayants droit peuvent lui envoyer un courrier de mise en demeure de leur payer des dommages et intérêts. À défaut de régler cette somme, il est indiqué à l'internaute qu'il pourra être poursuivi en justice.

Cette pratique fait toutefois l'objet de controverses, notamment après la décision de la CJUE du 21 décembre 2016 en matière de conservation et de communication des données personnelles par les fournisseurs d'accès à internet^[4]. La cour administrative de Stockholm a cependant jugé en février 2018 que les fournisseurs d'accès à internet étaient tenus de dévoiler l'identité des internautes aux ayants droit. Le fournisseur d'accès à internet, Bahnhof, qui refusait de dévoiler l'identité de ses abonnés dans les affaires pénales autres que criminelles – et qui est depuis 2016 sous le coup d'une injonction du régulateur de télécommunications – a fait appel de cette décision.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] CJUE, 21 décembre 2016, C 203/15 et C-698/15, *Tele2 Sverige AB (C 203/15) et Secretary of State for the Home Department*.

En 2020, des cabinets d'avocats agissant au nom des ayants droit ont obtenu en justice l'autorisation d'obliger plusieurs fournisseurs d'accès à internet suédois à transmettre les données personnelles des clients derrière des milliers d'adresses IP. Or, le principal cabinet menant ces actions est actuellement confronté à de graves accusations de fraude au Danemark. Le fournisseur d'accès Bahnhof a quant à lui réitéré sa volonté de ne pas dévoiler l'identité de ses abonnés, qualifiant ces demandes « d'extorsion ».

LA PROMOTION DE L'OFFRE LÉGALE

Le bureau d'enregistrement des marques et brevets propose un portail de l'offre légale, [Streamalagligt.se](https://www.streamalagligt.se)^[5], qui permet aux internautes de trouver des films, séries, musiques. Les ayants droit ont mis en place le portail de l'offre légale Moviezine, qui permet également aux internautes de trouver des films et séries de manière légale.

Sous l'impulsion du gouvernement^[6], une campagne de communication a été organisée en mai 2018 pour encourager les internautes à visionner du *streaming* légalement.

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

L'utilisation de boîtiers dotés d'applications permettant d'accéder à des contenus mis illicitement à disposition sur des sites et/ou à des programmes télévisés non accessibles sans abonnement^[7] connaît une expansion importante ces dernières années en Suède et est devenue l'une des priorités principales des parties prenantes de la lutte contre le piratage avec un des taux d'usage les plus élevés en Europe : entre 8 % à 9 % de la population.

Afin de déterminer la gravité de l'atteinte, il faudrait désormais tenir compte de plusieurs facteurs tels que la préméditation, le caractère « organisé » de l'infraction ou encore sa nature particulièrement dangereuse.

Il est prévu que cette proposition de loi entre en vigueur en septembre 2020.

LES ACTIONS CONTRE LES SERVICES ILLICITES ET LEURS OPÉRATEURS

La politique en matière de lutte contre la contrefaçon commerciale comporte un fort volet pénal mis en œuvre par la police, qui dispose d'un service dédié. La Suède dispose de procureurs et de juridictions spécialisées. Des peines de prison de plusieurs mois sont prononcées à l'égard de créateurs de sites implantés en Suède^[8].

En novembre 2016, le *tracker Rarat.org* a été fermé et son créateur arrêté à la suite d'une action ayant impliqué la collaboration de la police, de *Rights Alliance* et de PayPal, qui a permis d'identifier le bénéficiaire des paiements reçus par le site.

Le gouvernement a introduit un projet de loi^[9] qui prévoit de faire passer de deux à six ans de prison les condamnations pour contrefaçon aggravée de la propriété intellectuelle, avec une peine minimale de six mois.

Des ayants droit représentant des chaînes de télévision ont assigné des fournisseurs de flux en *streaming* qui proposaient sans autorisation leurs chaînes, notamment de sport. Les opérateurs ont été condamnés par la cour des brevets et du marché de Stockholm le 29 juin 2018^[10] pour contrefaçon et utilisation frauduleuse des flux à de la prison et des dommages et intérêts à hauteur d'environ 21 millions d'euros.

[5] <https://www.streamalagligt.se/na/en>

[6] <https://www.prv.se/en/copyright/streama-lagligt/>

[7] *Illegal IPTV In the European union*, EUIPO, novembre 2019, https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Illegal_IPTV_in_the_European_Union/2019_Illegal_IPTV_in_the_European_Union_Full_en.pdf

[8] http://www.hogstodomstolen.se/Domstolar/hogstodomstolen/Avgoranden/2017/2017-06-12_%20B_%203878-15_%20dom.pdf

[9] <https://www.regeringen.se/4931b8/contentassets/048b5202b6f24645889ad1fad230a6e7/skarpta-straff-for-de-allvarligaste-fallen-av-immaterialrattsintrang.pdf>

[10] <https://torrentfreak.com/images/StockholmsBein.pdf>

LES MESURES JUDICIAIRES DE BLOCAGE

En février 2017^[11], une injonction de blocage a été prononcée pour la première fois à l'encontre d'un fournisseur d'accès à internet afin d'empêcher l'accès au site « *The Pirate Bay* » pour une durée de trois ans, dans le cadre d'une procédure intentée par les ayants droit de la musique et de l'audiovisuel. Le fournisseur d'accès à internet risque une amende d'environ 53 000 euros s'il n'exécute pas le jugement. Les fournisseurs d'accès à internet non partie à l'instance ont indiqué qu'ils ne bloqueraient pas volontairement le site sans décision les concernant directement.

En décembre 2019, dans le cadre d'une procédure introduite par les ayants droit de l'audiovisuel, la cour des brevets et du marché de Stockholm a émis à l'encontre du fournisseur d'accès internet Telia, pour la première fois, une injonction dynamique de blocage à l'encontre de quatre sites dont « *The Pirate Bay* », d'une durée de trois ans^[12]. Les ayants droit pourront désormais demander l'actualisation des mesures de blocage des noms de domaine et adresses IP permettant d'accéder à « *The Pirate Bay* » sans passer devant le juge. Si Telia n'exécute pas la décision, le fournisseur d'accès à internet risque une amende d'environ 47 000 euros^[13]. L'injonction ne précise pas selon quel formalisme les ayants droit doivent informer le fournisseur d'accès quant aux nouveaux noms de domaine ou adresse IP à bloquer. L'appel de Telia a été rejeté en juillet 2020^[14]. La cour a précisé dans cette décision que Telia n'est pas tenu de rechercher activement les nouveaux domaines sous lesquels ces sites sont rendus accessibles. Cette tâche incombera aux titulaires de droits, après quoi le fournisseur d'accès dispose de deux à trois semaines pour mettre à jour sa liste de blocage.

L'IMPLICATION DU REGISTRE LOCAL

Le 22 décembre 2017, la Cour suprême a considéré que les noms de domaine constituaient des biens qui pouvaient être saisis par l'État. Le procureur de la République avait assigné « Punkt SE », l'organisation suédoise en charge de la gestion du « .se », car il considérait que les noms de domaine « *ThePirateBay.se* » et « *PirateBay.se* » sont des outils qui facilitent et encouragent le piratage et peuvent ainsi être saisis par l'État suédois. En effet, la section 53-a de la loi sur le droit d'auteur^[15] prévoit que les biens utilisés ou qui vont être utilisés pour commettre des infractions peuvent être saisis pour prévenir d'autres infractions.

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

Une initiative de type « *Follow the money* » est mise en œuvre dans le cadre d'une collaboration entre le groupe anti-piratage *Rights Alliance* et des acteurs de la publicité en ligne. Dans ce cadre, une liste de sites contrefaisants est établie par les ayants droit et communiquée à leurs partenaires du secteur publicitaire, lesquels font en sorte de ne pas diffuser de publicités sur ces sites. La liste a été actualisée en février 2019.

[11] En première instance, le juge n'avait pas fait droit à la demande de blocage.

[12] Cour des brevets et du marché, 9 décembre 2019 : <https://torrentfreak.com/images/Stockholms-TR-PMT-7262-18-Dom-2019-12-09-1.pdf>

[13] <https://ipkitten.blogspot.com/2020/01/the-swedish-patent-and-market-court.html>

[14] Cour des brevets et du marché, 3 juillet 2020 : <https://torrentfreak.com/images/Svea-HR-PMT-13399-19-Dom-2020-06-29.pdf>

[15] Loi sur la propriété littéraire et artistique, SFS 1960 : 729 modifié le 1^{er} avril 2011, https://www.wipo.int/wipolex/en/text.jsp?file_id=290912

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

8,7 POPULATION^[1]
en millions93,2 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]USAGES ILLICITES^[3]0,56 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards69 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illicites par mode d'accès en %



Une réforme dite du « droit d'auteur modernisé » est entrée en vigueur le 1^{er} avril 2020^[4]. La nouvelle réglementation suisse prévoit des actions tant

à l'égard des internautes qu'à l'égard des sites et des plateformes.

LES ACTIONS VISANT LES INTERNAUTES

LE DISPOSITIF DE MISE EN DEMEURE INDEMNITAIRE

Avec la révision de la loi, une nouvelle disposition concernant la collecte des données personnelles a été introduite afin de faciliter la mise en œuvre du droit d'auteur dans les cas de mise à disposition non autorisées (le téléchargement à partir de sources illicites reste couvert par l'exception de l'utilisation privée). Pour les cas de mises à disposition non autorisées, la nouvelle réglementation prévoit que le titulaire de droit d'auteur qui subit une violation peut initier une procédure et, dans cette perspective, il est autorisé à « *traiter des données personnelles [...] pour déposer une plainte ou une dénonciation) pénale [...]. Il peut également utiliser ces données pour faire valoir des conclusions civiles par voie d'adhésion ou pour les faire valoir au terme de la*

procédure pénale. Il est tenu de déclarer publiquement le but, le type de données traitées et l'étendue de leur traitement ».

Le droit d'auteur modernisé prend ainsi le contrepied d'une jurisprudence suisse de 2010, dite « Logistep », très protectrice en matière de données personnelles, et qui avait créé une incertitude quant à la licéité de la collecte d'adresses IP par les ayants droit en vue d'initier des poursuites pour les cas de mises à disposition illicites, et par conséquent une incertitude quant à l'admissibilité des adresses IP en tant que preuve dans le cadre de poursuites pour violation de droits d'auteur. L'inscription d'une base légale dans la loi révisée sur le droit d'auteur autorisant le traitement de données dissipe désormais ces incertitudes.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] <https://www.parlament.ch/centers/eparl/curia/2017/20170069/Texte%20pour%20le%20vote%20final%201%20NS%20F.pdf>

LES ACTIONS DE SENSIBILISATION

L'Office fédéral de la communication (OFCOM), un organe exécutif qui relève du Conseil fédéral, réalise régulièrement des campagnes de communication pour sensibiliser aux dangers d'internet et a sorti en mai 2020 une bande dessinée numérique^[5].

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES MESURES JUDICIAIRES DE BLOCAGE

Le 27 février 2019^[6], le tribunal fédéral de Lausanne a rejeté une requête aux fins de voir ordonné à l'un des principaux fournisseurs d'accès à internet suisse de procéder au blocage de sites illicites. Le juge rappelle que les administrateurs des sites en cause enfreignent la loi, mais considère que le fournisseur d'accès à internet n'est en aucune manière impliqué dans les infractions au droit d'auteur. Dès lors, il ne saurait être enjoint à prendre des mesures de blocage. La nouvelle loi précitée ne comporte pas de disposition permettant de combattre cette jurisprudence car elle n'a finalement pas introduit cette possibilité en droit suisse, contrairement à ce qui a pu un temps être envisagé.

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

Le partenariat public-privé, « Stop à la piraterie », réfléchit aux modalités de mise en œuvre de l'approche dite « *Follow the money* » visant à impliquer les acteurs de la publicité en ligne dans la lutte contre le piratage.

LES ACTIONS CONTRE LES SITES ILLICITES ET LEURS OPÉRATEURS

En novembre 2020, un service d'IPTV basé en Suisse a été fermé par la police locale avec l'aide d'Europol, après une plainte déposée par une entreprise télévisuelle et une société de lutte contre le piratage. Cette action semble être la première du genre en Suisse.

LES ACTIONS VISANT À RESPONSABILISER LES PLATEFORMES DE PARTAGE DE CONTENUS

La Suisse ne disposait auparavant pas de régime légal spécifique pour les intermédiaires techniques. La nouvelle législation a introduit désormais des dispositions visant à encadrer les activités des hébergeurs en imposant une obligation spécifique aux plateformes qui « *en raison de [leur] fonctionnement technique ou de [leurs] objectifs économiques favorisent les violations du droit,*

génère[nt] un risque particulier qu'une telle violation soit commise ». Ceux-ci doivent désormais prévenir les nouvelles mises en ligne de contenus protégés qui leur ont préalablement été notifiées (*Stay down*) en prenant « *les mesures qui peuvent être raisonnablement exigées d'[eux] d'un point de vue technique et économique compte tenu du risque de violation* ».

[5] <https://www.websters.swiss/fr/>

[6] <https://torrentfreak.com/images/Swisscom-ruling-27-2-19.pdf>

TAÏWAN

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

23,6 POPULATION^[1]
en millions

88,8 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

2 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

97 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



Il existe en droit taïwanais un dispositif de type graduel prévu par la loi mais celui-ci n'est pas mis en œuvre. Par ailleurs, peu d'outils dédiés

semblent prévus pour lutter contre les services contrefaisants.

LES ACTIONS VISANT LES INTERNAUTES

LE DISPOSITIF D'AVERTISSEMENT DES INTERNAUTES

Taïwan a introduit un mécanisme législatif d'avertissement graduel en 2009 qui prévoit que les intermédiaires techniques (fournisseurs d'accès à internet et plateformes) doivent :

- transmettre des notifications aux internautes ;
- se doter d'un dispositif permettant de suspendre ou résilier les abonnements ou comptes des internautes qui ont porté plusieurs fois atteinte au droit d'auteur.

À défaut, ceux-ci ne pourraient pas bénéficier du régime de responsabilité limitée.

Toutefois, la mise en œuvre pratique du dispositif n'est détaillée par aucun texte.

Des ayants droit du domaine de la musique et un fournisseur d'accès à internet, HiNet, auraient décidé de tester pendant six mois ce dispositif en 2013. Toutefois, il serait ressorti de cette expérience que moins de 30 % des notifications adressées par les ayants droit auraient pu être délivrées avec succès aux abonnés, notamment parce que les internautes n'auraient pas l'obligation de fournir une adresse *e-mail* aux fournisseurs d'accès à internet.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES SERVICES ILLICITES ET LEURS OPÉRATEURS

Les ventes de boîtiers permettant d'accéder à des contenus illicites semblent très importantes et ce depuis plusieurs années. Il existerait trente marques différentes de ce type de matériel à Taïwan selon l'*International Intellectual Property Alliance* (IIPA), une association d'ayants droit américains.

En avril 2019, la loi sur le droit d'auteur a été modifiée pour prévoir des sanctions pénales pour les personnes physiques et les personnes morales qui :

- fournissent des logiciels, tels que des logiciels pair à pair ou des applications qui permettent au public d'accéder à des copies non autorisées de films et de programmes de télévision sur internet ;
- aident le public à accéder à ces copies non autorisées de films et d'émissions de télévision ;
- ou fabriquent ou importent des appareils avec ces logiciels ou applications préchargés.

Les sanctions encourues sont une peine pouvant aller jusqu'à deux ans d'emprisonnement et/ou une amende maximale d'environ 15 000 euros.

Cette modification législative est intervenue à la suite des directives publiées en 2018 par l'Office de propriété intellectuelle de Taïwan, selon lesquelles les lecteurs de contenu en *streaming* sont interdits en vertu de la loi sur le droit d'auteur, ainsi que d'une décision de la cour de propriété intellectuelle d'août 2018 confirmant cette interprétation.

C'est dans ce contexte que le 31 juillet 2019, la cour de propriété intellectuelle a statué contre une entreprise qui exploitait une application qui facilitait l'accès à du contenu télévisé non autorisé. Bien que la cour ait infligé à l'entreprise des amendes relativement faibles, elle a également prononcé des peines de prison contre deux dirigeants de l'entreprise.

En avril 2020, la police de Taïwan a fermé 8maple.ru, le plus grand site de films et d'émissions de télévision pirates du pays. L'action est intervenue à la suite d'une enquête menée par l'ACE, la MPA et le groupement anti-piratage japonais CODA.

VIETNAM

CHIFFRES CLÉS 2020

DÉMOGRAPHIE

97,3 POPULATION^[1]
en millions

68,7 % TAUX DE PÉNÉTRATION
INTERNET (2019)^[2]

USAGES ILLICITES^[3]

3,6 NOMBRE DE VISITES DE SERVICES ILLICITES
en milliards

53 NOMBRE DE VISITES DE SERVICES
ILLICITES PAR INTERNAUTE

Répartition des usages illícites par mode d'accès en %



La MPA relevait en 2017 que les sites illícites vietnamiens recevaient 105 millions de visiteurs par mois quand les sites de l'offre légale n'en recevaient que deux millions^[4].

Le piratage s'est en outre vu renforcé par l'accès d'une majorité grandissante de la population à l'internet à haut débit^[5].

Dans ce contexte, le gouvernement s'est impliqué dans la lutte contre le piratage. Un décret de 2017 (le décret n° 17/2017 / ND-CP) autorise ainsi le ministère de l'Information et de la Communication

(MIC) à prendre des mesures contre les infractions en ligne.

Le ministère a également publié la décision n° 1278 / QD-BTTTT, qui a autorisé un projet visant à « renforcer la capacité du MIC à lutter contre les infractions et les délits en ligne ». Dans le cadre de ce projet, mis en œuvre de 2017 à 2020, il est prévu que le ministère et les autres autorités compétentes modifient la réglementation pour améliorer la protection des droits, mettent en place des formations techniques et travaillent à une réforme institutionnelle.

LES ACTIONS VISANT LES INTERNAUTES

La législation vietnamienne prévoit que le ministère de l'Information et de la Communication peut prononcer des amendes d'un montant maximum de 250 millions de dongs (soit environ 10 000 euros) pour une personne phy-

sique et 500 millions de dongs (soit plus de 19 000 euros) pour une personne morale.

[1] Fonds des Nations unies pour la population (UNFPA).

[2] Union internationale des télécommunications (UIT).

[3] MUSO.

[4] <https://vietnamnews.vn/sunday/features/379196/tv-film-piracy-remain-big-concern-in-vn.html#p8IIRd0OqHf78Vky.97>

[5] D'après le rapport *Measuring the Information Society Report 2017* disponible via le lien suivant

https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf, le pourcentage de personnes utilisant internet au Vietnam est passé de 43,5 % en 2015 à 46,5 % en 2016, et en 2016 on dénombrait environ 47 abonnements à internet à haut débit pour 100 résidents vietnamiens.

Par ailleurs, une circulaire conjointe du ministère de l'Information et de la Communication et du ministère de la Culture, des Sports et du Tourisme de 2012^[6] impose aux opérateurs de réseaux sociaux, en plus de la suppression des contenus litigieux, d'envoyer un

avertissement à leurs utilisateurs qui ont violé le droit d'auteur, les sensibilisant sur la possibilité qu'il leur soit réclamé de réparer les dommages civils causés par ces violations et la possibilité de sanctions administratives et de poursuites pénales.

LES ACTIONS VISANT À LUTTER CONTRE LES SERVICES ILLICITES

LES ACTIONS CONTRE LES SERVICES ILLICITES ET LEURS OPÉRATEURS

Alors que le Vietnam a pu être cité comme un pays hébergeant des sites illicites très populaires, la mise en œuvre des outils existants ne semble pas permettre de lutter efficacement contre ces services. Ainsi, une plainte administrative a été déposée en 2016 contre le site Chiasenhac, qui proposait illicitement des œuvres musicales, et qui appartient à une société vietnamienne. À la suite de cette plainte auprès du ministère de l'Information et de la Communication, le site a été condamné à une amende et enjoint de supprimer tout contenu contrefaisant. Cependant, ses activités illicites ont continué depuis lors. Il en a été de même pour le site 123movies, pour lequel les titulaires de droits américains ont fourni des preuves des violations au ministère de la Sécurité publique. Le site a ensuite fermé mais ses opérateurs n'ont pas été poursuivis et de nombreux sites « miroirs » ont ensuite vu le jour.

LES MESURES ADMINISTRATIVES DE BLOCAGE

Le ministère de l'Information et de la Communication et le ministère de la Culture, des Sports et du Tourisme (MCST) ont promulgué en 2012 une circulaire qui impose aux fournisseurs de services intermédiaires – soit les fournisseurs d'accès à internet, les fournisseurs de services d'hébergement, les moteurs de recherche, les plateformes et les réseaux sociaux – à la demande de ces ministères ou à celle de toute autre autorité gouvernementale, de supprimer ou de désactiver l'accès aux contenus litigieux et de mettre un terme à la fourniture de leurs services lorsque le droit d'auteur et les droits voisins seraient menacés. En novembre 2018, un site rediffusant illicitement des rencontres sportives a ainsi été bloqué.

LES MESURES D'ASSÈCHEMENT DITES « FOLLOW THE MONEY »

La *Vietnam Content Alliance* – regroupant des producteurs et des distributeurs de contenus vietnamiens et internationaux, notamment américains – a mis en place la création d'une liste de sites illicites, laquelle est utilisée dans le cadre d'un effort conjoint du secteur privé et du gouvernement afin d'empêcher le placement de publicités sur les sites listés.

[6] Circulaire No. 07/2012/TTLT-BTTTT-BVHTTDL sur les stipulations relatives à la responsabilité des fournisseurs de services intermédiaires concernant la protection du droit d'auteur et des droits voisins sur internet et les réseaux de télécommunications.

HAUTE AUTORITÉ POUR
LA DIFFUSION DES ŒUVRES
ET LA PROTECTION
DES DROITS SUR INTERNET

4 rue du Texel - 75014 Paris - France
www.hadopi.fr