

Le piratage audiovisuel

De l'urgence d'apporter
une réponse transversale

LIVRE BLANC
JUN 2021

Forward 

À PROPOS

Forward Global est une société d'intelligence économique, d'affaires internationales et de cybersécurité. Notre mission consiste à réduire les risques auxquels sont exposés nos clients (institutions, entreprises, dirigeants), à renforcer les positions en amont d'une décision, mais également dans la conduite des opérations.

Le cabinet accompagne ses clients, au niveau local et international :

- dans la gestion des affaires sensibles (négociations, attaques cyber, litiges, restructurations) ;
- lors d'opérations de croissance (M&A, implantation internationale, accompagnement sur les grands projets) ;
- au moment de construire un positionnement stratégique (communication, affaires publiques, digital) ;
- dans la maîtrise de leurs risques cyber et la réponse aux attaques ciblant l'ensemble des systèmes critiques.

Forward Global produit des rapports et des études de référence et accompagne ses clients dans leur exploitation. Ils sont destinés à une mise en œuvre immédiate, au service du développement commercial opérationnel ou de la prise de décision stratégique. Ces analyses et recommandations sont directement actionnables et sont conçues comme des outils avec un effet de levier à fort impact.

Dans les opérations de lutte contre la fraude et la criminalité internationale, Forward Global intervient dans de nombreux contextes : piratage de contenus (*streaming*, P2P, DDL, IPTV), contrebande, contrefaçon de produits ou de modèles, mésusage, craquage de logiciels ou de matériels, fraude, identification, suivi et accompagnement au démantèlement de réseaux criminels, recel de fuites de données. Le cabinet offre à cet égard un continuum d'expertises pour la cartographie et analyse des écosystèmes criminels, l'altération de l'offre illicite et l'évaluation de l'exposition à la menace.

AUTEURS

Matthieu Creux est le fondateur et le président d'Forward Global. Il fut auparavant membre du cabinet du ministre de l'Enseignement supérieur et de la Recherche et consultant en affaires publiques. Spécialiste des questions de criminalité sur Internet, du suivi des activistes en ligne, en passant par le piratage et la contrefaçon, il est notamment l'auteur d'un ouvrage sur le cyberdijihadisme, publié en 2019.

Directeur général d'Forward Global, **Antoine Violet-Surcouf** détient une expertise spécifique dans les opérations de surveillance complexes et de lutte contre la criminalité économique, dont la contrefaçon et la fraude.

Samuel Dralet est le fondateur de la société Lexfo, filiale cybersécurité d'Forward Global, qui s'est imposée comme un acteur majeur de l'évaluation de la sécurité et de la réponse aux incidents. Il accompagne depuis une dizaine d'années, sur les aspects techniques, plusieurs acteurs de l'audiovisuel, du luxe ou pharmaceutiques sur les problématiques de marché noir (piratage, contrefaçon, fraude...).

Julien Tran Van Nhieu est consultant au pôle Intelligence stratégique d'Forward Global. Il intervient principalement sur des sujets relatifs au numérique et à la défense.

avisa
partners



Dans le domaine du piratage en ligne également, on assiste à une redéfinition des acteurs. Se sont créées, notamment autour du streaming, de véritables organisations mafieuses internationales qui mélangent souvent l'abus en matière de droits d'auteur, la pornographie et d'autres types de délinquance numérique.

Mounir MAHJOUBI

Secrétaire d'État chargé du Numérique
Propos à l'Assemblée nationale,
le 27 septembre 2017

Ce mois de juin, l'Assemblée nationale examinera le projet de loi relatif à « *la protection de l'accès du public aux œuvres culturelles à l'ère numérique* » destiné à instaurer de nouvelles mesures contre le piratage audiovisuel. Un texte adopté en première lecture au Sénat en mai dernier, qui s'inspire des dispositions initiées en novembre 2019, relatives à « *la communication audiovisuelle et à la souveraineté culturelle à l'ère numérique* », suspendues en raison de la crise sanitaire. À cette occasion, Forward Global dresse un panorama des enjeux liés au piratage et des solutions envisageables pour maximiser l'efficacité du dispositif de lutte contre ce phénomène.

Le piratage, considéré à tort comme « *un crime sans victime* », n'est pas un simple « *concurrent sans visage* » pour les créateurs de contenus, les ligues sportives et leurs ayants droit. Son écosystème a beaucoup évolué ces dernières années, avec une « *criminalité en col blanc* » qui s'est progressivement substituée aux « *Robins des bois* » des premières heures d'Internet. Ces nouveaux acteurs, qui ont migré vers un espace peu régulé dans lequel il leur est techniquement aisé de préserver leur anonymat, se servent aujourd'hui du piratage pour se financer en complément de leurs activités « *offline* » historiques (trafic de drogue, proxénétisme, trafic d'êtres humains...).

Une réalité bien souvent méconnue du grand public comme de certains élus, et qui amène à s'interroger sur l'adaptabilité du dispositif actuel de lutte contre le piratage. D'autant plus au regard des dommages qui découlent de cette pratique pour l'économie française, et plus particulièrement pour les secteurs de la culture et du sport, mais aussi pour les utilisateurs eux-mêmes, notamment les plus jeunes.

Et force est de constater que celui-ci ne prend pas la mesure de l'adversaire auquel nous faisons face, ni les difficultés inhérentes à la multiplicité des acteurs impliqués (hébergeurs, moteurs de recherche, fournisseurs d'accès à Internet...), et encore moins le haut niveau de réactivité nécessaire pour faire face à cette pratique.

Dès lors, dans l'objectif de maximiser l'efficacité de notre système de lutte contre le piratage et ainsi rétablir un semblant d'équité entre les forces en présence, les propositions suivantes devraient être prises en considération.

De manière générale

- Renforcer les campagnes de prévention sur les dangers du piratage, notamment auprès des plus jeunes, en requalifiant cette problématique en tant qu'enjeu transversal ;
- Promouvoir au niveau européen la redéfinition du régime de responsabilité des hébergeurs Web et des sites d'hébergement de fichiers dans le cadre du Digital Services Act (DSA), dont les dispositions « *Know your business customer* » (KYBC) doivent être étendues à ces acteurs ;
- Encadrer l'utilisation des DNS alternatifs afin d'améliorer l'efficacité des blocages exercés par les fournisseurs d'accès à Internet (FAI) ;
- Limiter l'apparition de contenus enfreignant le droit d'auteur sur les moteurs de recherche. Si Google doit faire l'objet d'une attention particulière, d'autres tels que Bing, Yahoo... ne peuvent être négligés.

Au niveau procédural

- Réformer les délais d'enquête et de procédure afin d'accélérer le traitement des atteintes aux droits de la propriété intellectuelle ;
- Créer un délit d'atteinte aux droits d'exploitation des manifestations ou compétitions sportives au sens de l'article L333-1 du Code du sport ;
- Doter le projet d'un « *Parquet national numérique* » d'une compétence concurrente nationale pour la poursuite des infractions en matière d'atteintes aux droits de la propriété intellectuelle et des infractions connexes ;
- Créer une compétence concurrente du tribunal judiciaire de Paris avec des attributions sur l'ensemble du territoire national pour la poursuite, l'instruction et le jugement des infractions en matière d'atteintes aux droits de la propriété intellectuelle et d'infractions connexes. Le procureur de la République, le pôle de l'instruction, le tribunal correctionnel exerçant une compétence concurrente à celle qui résulte de l'application des articles 43, 52 et 382 du Code de Procédure pénale, le tout avec pouvoir de dessaisissement du Parquet ou du juge d'instruction déjà saisi d'une affaire ;

- Créer un référent cyber de niveau « *magistrat* » dans chaque tribunal judiciaire de France, tant au siège qu'au parquet, afin d'orienter les affaires, communiquer avec les autres référents et mettre en œuvre les actions de coordination sous l'égide du « *parquet national numérique* » ;

- Former de manière continue et approfondie tous les intervenants de la chaîne pénale (enquêteurs et magistrats du parquet et du siège), incluant des missions d'observations à l'étranger et des rencontres avec leurs homologues européens et internationaux.

En termes de moyens opérationnels

- Renforcer significativement les ressources humaines, techniques et financières des services d'enquête en matière d'atteinte à des droits de propriété intellectuelle et aux droits d'exploitation des manifestations ou compétitions sportives ;
- Créer une Brigade anti-cybercriminalité unifiée (BACU) regroupant les moyens et les ressources de plusieurs services d'enquête (l'OCLCTIC, le C3N, la DNRED-SNDJ, voire la DGSJ suivant l'ampleur de l'organisation criminelle) et compétente en matière d'atteintes aux droits de la propriété intellectuelle ;
- Étendre les pouvoirs d'enquête spéciaux aux infractions en matière de droits de la propriété intellectuelle ou à des droits similaires, par extension de l'application des articles 706-80 à 706-87 (surveillance et infiltration), 706-89 à 706-94 (perquisitions) et 706-95 à 706-103 (accès à distance aux correspondances, recueil des données techniques de connexion et des interceptions de correspondances, sonorisation, captation des données informatiques) du Code de procédure pénale, à l'image de la récente extension de leur application aux atteintes aux systèmes de traitement automatisé de données (STAD) ;
- Renforcer significativement la coopération internationale entre les services d'enquête à des fins de collecte des preuves.



SOMMAIRE

INTRODUCTION	2
CHAPITRE 1 / LE PIRATAGE AUDIOVISUEL EN FRANCE	5
1. Un manque à gagner substantiel pour l'État et la filière audiovisuelle	6
2. Vers une industrialisation professionnelle du piratage	9
CHAPITRE 2 / UN ENVIRONNEMENT COMPLEXE ET STRUCTURÉ	14
1. La structuration d'une économie souterraine lucrative	22
2. Panorama des principales conséquences du piratage	29
CHAPITRE 3 / LA NÉCESSITÉ D'UNE ACTION RÉGALIENNE, SYSTÉMIQUE ET TRANSVERSALE	29
1. Le piratage audiovisuel : facteur de déstabilisation de l'ordre public numérique	30
2. Un cadre législatif à réformer pour contrer le caractère protéiforme du piratage	32
3. L'indispensable concours d'un renforcement de la sphère police-justice	39
ANNEXES	50
REMERCIEMENTS	65

A decorative dotted line in white and light blue starts from the top left corner and curves downwards towards the right, ending near the center of the page.

INTRODUCTION

La crise sanitaire a rappelé que la culture, outre son importance dans le quotidien de beaucoup d'individus, était plus que jamais un « *réconfort en période d'anxiété* ».

Lors du confinement de mars 2020, les consommations culturelles en ligne des Français ont considérablement augmenté. L'audiovisuel (films et séries télévisées), déjà bien ancré dans leurs habitudes, en a été le principal bénéficiaire².

Si la consommation audiovisuelle s'est développée lors du premier confinement, celle de contenus piratés également. La crise sanitaire a en effet remis en cause les efforts de lutte contre le piratage³, initiés depuis plusieurs années, par les autorités publiques et les ayants droit. En témoigne notamment le report du projet de loi sur l'audiovisuel de novembre 2019 pourtant encourageant en la matière.

En novembre 2019, le gouvernement a initié le projet de loi relatif à la « communication audiovisuelle et à la souveraineté culturelle à l'ère numérique », amendé par la Commission des affaires culturelles de l'Assemblée nationale en mars 2020. Le texte prévoyait des mécanismes innovants pour la protection en ligne les contenus audiovisuels, aussi bien en termes de prérogatives que de moyens, avec la fusion de l'Hadopi et du CSA au sein d'une autorité aux pouvoirs élargis. Reportés avec la crise Covid-19, les échanges parlementaires ont été relancés en mai 2021.

Le piratage audiovisuel est une pratique ancienne. Il consiste à partager illégalement des contenus linéaires (télévision et matchs sportifs) et non linéaires (films, séries, etc.), auxquels sont attachés des droits d'auteur ou d'exploitation. Auparavant diffusés sur des supports physiques (tels que la VHS et le DVD), les contenus piratés sont désormais de plus en plus diffusés sur Internet via de nombreux protocoles de communication, tels que le *peer-to-peer* le *streaming* et le téléchargement direct.

Peer-to-peer (P2P)

Réseau d'échange et de partage de fichiers entre internautes, qui consiste à mettre directement en liaison un demandeur avec un détenteur du contenu convoité

Streaming

Mode de transmission de données vidéos en flux continu dès que l'utilisateur sollicite le contenu audiovisuel plutôt qu'après son téléchargement complet

Téléchargement direct (DDL)

Pratique de mise à disposition de fichiers téléchargeables directement sur le serveur d'une plateforme d'hébergement de fichier

Bien loin d'être un « crime sans victime », le piratage touche l'ensemble de la chaîne de valeur de la création audiovisuelle et du sport. Si cette pratique nuit à de nombreux métiers (scénaristes, distribution, sport amateur, etc.), elle profite en revanche à tout un écosystème d'acteurs qui cherchent à s'approprier les bénéfices de contenus en les copiant et en les partageant illégalement.

¹ Ernesto Ottone, « La culture, un besoin vital en temps de crise », *UNESCO [en ligne]*, 29 mars 2020.

² Anne Jonchery, Philippe Lombardo, « Pratiques culturelles en temps de confinement », *Culture - Étude*, Juin 2020, p. 12.

³ Hadopi, *Baromètre de la consommation de biens culturels dématérialisés*, Février 2021, pp. 30-31.

Plusieurs raisons poussent le consommateur vers des contenus piratés dits « warez⁴ » :

- Des motifs économiques (« *Je ne vais pas payer pour quelque chose de gratuit en ligne* ») avec des offres légales dont le cumul est parfois onéreux (« *Je paie déjà deux abonnements TV pour le foot* ») ;
- La disponibilité des contenus (l'envie d'accéder immédiatement à des nouveautés), là où les catalogues d'offres légales peuvent être jugés limités (« *Ce documentaire n'est pas sur le Netflix français* ») ;
- La banalisation du piratage (« *Tout le monde le fait, pourquoi pas moi ?* »).

La consommation d'œuvres illicites revêt ainsi plusieurs formes : elle peut être ponctuelle, hybride (complémentaire à une offre légale) ou exclusive, rendant le piratage plus difficile à appréhender. D'autant que l'impact réel sur les ventes légales est ambigu, en raison des effets d'échantillonnage et de substitution qui peuvent s'assortir à un acte de piratage. Ces effets consistent respectivement à tester un contenu avant de l'acheter, pour en vérifier la qualité, et à considérer qu'une œuvre acquise illégalement ne conduira pas à son achat⁵. S'il reste difficile de savoir quel effet prévaut pour les films et les séries, celui de la substitution domine dans le cas des retransmissions sportives, tant un match perd de sa valeur une fois terminé.

Le retrait rapide de contenus illicites est un enjeu au cœur de la lutte contre le piratage

Les enjeux relatifs au piratage de films et de séries sont alors sensiblement distincts à ceux des événements sportifs, qui appellent à une réaction quasi instantanée. Pour autant, leurs conséquences sont similaires et ne concernent plus seulement l'atteinte à des droits d'auteur ou d'exploitation.

Le niveau de réactivité au partage de contenus contrefaisants demeure l'un des principaux enjeux de la lutte contre le piratage. Ce défi appelle à une réflexion sur les outils dont les créateurs de contenus, les diffuseurs sportifs et leurs ayants droit disposent pour obtenir le retrait de leurs œuvres mises en ligne illégalement. La suppression totale de ce type d'infractions étant un vœu pieux, il s'agit surtout de réduire leur volumétrie jusqu'à un niveau « supportable », afin d'une part de limiter les impacts néfastes sur les consommateurs, et d'autre part de préserver le potentiel de création de l'industrie culturelle.

Le présent livre blanc, après avoir rappelé le contexte et les fondements du piratage audiovisuel, s'efforcera de présenter son écosystème d'acteurs, ainsi que les limites des différentes mesures mises en place jusqu'à présent pour contrer cette menace. Il formule également des recommandations au profit des législateurs.

⁴ Jargon pour désigner la distribution illicite de biens culturels copiés.

⁵ Bastard Irène, Bourreau Marc, Moreau François, « L'impact du piratage sur l'achat et le téléchargement légal. Une comparaison de quatre filières culturelles », *Revue économique*, Vol. 65, 2014, p. 574.

LE PIRATAGE AUDIOVISUEL EN FRANCE



avisa
partners

UN MANQUE À GAGNER SUBSTANTIEL POUR L'ÉTAT ET LA FILIÈRE AUDIOVISUELLE

Le piratage de contenus audiovisuels (films, séries, événements sportifs, etc.) représente un coût social et économique significatif pour l'État et les ayants droit. Ce phénomène englobe une diversité de pratiques illicites qui, outre porter atteinte aux droits de la propriété intellectuelle, sont à l'origine d'un manque à gagner considérable pour les acteurs des secteurs de l'audiovisuel et du sport.

COÛT DU PIRATAGE AUDIOVISUEL ET SPORTIF EN 2019⁶



11,8 millions de consommateurs uniques de contenus illégaux



Potentiel de **création de 2 650 emplois** dans la filière audiovisuelle



Pertes de **332 millions d'euros** pour les finances publiques



Un manque à gagner total estimé à **1,03 milliards d'euros**



Complémentaire avec la lutte contre les services illicites, la promotion des offres légales demeure un outil très efficace contre le piratage.

Pauline BLASSEL
Secrétaire générale de l'Hadopi

L'Hadopi relève désormais l'existence d'une « *consommation hybride légale et illicite*⁷ » des contenus audiovisuels. Les internautes contrevenants étant bien souvent abonnés en parallèle à des services légaux de télévision payante et/ou de vidéo à la demande. Leur consommation illicite se restreint donc à des contenus plus ciblés leur permettant de compléter des offres légales dont les catalogues sont jugés trop restreints, ou d'éviter de cumuler des abonnements dont le coût total est considéré comme trop élevé. Cet usage mixte a résolument influencé la consommation de contenus⁸.

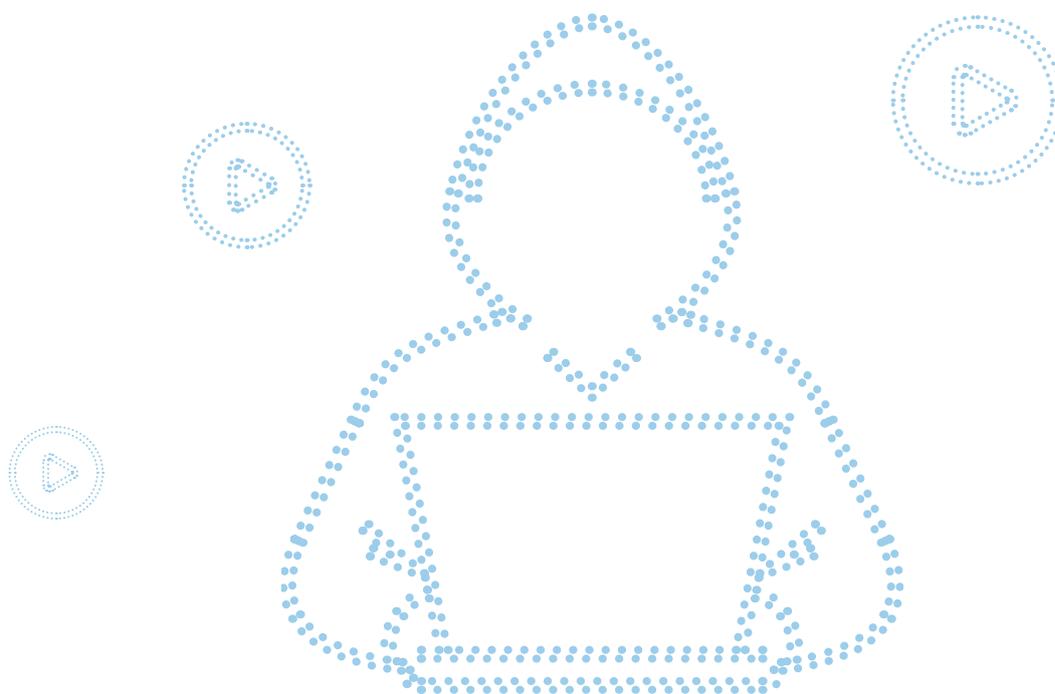
⁶ Hadopi, *Étude de l'impact économique de la consommation illicite en ligne de contenus audiovisuels et de retransmissions*, Décembre 2020, p. 3.

⁷ *Op. cit.* Hadopi, Décembre 2020, pp. 33-34

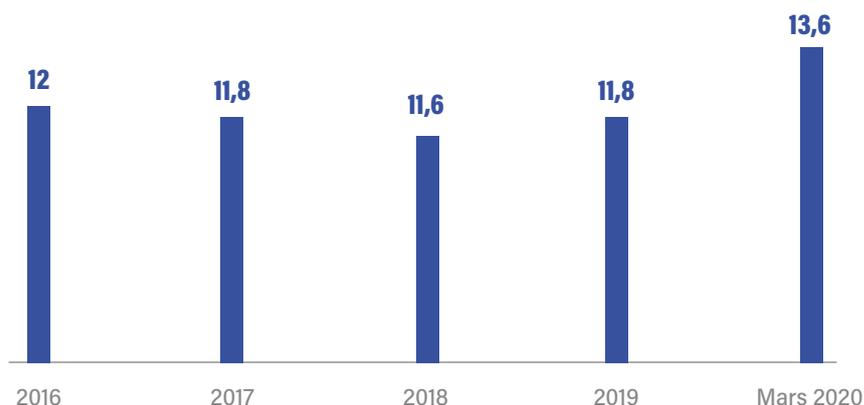
⁸ EY, *Piratage en France*, Juin 2018, p. 8.

En 2019, les individus ayant consommé de façon illicite au moins un bien culturel dématérialisé dans l'année – musique, film, série, photo, jeux vidéo, logiciel et livre – représentaient 26 % des internautes de plus de quinze ans. Plus d'un internaute sur quatre pratique donc la consommation de contenus piratés.

Si le développement et la promotion des offres légales ont contribué à impulser une légère réduction de la proportion de consommateurs de biens piratés parmi les internautes depuis 2017, cette dernière s'est néanmoins interrompue à partir de 2019 avec de nouveaux facteurs haussiers (tels que l'essor de l'IPTV) auxquels se sont rajoutés les effets de la crise sanitaire en général et des confinements en particulier sur les pratiques de consommation culturelle. Le nombre de consommateurs de contenus audiovisuels portant atteinte au droit d'auteur est ainsi devenu très sensiblement supérieur au niveau de 2016, avec plus de 1,5 million de nouveaux internautes pirates sur cette période.



NOMBRE D'INTERNAUTES AYANT DES USAGES AUDIOVISUELS ILLICITES (EN MILLIONS) 2016 - 2020^{9, 10}



13,6 millions de consommateurs de contenus piratés en mars 2020

La crise du Covid-19 et le premier confinement ont en effet modifié les habitudes de consommation de nombreux internautes. Il peut ainsi être observé, au premier semestre 2020, une augmentation de la consommation de contenus piratés en tout genre (audiovisuels, musique, livre, etc.).

En 2019, le manque à gagner était évalué à 1,03 milliard d'euros, soit environ la moitié du budget du plan de relance économique post-crise consacré à la culture en France¹¹. En particulier, des modes de consommation tels que la vente physique (DVD et disque Blu-ray), la vidéo à la demande par abonnement (SVOD), ainsi que la vente d'abonnements à la télévision payante, ont par exemple subi des manques à gagner conséquents, à hauteur de 76 %, 10 % et 8 % de leurs marchés respectifs sur l'année 2019¹².



⁹ *Op. cit.* Hadopi, Décembre 2020, p. 31.

¹⁰ *Compte rendu n°19*, Commission des affaires culturelles et de l'éducation, Assemblée nationale, 8 Décembre 2020.

¹¹ Plan de relance : un effort de 2 milliards d'euros pour la Culture, *Ministère de la Culture* [en ligne], 3 septembre 2020.

¹² *Op. cit.* Hadopi, Décembre 2020, p. 38.

VERS UNE INDUSTRIALISATION PROFESSIONNELLE DU PIRATAGE

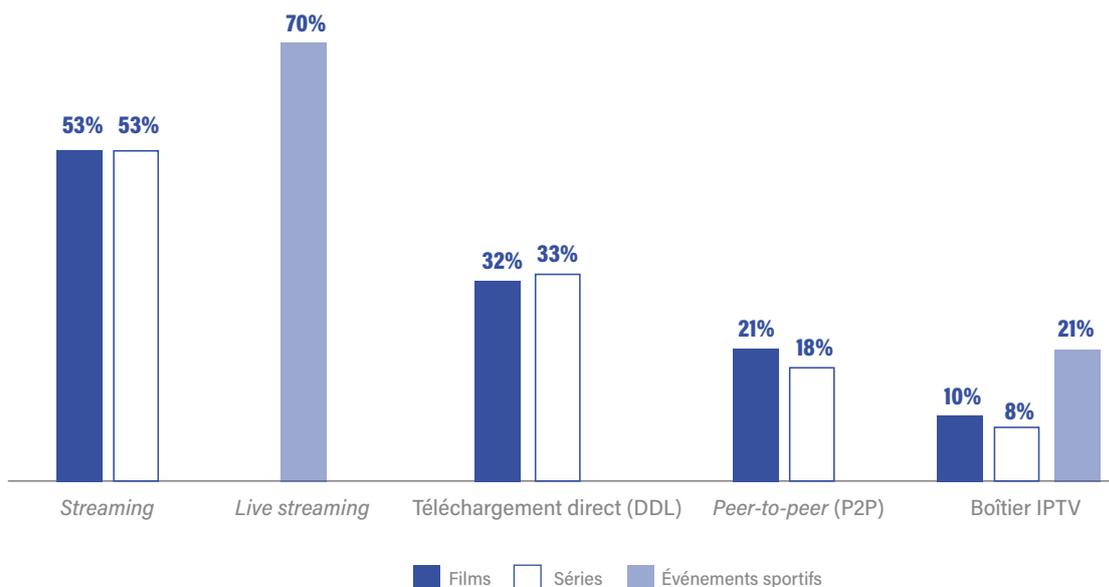
Deux grands modèles économiques structurent désormais les modes de piratage¹³ :

- La monétisation publicitaire, qui permet aux hébergeurs de fichiers et aux sites de référencement de contenus illicites de valoriser leurs audiences. Ces acteurs privilégient des types spécifiques de piratage (*streaming*, *peer-to-peer*, téléchargement direct) qui se sont pérennisés avec la numérisation accrue des espaces publicitaires et le développement du numérique (réduction des coûts de stockage, augmentation des niveaux de compression vidéo et de débit Internet).
- Les offres d'abonnement mensuels voire annuels, sur lesquels les services d'*Internet Protocol Television* (IPTV) se fondent. Alors que l'accès par abonnement à des contenus linéaires s'effectuait auparavant via des pratiques complexes (telles que le *card sharing*), l'IPTV permet désormais d'accéder à des contenus linéaires et non linéaires, légaux et illégaux, en tout simplicité.

Le développement de l'IPTV illégal est le signe d'une industrialisation en cours de solutions désormais semi-professionnelles de piratage. Loin d'être le fait de hackers isolés, cette pratique à grande échelle est organisée par des réseaux mafieux qui se rémunèrent grâce aux abonnements¹⁴.

L'IPTV est un mode de piratage dont l'utilisation monte en puissance partout en Europe

MODES DE CONSOMMATION ILLICITE DE CONTENUS AUDIOVISUELS



SOURCE : HADOPI¹⁵

¹³ *Op. cit.* Hadopi, Décembre 2020, p. 34.

¹⁴ « IPTV : le streaming dans l'ombre de la mafia », *Rude Baguette* [en ligne], 27 janvier 2020.

¹⁵ *Op. cit.* Hadopi, Février 2021, p. 39.

Principaux modes de piratage audiovisuel

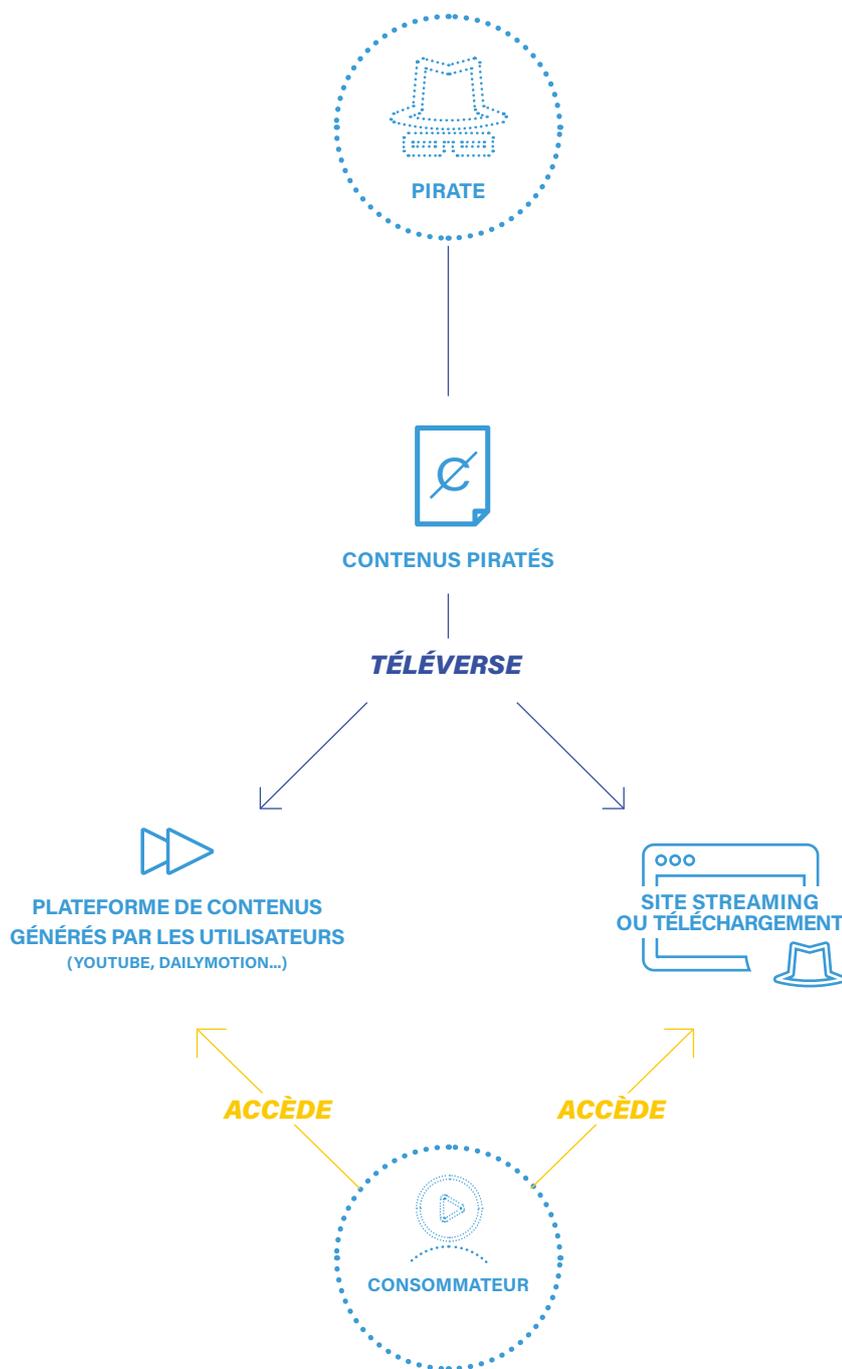
Mode de piratage	Description	Taux d'utilisation*		Acteurs impliqués**	Financement
		Films et séries	Événements sportifs		
<i>Streaming</i>	Ce mode de transmission de données en flux continu permet à un internaute de visionner directement des vidéos à partir d'un site Internet.	50%		Moteur de recherche Fournisseur d'accès à Internet Virtual Private Network Registraire de nom de domaine Hébergeur web Hébergeur de fichiers Réseaux sociaux Régie publicitaire Intermédiaire de paiement	Publicité
<i>Peer-to-peer (P2P)</i>	Le P2P permet le téléchargement d'un fichier partagé sur un réseau d'ordinateurs de particuliers. Ce protocole met un utilisateur en liaison directe avec un ou plusieurs autres pour l'obtention d'un fichier spécifique.	20%			
<i>Téléchargement direct (DDL)</i>	Mise à disposition d'un fichier sur un serveur de stockage accessible depuis un site Web. Cette pratique propose des contenus souvent de bonnes qualités.	30%			
<i>Card sharing</i>	Le <i>card sharing</i> repose sur l'acquisition, outre d'un décodeur et d'une parabole, à un abonnement partagé sur Internet pour accéder gratuitement à des bouquets de TV payante.	NC	NC		Abonnement
<i>Internet Protocol Television (IPTV)</i>	Mode de consommation de flux de télévision via un protocole Internet. Un service IPTV consiste en un logiciel ou un boîtier à connecter qui permettent à l'utilisateur d'accéder à un serveur dans lequel des contenus piratés sont stockés.	9%	21%	Moteur de recherche Fournisseur d'accès à Internet Virtual Private Network Registraire de nom de domaine Hébergeur web Fabricant de boîtiers IPTV Site de commerce de boîtiers IPTV Intermédiaire de paiement	
<i>Live streaming</i>	Mode de consommation d'un contenu linéaire diffusé en direct depuis un site Internet. Ce protocole repose sur le piratage d'offres légales, plus précisément des flux entrants et sortants des décodeurs et des boîtiers connectés à une télévision par câble HDMI.		70%	Moteur de recherche Fournisseur d'accès à Internet Virtual Private Network Registraire de nom de domaine Hébergeur web Hébergeur de fichiers Plateforme de contenu généré par les utilisateurs Fabricant de boîtiers IPTV Site de commerce de boîtiers IPTV Régie publicitaire Intermédiaire de paiement	

* Chez les consommateurs de contenus piratés en 2020. Les modes de piratage peuvent être cumulatifs (Source : Hadopi, Février 2021)

** Les retransmissions sportives sont également diffusées illégalement sur certains réseaux sociaux.

PIRATAGE AUDIOVISUEL

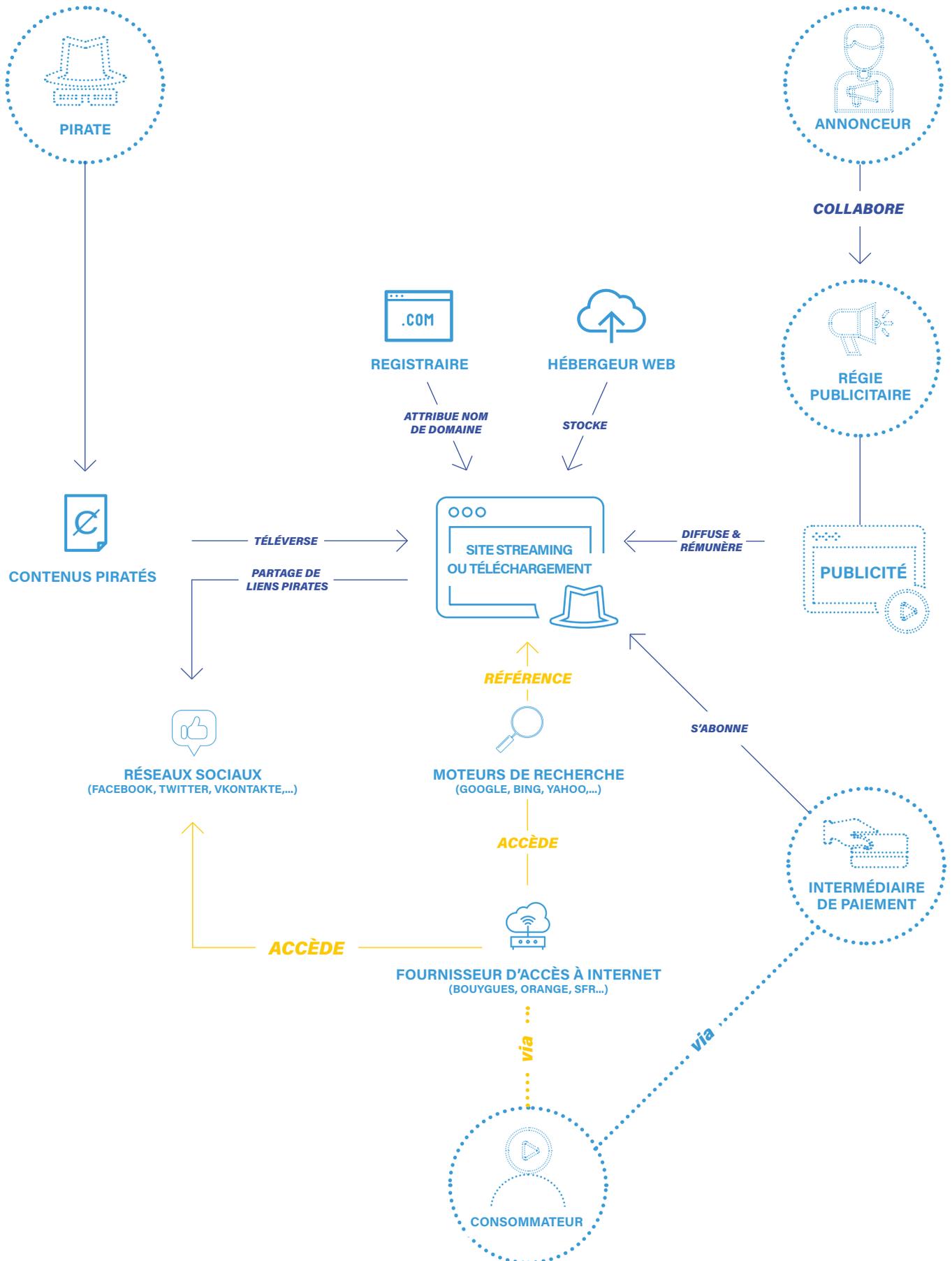
GÉNÉRALITÉS



CARTOGRAPHIE

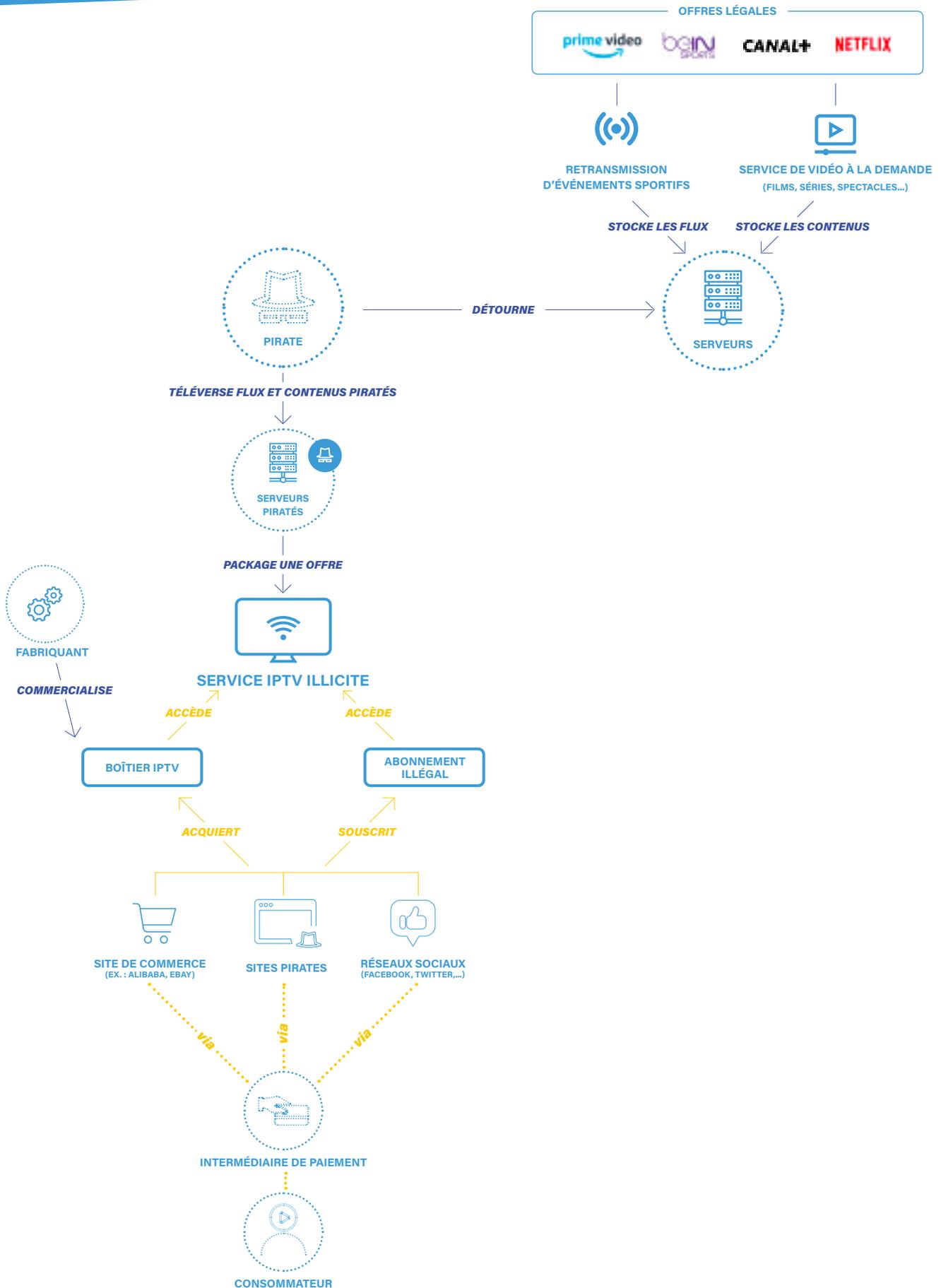
DE LA CHAÎNE DES ACTEURS IMPLIQUÉS DANS LE STREAMING, P2P ET DDL

LE PIRATAGE AUDIOVISUEL : DE L'URGENCE D'APPORTER UNE RÉPONSE TRANSVERSALE



CARTOGRAPHIE

DE LA CHAÎNE DES ACTEURS IMPLIQUÉS DANS L'IPTV

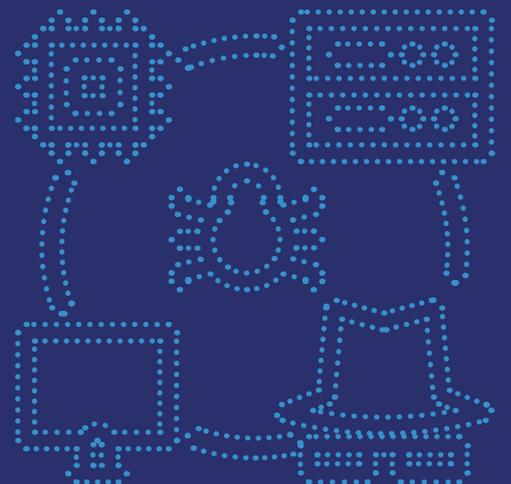


LE PIRATAGE AUDIOVISUEL : DE L'URGENCE D'APPORTER UNE RÉPONSE TRANSVERSALE



**UN
ENVIRONNEMENT
COMPLEXE ET
STRUCTURÉ**

avisa
partners



**LA STRUCTURATION
D'UNE ÉCONOMIE
SOUTERRAINE LUCRATIVE**

1



Un modèle d'organisation quasi générique

En France, les cas récents d'arrestation d'administrateurs de sites illicites permettent de mieux mesurer la portée du piratage audiovisuel. Ces dernières années ont en effet été témoins de la mise en examen de responsables de plusieurs sites, dont ceux de téléchargement direct, « Zone Téléchargement^{16, 17} » (2016), de *peer-to-peer* « Torrent 411^{18, 19} » (2017), de *live streaming* « Beinsport-streaming^{20, 21} » (2018) et de *streaming* « SerieFR^{22, 23} » (2019).

SITES PIRATES FAISANT L'OBJET D'UNE PROCÉDURE JUDICIAIRE

Site	Chiffre d'affaires (en M euros)	Nombre d'internautes (par mois)	Pays			
			Administrateurs	Comptes bancaires	Régies publicitaires	Serveurs
Zone Téléchargement (DDL)	1,5 par an	3 millions	France	Andorre Bélice Chypre, Malte	NC	Allemagne Islande
Torrent 411 (P2P)	6 à 7 par an	2 millions	France, Suède Ukraine	NC	Estonie Suisse	Suède
Beinsport-streaming (<i>live streaming</i>)	NC	500 000	France	Suisse Îles vierges britanniques	NC	NC
SerieFR (<i>streaming</i>)	NC	700 000	France	NC	Estonie Espagne Israël	Pays-bas Suisse

Les quatre sites présentent des modèles d'organisation similaires par le recours à des structures offshore dans le but de préserver au maximum leur anonymat, avec l'utilisation notamment de serveurs et de comptes bancaires situés à l'étranger. Dans chaque cas, les régies publicitaires ont joué un rôle central dans le financement des pirates, ces dernières ayant été à l'origine de la majeure partie de leurs revenus.

¹⁶ Morgane Tual, « Zone Téléchargement : sept questions pour comprendre sa fermeture mouvementée », *Le Monde* [en ligne], 29 novembre 2016.

¹⁷ Gilbert Kallenborn, « Zone Téléchargement, ce petit business familial de 1,5 million d'euros par an », *01net* [en ligne], 29 novembre 2016.

¹⁸ « Fermeture de T411. Que risquent les habitués du site de téléchargement ? », *Ouest France* [en ligne], 28 juin 2017.

¹⁹ Corentin Durand, « T411 : 7 millions d'euros par an, 6 interpellations, 3 ans d'enquête internationale », *Numerama* [en ligne], 27 juin 2017.

²⁰ « Un site pirate de streaming sportif fermé, 5 responsables bientôt jugés », *Rude Baguette* [en ligne], 25 juin 2019.

²¹ « Leurs sites de streaming diffusaient Canal+ et BeInSport », *Capital* [en ligne], 6 mars 2020.

²² « Site illégal de streaming : 8 mois de prison avec sursis requis contre le jeune pirate informatique franc-comtois », *franceinfo* [en ligne], 13 novembre 2019.

²³ « Streaming séries tv : arrestation de plusieurs pirates français », *ZATAZ* [en ligne], 28 mai 2019.

Les pirates : du passionné d'informatique à la criminalité organisée

La diversité des profils impliqués dans le fonctionnement de sites et de services illicites met en exergue la complexité et l'opacité de l'écosystème du piratage audiovisuel. Les informations issues d'opérations des forces de l'ordre et de procédures judiciaires permettent de distinguer *a minima* quatre catégories de pirates :

Une véritable concurrence s'est instaurée à mesure que les sites pirates sont devenus rentables. Les cyberattaques, notamment par déni de service (DDoS), et les tentatives de vols de base de données sont devenues monnaie courante entre sites rivaux, que ce soit par jalousie, dans le cadre de règlements de comptes ou par volonté d'éliminer les nouveaux entrants.

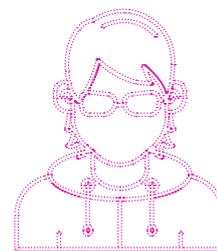


Didier WANG

Expert en protection des contenus et lutte contre le piratage à l'Hadopi

LES « ROBIN DES BOIS »

Ayant pour la plupart la vision d'un Internet gratuit, ces contrevenants mettent à profit leurs compétences techniques dans le but de « rendre service²⁴ » à leurs semblables. Le piratage leur apparaît alors soit comme un moyen d'exercer leur passion pour l'informatique en mettant en place des sites, soit de donner la possibilité de regarder un contenu à ceux n'ayant pas les moyens ou l'envie de souscrire à une offre légale. Ne mesurant pas toujours la gravité et le caractère illégal de leurs activités, ils sont parfois motivés par le gain financier, sans que cela ne constitue leur motivation principale. Cette catégorie concerne aussi bien des étudiants que des salariés à la recherche de revenus complémentaires, qui peuvent agir de manière isolée ou en groupe, sans forcément se connaître.



Les « Robins des bois » sont désormais minoritaires dans l'écosystème des acteurs impliqués dans le piratage audiovisuel en ligne.



Général de brigade Éric FREYSSINET

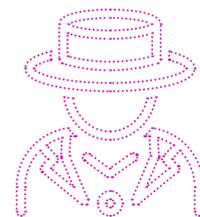
Chef du pôle national de la lutte contre les cybermenaces de la Gendarmerie nationale

²⁴Tristant Brossat, « Vincent, 17 ans, lycéen, et créateur d'un des sites les plus populaires de streaming illégal », *Le Monde* [en ligne], 20 octobre 2018.

LES CYBERCRIMINELS

Cette catégorie se distingue de la précédente par une motivation strictement pécuniaire et par leur professionnalisation. En août 2020, Eurojust a mené une opération contre le groupe Sparks²⁵ actif depuis 2011²⁶ qui formulait des demandes frauduleuses de copies de DVD et de disques Blu-ray auprès de distributeurs légaux. Sparks téléversait ensuite les contenus piratés sur des serveurs disséminés dans le monde entier (France, Corée du Sud, Suisse, etc.), puis les diffusait en exclusivité par voies de *streaming* et de *peer-to-peer*. Les nationalités des membres accusés (États-Unis, Norvège et Royaume-Uni) laissent supposer qu'ils se sont organisés à distance, tout en ne se connaissant pas entre eux réellement.

Cette catégorie de cybercriminels forme le « *noyau dur* » du piratage car elle alimente en nouveautés les réseaux de contrefaçon, puis par ricochet l'ensemble des sites et des services illicites. Leurs productions seraient vendues en priorité aux plus demandeurs, pour être ensuite recopiées à l'envie un peu partout sur la planète. Ces pros de la copie agissent depuis longtemps, à l'échelle internationale, dans les cinémas et ils cherchent constamment à s'infiltrer le plus en amont possible dans les chaînes de production et de distribution des contenus audiovisuels sur support vidéo. Ces pirates ont su diversifier leurs sources d'approvisionnement avec l'émergence des offres et des plateformes numériques.



Le piratage audiovisuel est une source de revenus complémentaires, parmi d'autres activités dédiées à la contrefaçon, de certaines organisations criminelles.

Delphine SARFATI-SOBREIRA
Directrice générale de l'UNIFAB

²⁵ « New major crackdown on one of the biggest online piracy groups in the world: international coordination led by Eurojust », *Eurojust* [en ligne], 26 août 2020.

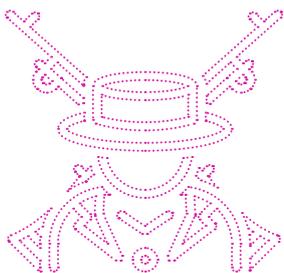
²⁶ Catalin Cimpanu, « Two members of movie piracy group 'Sparks' arrested in Cyprus and the US », *ZDNet* [en ligne], 26 août 2020.

LE CRIME ORGANISÉ

Europol a souligné l'implication d'une « *criminalité en col blanc*²⁷ » dans le piratage audiovisuel. Des réseaux mafieux se sont en effet approprié cette activité, initialement fondée sur le partage et la gratuité, pour structurer un véritable marché mondial²⁸. Pour ces organisations, cette activité à l'avantage d'être peu risquée, sur le plan pénal, et d'apporter un revenu complémentaire à leurs activités historiques²⁹. Partout dans le monde (Canada, Hong Kong, Italie, Japon, Malaisie entre autres), plusieurs groupes sont impliqués à la fois dans le piratage de contenus audiovisuels, la prostitution, les jeux d'argent illégaux, ainsi que le trafic d'armes, de drogues³⁰ et d'êtres humains³¹.

Le crime organisé s'est longtemps appuyé sur la vente physique de DVD pirates et s'est donc logiquement adapté à la numérisation des usages. Selon le quotidien italien *Gazzetta dello Sport*, une branche de la Camorra serait par exemple directement impliquée dans un réseau de service illégal IPTV en Italie³².

En novembre 2020, le Brésil, les États-Unis et le Royaume-Uni ont conjointement mené la seconde phase de l'opération surnommée « 404 », qui a conduit au démantèlement de 282 sites pirates (252 sites brésiliens, 27 sites britanniques et 3 sites américains). Les autorités américaines ont alors déclaré que le *streaming* illégal n'était pas « *un crime sans victime* » et qu'il alimentait « *une entreprise criminelle dont les profits soutiennent les activités du crime organisé*³³ ».



²⁷ Damien Licata, « Rojdirecta, LiveTV Qui se cache derrière les sites de streaming de foot ? », *Le Parisien* [en ligne], 6 novembre 2018.

²⁸ « IPTV : le streaming dans l'ombre de la mafia », *Rude Baguette* [en ligne], 27 janvier 2020.

²⁹ Rémy Sabathie, « Le piratage, un crime presque parfait », *Les dossiers des Yeux du Monde*, n°4, Avril 2014, p. 3.

³⁰ Europol, *IP crime and its link to other serious crimes*, Juin 2020.

³¹ « Film Piracy and Its Connection to Organized Crime and Terrorism », *RAND Corporation* [en ligne], 2009.

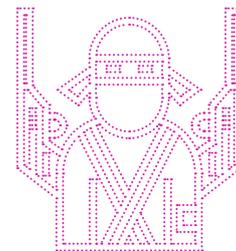
³² « Pirateria tv: ecco l'uomo da 6 milioni di euro. C'è l'ombra della camorra », *Gazzetta dello Sport* [en ligne], 21 octobre 2019.

³³ « U.S. Law Enforcement Assists Brazilian Law Enforcement Takedown of Numerous Digital Piracy Sites and Apps Alleged to Have Caused Millions of Dollars in Losses to U.S. Media Companies », *US Department of Justice* [en ligne], 5 novembre 2020.

LES ORGANISATIONS TERRORISTES

Des liens étroits existent entre le terrorisme et la contrefaçon de manière générale³⁴. Comme pour le crime organisé, certaines organisations terroristes ont fait de la vente de produits contrefaits un moyen d'augmenter leurs revenus et de financer leurs activités, allant du recrutement à l'acquisition d'armes³⁵.

En ce qui concerne plus précisément les contenus audiovisuels, des organisations telles que PIRA (Irlande du Nord) et D-Company (Pakistan) ont eu recours à la vente physique illégale de films³⁶. Au début des années 2000, près de 40 % des confiscations anti-piratage au Royaume-Uni étaient des DVD copiés et commercialisés par la branche pakistanaise d'Al-Qaïda³⁷. Bien qu'il n'existe pas de cas plus récents étudiés, la consommation accrue de supports numériques (*streaming* et téléchargement), au détriment de ceux matériels, pose l'hypothèse d'une possible adaptation ou non de certaines organisations terroristes.



Quels qu'ils soient, les pirates se sont développés de manière relativement indépendante et progressive au cours des dernières années. Alors que certains ont des liens avec des groupes criminels, voire terroristes, d'autres ont progressivement évolué d'eux-mêmes vers une forme de criminalité en bande organisée. Les individus à l'esprit « *Robin des bois* » sont aujourd'hui très minoritaires et ont laissé place à des organisations davantage structurées et professionnelles. Ces derniers agissent avec davantage de moyens pour préserver leur anonymat dans l'espace numérique, les rendant alors plus difficiles à identifier pour les ayants droit et les services d'enquête.

³⁴ Carole Gomez, « Contrefaçon et terrorisme : comprendre les mécanismes », *Revue internationale et stratégique*, n°107, 2017, pp. 32-40.

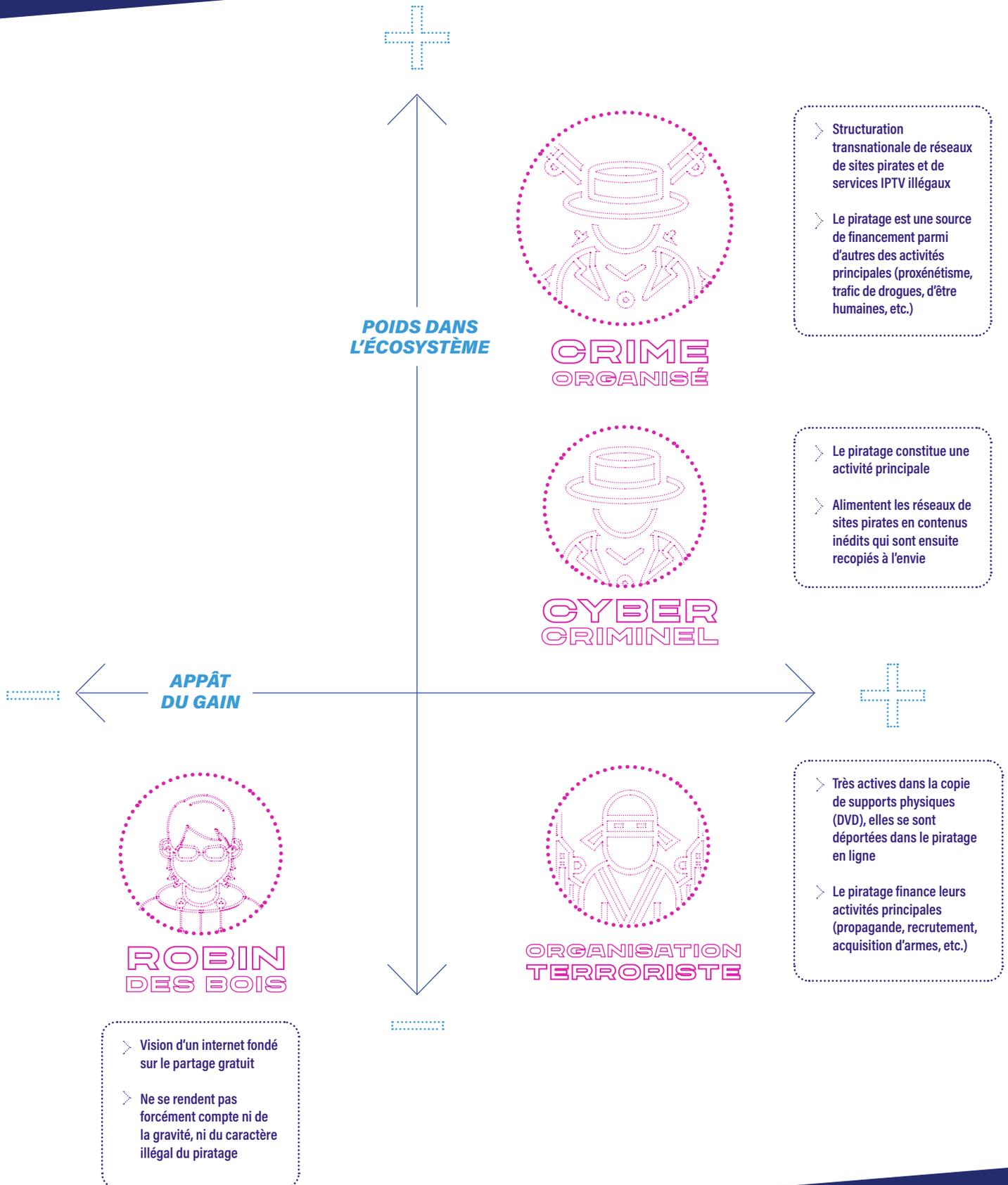
³⁵ UNIFAB, *Contrefaçon et Terrorisme*, 2018.

³⁶ *Film Piracy, Organized Crime, and Terrorism*, RAND Corporation, 2009, pp. 82-95.

³⁷ Kavita Philip, *What is a technological author? The pirate function and intellectual property*, *Postcolonial Studies*, Vol. 8, Institute of Postcolonial Studies, Melbourne, 2005, pp. 200-201.

CARTOGRAPHIE

DES PROFILS DE PIRATES 2.0



PANORAMA DES PRINCIPALES CONSÉQUENCES DU PIRATAGE

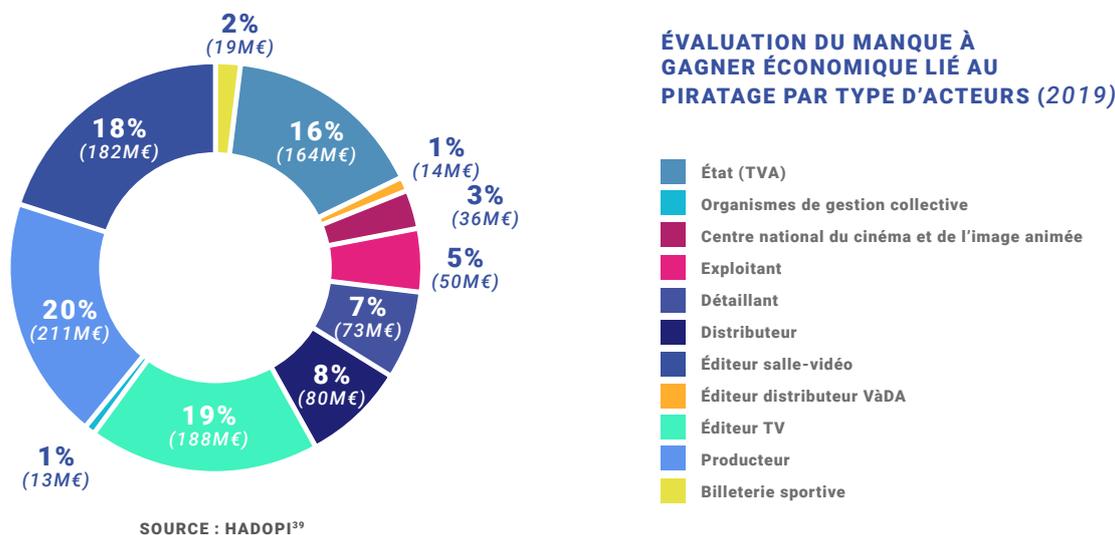
Destruction de valeur dans le domaine de la culture

La chaîne de valeur de l'audiovisuel se structure autour de trois grandes catégories de métiers³⁸ :

- La production des contenus audiovisuels (films, séries, documentaires, contenus de flux, etc.) dont les acteurs, situés en amont de la chaîne, sont les producteurs, les créateurs et leurs ayants droit ;
- L'édition, qui regroupe les éditeurs vidéo (éditeur salle et éditeur physique), les services de télévision, de la vidéo à la demande (VOD) et de la vidéo à la demande par abonnement (SVOD). Tous ces acteurs sont chargés d'agrèger une offre de contenus cohérente, de les éditer (enrichissement, mise en forme et habillage) et de leur *marketing*. Si certains éditeurs commercialisent leurs offres à des distributeurs, d'autres s'autodistribuent directement tels qu'Amazon Prime Video, Apple TV+, Canal+ et Netflix ;
- La distribution, qui consiste à la commercialisation des offres audiovisuelles au grand public. En aval de la chaîne, cette activité regroupe notamment les exploitants de salles de cinéma (UGC, Pathé-Gaumont, etc.), les détaillants de supports physiques (site e-commerce, grandes surfaces spécialisées, etc.) et les acteurs commercialisant une offre de télévision (Bouygues Telecom, Orange, etc.).

Selon une modélisation effectuée par l'Hadopi (cf. *infra*), le piratage a chaque année un impact sur l'ensemble de cette chaîne de valeur. En 2019, les métiers de la production ont par exemple été victimes d'un manque à gagner estimé à 211 millions d'euros, ce qui se traduit concrètement par une réduction de moyens pour les producteurs et les créateurs de contenus audiovisuels.

En 2019, le manque à gagner lié au piratage équivaut à presque 47 saisons du « Bureau des Légendes » ou 515 fois le budget du film « Les Misérables »



En 2019, le manque à gagner économique de la filière audiovisuelle équivaut à presque 47 saisons de la série « *Bureau des Légendes* » ou à 515 fois le budget du film « *Les Misérables* », qui font partie des plus grands succès français à l'international ces dernières années⁴⁰. Le piratage prive la France d'un potentiel considérable de rayonnement culturel dans le monde.

Mise en péril du sport amateur et professionnel

Depuis 2000, la taxe dite « *Buffet* » prélève une part de 5 % des droits télévisés d'événements sportifs, au profit du sport amateur. Or, qu'il s'agisse de services illégaux de *live streaming* ou autres, le piratage engendre un manque à gagner pour les diffuseurs qui se répercute sur toute la chaîne de valeur du sport, les diffuseurs étant logiquement de moins en moins enclin à payer pour des événements dont ils savent qu'ils seront piratés.

Dans le cas du football, les pertes liées au piratage audiovisuel sont par exemple estimées entre 100 et 500 millions d'euros par an^{41, 42}. Comme le précise Aurore Bergé, députée LREM et rapporteure générale du projet de loi audiovisuel discuté début 2020 à l'Assemblée nationale, la réduction en valeur des droits télévisés a un impact sur la ligue professionnelle puis sur le football amateur, et enfin sur l'enfant « *qui va à son club le dimanche*⁴³ ». Le manque à gagner se traduit ainsi par une diminution des moyens des « *petits* » clubs qui sont pourtant les plus « *grands pourvoyeurs de futurs champions*⁴⁴ ».

³⁹ *Ibid*, p. 41.

⁴⁰ La dernière saison du *Bureau des Légendes* et *Les Misérables* ont respectivement eu un budget de 22 millions et de 2 millions d'euros.

⁴¹ Clément Martel, « Le football français veut éradiquer le streaming illégal des matchs », *Le Monde* [en ligne], 2 février 2021.

⁴² « Piratage des retransmissions sportives : « Est-ce que le système n'a pas généré sa fragilité, en étant trop cher et en allant pomper trop de fric ? » », *Public Sénat* [en ligne], 23 janvier 2019.

⁴³ Marc Rees « Interview d'Aurore Bergé : sans sanction, « on continuera à avoir un piratage massif » », *Next INpact* [en ligne], 10 octobre 2018.

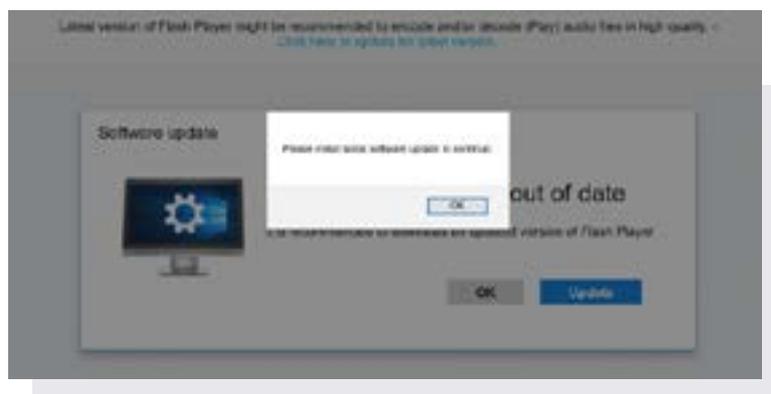
⁴⁴ « Covid-19 : déjà affaibli par le piratage, le football français au bord du gouffre », *360 Sport* [en ligne], 10 novembre 2019.

Du piratage audiovisuel au piratage informatique

De 79% à 97 % des sites pirates seraient infectés par des malwares pouvant infecter les machines (ordinateurs, smartphones...) des visiteurs

Par la popularité des contenus qu'ils proposent, certains sites illégaux de *streaming*, de *live streaming* et de téléchargement attirent de nombreux internautes et deviennent *de facto* des supports privilégiés pour les pirates informatiques, qui y voient des victimes potentielles. Le manque de ressources des administrateurs pour les sécuriser y favorise la diffusion de logiciels malveillants (*malwares*)⁴⁵ : de 79 % à 97 % des sites illicites seraient infectés^{46, 47}. En 2015, une étude américaine estimait que les chances d'infection par *malware* étaient 28 fois plus élevées sur un site pirate que sur un site *mainstream*⁴⁸.

Un clic sur une publicité abusive suffit parfois à faciliter une infiltration dans un terminal. La technique de la fausse alerte, sous la forme de fenêtre *pop-up*, consiste par exemple à faire croire à la cible en l'existence d'un problème technique, voire d'une mise à jour nécessaire sur son ordinateur. La victime se voit alors proposer le téléchargement d'un logiciel qui peut s'avérer être en réalité un *malware*⁴⁹.



DEMANDE INTRUSIVE DE TÉLÉCHARGEMENT D'UNE MISE À JOUR LOGICIELLE

Les pirates informatiques (aussi désignés « *attaquants* ») disposent d'une importante gamme d'outils pour infecter leurs cibles, dont les chevaux de Troie (logiciels fiables en apparence, mais abritant un code malveillant) et les *adwares* (affichage de publicités intempestives). Ces pirates peuvent aussi diffuser un logiciel de *cryptomining* qui utilise la puissance de l'ordinateur de la victime pour générer de la cryptomonnaie. Leurs objectifs vont alors de l'endommagement (ralentissement, voire interruption) à la prise de contrôle total d'un système d'information (SI).

⁴⁵ Victor Poitevin, « Streaming illégal : gare au retour de bâton », *Stormshield* [en ligne], 2 mai 2019.

⁴⁶ « Connaître les risques associés à la consommation illicite », *Hadopi* [en ligne], consulté en Mars 2021.

⁴⁷ *Illegal Streaming and Cyber Security Risks*, Association of Internet Security Professionals, Automne 2014, p. 20.

⁴⁸ *Digital Bait*, Digital Citizens Alliance, RiskIQ, Décembre 2015, p. 6.

⁴⁹ *Op. cit.* Stormshield, 2 mai 2019.

Des attaquants peuvent aussi modifier le code qu'une régie publicitaire transmet à ses clients de sorte à afficher des publicités malveillantes sur leurs sites Internet⁵⁰ (*malvertising*). Les visiteurs sont ainsi infectés via la publicité. Lorsqu'un individu consulte une page Web, son ordinateur se connecte en effet de manière imperceptible à plusieurs adresses, prévues entre autres par le code de la régie, pour accélérer par exemple l'ouverture des fenêtres *pop-up*. Les noms de domaine cachés peuvent favoriser les infiltrations malveillantes sur son SI⁵¹ ou le renvoyer contre son gré sur des sites spécifiques.

Les pirates informatiques recourent en parallèle à d'autres modes opératoires pour agir. Certains sites illicites requérant l'authentification de leurs utilisateurs pour l'accès aux contenus peuvent faire l'objet, en amont, d'une compromission permettant aux attaquants de collecter les informations personnelles et/ou les numéros de carte de crédit renseignés lors de l'inscription à la plateforme⁵². Les données bancaires peuvent alors être utilisées à des fins de dépenses frauduleuses, et ce par le biais parfois d'une revente sur le *darknet*. Les coordonnées de la victime peuvent aussi être réutilisées pour lui envoyer régulièrement des courriers indésirables (*spams*).

D'autres sites, pour lancer le visionnage de leurs contenus, imposent l'installation d'une application gratuite de *streaming* qui peut elle aussi être piégée⁵³. Les lecteurs multimédias utilisés pour le *streaming* ou le *live streaming* constituent par ailleurs une porte d'entrée pour des actes malveillants. Les pirates informatiques, outre l'exploitation des vulnérabilités de ces lecteurs, peuvent y insérer des sous-titres infectés comme ce fut le cas avec VLC, Popcorn Time et Kodi en 2018⁵⁴. Les répertoires de sous-titres étant généralement considérés comme sans danger, les cybercriminels misent sur le sentiment de confiance des utilisateurs pour y glisser des fichiers malveillants, qui s'activent dès qu'un consommateur illicite choisit une langue spécifique.



UNE INSCRIPTION EST OBLIGATOIRE POUR DÉMARRER LA LECTURE DU CONTENU

⁵⁰ Gilbert Kallenborn, « Une régie pub de La Poste a été utilisée pour pirater 277 sites d'e-commerce », *01net* [en ligne], 18 janvier 2019.

⁵¹ Rahul Kashyap, « Why Malvertising Is Cybercriminals' Latest Sweet Spot », *Wired* [en ligne], Novembre 2014.

⁵² Alvaro Puig, « Malware from illegal video streaming apps: What to know », *FTC* [en ligne], 2 mai 2019.

⁵³ *Op. cit.* Stormshield, 2 mai 2019.

⁵⁴ « Hacked in Translation – from Subtitles to Complete Takeover », *Check Point* [en ligne], 23 mai 2017.

Quant au téléchargement illégal, les séries télévisées sont fréquemment utilisées pour dissimuler des *malwares*. Par exemple, près d'une dizaine de milliers de logiciels malveillants ont été intégrés dans des fichiers se faisant passer pour des épisodes de *Game of Thrones* pour attaquer des internautes⁵⁵.

Un contenu piraté expose le consommateur à des risques d'usurpation d'identité, de vol de données personnelles et bancaires, de dommages contre ses équipements, ainsi qu'à l'accès à des publicités et des arnaques contre son gré. Dans des cas plus graves, les assaillants peuvent utiliser l'ordinateur de leur victime pour conduire des cyberattaques contre des tiers, voire des autorités étatiques.

**La majorité des
malwares sur les sites
illicites de streaming
et de téléchargement
sont issues des
bannières publicitaires.**

**Général de brigade
Éric FREYSSINET**

*Chef du pôle national de la lutte contre les
cybermenaces de la Gendarmerie nationale*

Impact psychologique

Internet est un espace public dans lequel les plus jeunes ne sont pas systématiquement accompagnés. Sa dimension immatérielle explique qu'il semble aujourd'hui plus facile de les y laisser seuls que dans un espace physique. Pour autant, si l'espace numérique offre nombre d'opportunités en termes d'éducation et de transmission de savoir, il est aussi porteur de menaces. Le *streaming* étant devenu un loisir particulièrement plébiscité des plus jeunes, la probabilité qu'ils soient exposés involontairement à des contenus publicitaires est dès lors très importante.

Or les publicités affectent le rapport au réel des enfants. Seuls devant l'écran, qu'il s'agisse d'une tablette ou d'un ordinateur, ils ne peuvent compter sur le filtre de l'esprit critique d'un adulte pour interpréter les contenus auxquels ils sont exposés et deviennent alors plus vulnérables à la manipulation⁵⁶.

Lorsqu'ils consultent un site pirate, les enfants sont exposés à des publicités inappropriées et intrusives, même s'ils y recherchent un contenu *a priori* inoffensif tel qu'un dessin animé. Il peut s'agir d'annonces pour des jeux érotiques, des sites de rencontre pour adultes et parfois même des sites pornographiques. En 2016, l'association Ennoccence⁵⁷ indiquait ainsi que 23 % des enfants ayant consulté un site pirate avaient été exposés à des images à caractère pornographique⁵⁸. Ces chiffres pourraient avoir augmenté depuis, tant la consommation illicite de contenus audiovisuels s'est accrue ces dernières années.

⁵⁵ « Les séries télévisées les plus célèbres peuvent être dangereuses », *Kaspersky Daily* [en ligne], 3 avril 2019.

⁵⁶ Delphine Bancaud, « Quelle est l'influence de la publicité sur les enfants ? », *20 Minutes* [en ligne], 18 octobre 2015.

⁵⁷ L'association **Ennoccence** s'est fixée comme mission de protéger les enfants contre les risques d'exposition non voulue à des contenus pornographiques en ligne.

⁵⁸ Ennoccence, *L'exposition des enfants aux images à caractère violent ou pornographique sur Internet*, 2016, p. 11.

L'association précise par ailleurs que la première exposition d'un enfant à de la pornographie aurait lieu, en moyenne, à l'âge de 11 ans et souvent via des fenêtres intrusives présentes sur des sites de *streaming* illégal⁵⁹. Une première exposition qui arrive par ailleurs de plus en plus tôt selon le ministère des Solidarités et de la Santé⁶⁰.

Selon une enquête réalisée au profit de *20 Minutes* en 2018, 62 % des jeunes adultes sondés ont déclaré avoir été exposés à de la pornographie pour la première fois avant l'âge de 15 ans, dont 31 % d'entre eux avant 12 ans⁶¹.

Si ces chiffres varient sensiblement d'un cas à l'autre, ils soulignent toutefois une réelle précocité et il demeure difficile pour un enfant de faire preuve de discernement face à ce type de contenus et d'en prendre de la distance. Celui-ci est nécessairement impacté par ces images et pourrait dans certains cas être tenté d'en voir davantage⁶² : 36 % des sondés dans l'étude mentionnée estiment ainsi que la pornographie a influencé leur représentation de la sexualité.

En juin 2018, le Collège national des gynécologues et obstétriciens français a interpellé les autorités publiques sur les dangers liés à l'exposition des enfants et des adolescents à la pornographie⁶³. Même si beaucoup prennent de la distance vis-à-vis de ces contenus, d'autres « *mal dans leur peau* », n'ayant pas le recul nécessaire, peuvent « *s'en emparer* ». Ces représentations erronées deviennent susceptibles d'affecter la construction de leur sexualité et de leur appréciation de la notion du consentement.

**En moyenne,
la première
exposition
d'un enfant à la
pornographie
s'effectue à
11 ans, souvent
en raison des
publicités sur
les sites pirates**



EXEMPLE DE PUBLICITÉ INTRUSIVE À CARACTÈRE PORNOGRAPHIQUE

⁵⁹ Baptiste Blanchard, « Une banalisation de la pornographie s'est imposée aux jeunes », *JDD* [en ligne], 28 février 2018.

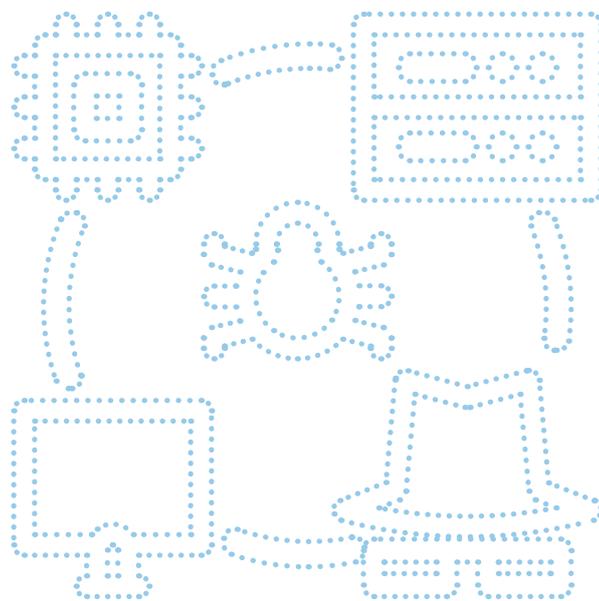
⁶⁰ « Exposition des jeunes à la pornographie », *Ministère des Solidarités et de la Santé* [en ligne], 8 février 2021.

⁶¹ Étude OpinionWay pour *20 Minutes* (2018) [en ligne].

⁶² Paulina Benavente, « Pornographie sur le web », *BFM* [en ligne], 20 mars 2017.

⁶³ Gaëlle Dupont, « L'appel solennel des professionnels de santé contre les dangers de la pornographie chez les jeunes », *Le Monde* [en ligne], 15 juin 2018.

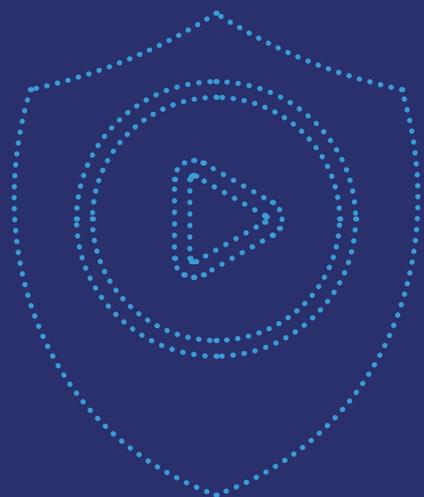
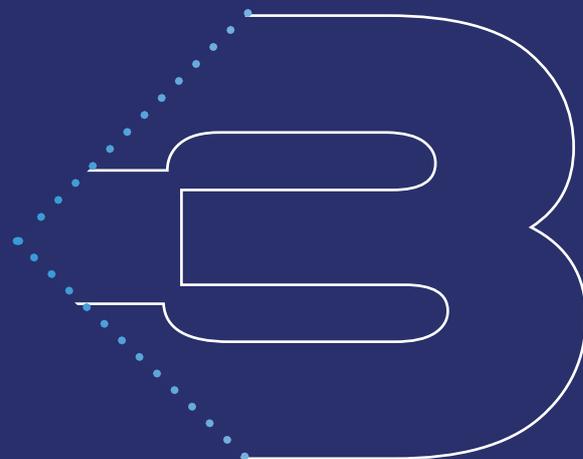
Les parents ne sont néanmoins pas toujours au courant de l'exposition de leurs enfants à de tels contenus et des potentielles conséquences⁶⁴. En novembre 2019, le Président de la République a annoncé faire de la lutte contre l'exposition des enfants à la pornographie un objectif national. Le gouvernement a ainsi mis en œuvre une série de mesures visant à responsabiliser et à sanctionner les sites à caractère pornographique qui permettent aux mineurs d'accéder à leurs contenus⁶⁵. Adoptée en juillet 2020, la loi visant à protéger les victimes de violences conjugales impose depuis à ces sites de mettre en place un système de vérification de l'âge. Pour autant, cette mesure ne prend pas en compte la question des publicités inappropriées et explicites, qui apparaissent souvent de manière intrusive lors d'une visite de site pirate.

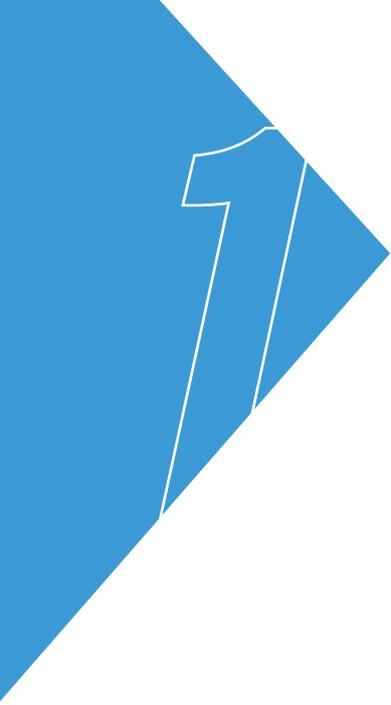


⁶⁴ « Exposition des jeunes à la pornographie », *Ministère des Solidarités et de la Santé* [en ligne], 8 février 2021.

⁶⁵ « Discours du Président Emmanuel Macron pour le 30ème anniversaire de la Convention internationale des droits de l'enfant », *Élysée* [en ligne], 20 novembre 2019.

**LA NÉCESSITÉ
D'UNE ACTION
RÉGALIENNE,
SYSTÉMIQUE ET
TRANSVERSALE**





LE PIRATAGE AUDIOVISUEL : FACTEUR DE DÉSTABILISATION DE L'ORDRE PUBLIC NUMÉRIQUE

Commissaire européen au marché intérieur, Thierry Breton a déclaré en octobre 2020 que l'espace numérique européen était « *dans bien des cas* » une « *zone de non-droit*⁶⁶ ». S'exprimant sur le projet de *Digital Services Act* (DSA), qui vise justement à réguler cet espace, il a précisé que l'esprit de ce texte était que « *tout ce qui est interdit dans l'espace public le sera aussi dans l'espace online* ».

Thierry Breton a rappelé à cette occasion que la régulation de l'espace numérique impliquait le retrait de tous les contenus identifiés comme « *illégaux* ». Parmi eux, il cite les contenus liés à la pédopornographie, l'antisémitisme, la vente de drogues, la désinformation et la haine en ligne, ainsi que la contrefaçon.

Si ces propos réaffirment le caractère illicite et transversal de la contrefaçon, ils mettent aussi en exergue le continuum entre les espaces public et numérique : le droit doit s'appliquer de la même manière aux deux.

L'une des formes les plus courantes de la contrefaçon dans l'espace numérique est celle du piratage audiovisuel. Celui qui s'y adonne cherche à s'approprier le fruit des investissements de titulaires d'un droit de propriété intellectuelle, ainsi que le bénéfice de leurs notoriétés. Si le basculement de cette pratique sur Internet a été favorisé par le développement des technologies de partage de contenus (P2P, *streaming*, DDL, IPTV, etc.), l'ère numérique a eu pour effet d'élargir la nature des préjudices liés à ce piratage, qui sont désormais loin de se limiter à l'atteinte au droit d'auteur.

Le piratage audiovisuel est aujourd'hui un vecteur de menaces diverses dans l'espace numérique. La délinquance traditionnelle s'est déplacée, renouvelée et développée sur Internet où elle s'exerce à l'échelle planétaire⁶⁷. Des réseaux organisés se sont emparés du piratage pour en faire une source de revenus complémentaires, voire de financement à leurs activités *offline* (trafic de drogues, proxénétisme, etc.). La capacité d'entreprendre, facilitée par la révolution numérique, leur permet de devenir des fournisseurs de services illicites et de bénéficier d'une large audience de demandeurs.

⁶⁶ Virginie Malingre, « Thierry Breton : « Dans bien des cas, l'espace numérique est une zone de non-droit » », *Le Monde* [en ligne], 22 octobre 2020.

⁶⁷ Jean-Marc Sauvé, *La protection des droits fondamentaux à l'ère du numérique (Discours)*, 12 décembre 2017.

Préservant leur anonymat par des pratiques courantes de la cybercriminalité (recours à des prête-noms, structures *offshore*, fausses identités, etc.), ils sont difficilement identifiables pour les ayants droit, les forces de l'ordre et les autorités judiciaires.

Toute la chaîne de valeur des créateurs de contenus audiovisuels, ainsi que celle du sport, se retrouvent alors victimes d'une concurrence déloyale et finalement peu régulée. Les outils juridiques à leur disposition ne permettent plus de contrer dans de brefs délais la sophistication croissante du piratage de leurs œuvres. Pour l'État, la poursuite de ces pratiques continue de remettre en cause sa souveraineté économique, par les importantes pertes fiscales engendrées (400 millions d'euros en 2019).

Renforcé dans l'espace numérique, l'exercice de la liberté d'expression accroît les risques de diffusion de contenus illicites, dont ceux de contrefaçon. Les publicités sans filtres qui les accompagnent peuvent affecter les personnes les plus vulnérables, en particulier les enfants. Qu'il s'agisse d'annonces pour des jeux d'argent ou à caractère pornographique, ces expositions de plus en plus précoces peuvent avoir un impact négatif sur leur santé et leur développement personnel. Si ces infractions sont sévèrement punies par la loi, elles n'en demeurent pas moins récurrentes sur les sites pirates.

Enfin, le piratage audiovisuel porte aussi atteinte au droit au respect de la vie privée, ainsi qu'à la protection des données personnelles. L'insuffisante sécurité des plateformes illégales, dont en premier lieu celles de *streaming*, est source pour les utilisateurs de risques de vol de données (personnelles, voire bancaires) et d'intrusions informatiques par des individus malveillants. Bien que l'accès frauduleux à des systèmes d'information et l'usurpation d'identité de tiers soient sanctionnés par le Code pénal, l'espace numérique offre aux pirates informatiques la possibilité d'agir furtivement.

Le piratage audiovisuel est une portée d'entrée à toute sorte d'actions susceptibles d'affecter l'ordre public et l'exercice des droits fondamentaux dans l'espace numérique



UN CADRE LÉGISLATIF À RÉFORMER POUR CONTRENER LE CARACTÈRE PROTÉIFORME DU PIRATAGE

Des mesures juridiques en décalage avec les modes de consommation



LES LIMITES DE LA RÉPONSE GRADUÉE À VISÉE PÉDAGOGIQUE

La loi Hadopi est l'un des principaux outils de la lutte contre le piratage en ligne de biens culturels. Entrées en vigueur en 2009, ces dispositions ont conduit à la création de la Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet (Hadopi), rattachée au ministère de la Culture, en 2011. Cette dernière, outre encourager le développement des offres légales, vise à sensibiliser les internautes sur les conséquences du piratage et à sanctionner ceux qui le pratiquent.

En matière de sanctions, l'Hadopi s'appuie sur la procédure de la « réponse graduée⁶⁸ », qui s'articule autour de mesures restrictives prévues par le Code de la propriété intellectuelle⁶⁹ (CPI). Celle-ci s'intéresse davantage à sanctionner les consommateurs plutôt que les pirates qui sont de plus en plus professionnels et criminels :

- Un internaute identifié pour infraction au droit d'auteur reçoit un premier courriel d'avertissement, le plus souvent sur l'adresse connue par son fournisseur d'accès à Internet (FAI);
- en cas de récidive dans les six mois, il reçoit un second avertissement sous la forme d'un courriel doublé d'une lettre recommandée. En vertu de cette dernière, l'internaute est dans l'obligation de mettre en place « un moyen de sécurisation » de son accès à Internet pour éviter tout piratage;
- après une seconde récidive dans les douze mois suivant l'envoi du courrier recommandé, l'internaute fait preuve de « négligence caractérisée ». L'Hadopi peut alors saisir le procureur de la République, à des fins de poursuites pénales et d'une éventuelle amende pouvant s'élever à 1 500 euros.

⁶⁸ « La réponse graduée », *Hadopi [en ligne]*, consulté en Mars 2021.

⁶⁹ Articles L.331-24, L.331-25 et R.335-5 du Code de la propriété intellectuelle.

Dans les faits, la réponse graduée sanctionne davantage la récidive de l'utilisateur, considérée comme une « *négligence caractérisée* », que le piratage en lui-même (article L.336-3 du CPI), témoignant alors de sa visée pédagogique. En 2019, la moitié des personnes ayant reçu un courrier recommandé ont en effet déclaré avoir opté en substitution pour une offre légale (contre 42 % en 2017).

Pour autant, le cumul des amendes prononcées entre 2011 et 2019 ne s'élève qu'à 87 000 euros⁷⁰. Bien que l'Hadopi n'ait pas vocation à être rentable, mais à faire « *changer les comportements*⁷¹ », ce montant traduit en réalité un nombre important d'avertissements pour peu de sanctions. Il doit être appréhendé à la lumière, pour la seule année 2019, du budget de la haute autorité qui a été de 9,45 millions d'euros⁷², ainsi que du manque à gagner de la filière audiovisuelle de 1,03 milliard d'euros.

Ce bilan attire l'attention sur les limites de l'Hadopi qui s'expliquent, sur le plan juridique, par un champ d'action lui-même restreint. Cette autorité découle d'une loi qui n'est pas technologiquement neutre la cantonnant à la lutte contre le *peer-to-peer* (P2P). Elle ne peut ainsi traiter par exemple ni le téléchargement direct (DDL) ni le *streaming*, qui sont les modes de piratage les plus utilisés aujourd'hui.

Combinée à la promotion de l'offre légale de contenus audiovisuels, l'approche pédagogique de la réponse graduée de l'Hadopi a participé à la réduction un temps des pratiques illicites. Pour autant, la diversification et la sophistication du piratage sont aujourd'hui telles que cette autorité ne peut plus, si elle veut être efficace, se limiter à la lutte contre le P2P. Le projet de fusion avec le CSA constituerait alors l'occasion de redonner une nouvelle impulsion à l'Hadopi et d'en augmenter la portée des activités.

Le projet de réforme de l'Hadopi ne peut faire l'économie du déplacement d'organisations criminelles vers le piratage : le dispositif de lutte doit sanctionner ces contrefacteurs « spécialisés » dans l'audiovisuel, et non les consommateurs de contenus piratés.

⁷⁰ Hadopi, *Rapport d'activité*, 2019, p. 42.

⁷¹ Guillaume Fournier, « Piratage informatique : Hadopi attend toujours des armes pour lutter contre le streaming », *Actu* [en ligne], 6 août 2020.

⁷² *Ibid*, p. 92.



DES PROCÉDURES DE RETRAIT ET DE BLOCAGE DE CONTENUS ENCORE TROP LONGUES

Face aux autres formes de piratage (*streaming*, DDL et IPTV), les ayants droit s'efforcent d'impliquer directement les intermédiaires techniques pour obtenir le retrait voire le blocage de contenus mis à disposition illégalement, plutôt que de chercher à sanctionner leurs consommateurs. Cette voie leur offre plus de réactivité que la plainte pour délit de contrefaçon prévue par l'article R331-42 du CPI.

Les moyens pour exiger le retrait et le blocage de contenus contrefaisants sont néanmoins limités. Selon l'article 6 (I-2) de la loi pour la confiance dans l'économie numérique (LCEN), les hébergeurs ne sont pas responsables des contenus illicites stockés sur leurs serveurs, tant qu'ils n'en sont pas informés.

Transposition de la directive européenne « e-commerce », la LCEN a été adoptée en 2004 pour encadrer le rôle des intermédiaires techniques, dont les hébergeurs, à un moment où ces derniers ne comptaient que quelques milliers d'utilisateurs, contre des millions aujourd'hui. Les législateurs n'ont pu mesurer ni la dimension que ces services allaient prendre ni leur détournement à des fins de piratage.

Le blocage systématique par les hébergeurs de tout téléversement de contenus ayant déjà été notifié demeure la meilleure pratique mais suppose une révision législative

› Procédure de notification et de retrait de contenus illicites

Les ayants droit peuvent appliquer la procédure prévue par l'art. 6 (I-5) de la LCEN pour notifier à un hébergeur l'existence sur ses serveurs d'un contenu portant atteinte à ses droits. Dès que l'hébergeur en a connaissance, il est tenu d'agir « *promptement* », pour le retirer ou le rendre inaccessible.

Cette procédure a d'abord donné lieu à une interprétation juridique selon laquelle un hébergeur devait empêcher tout autre téléversement par ses utilisateurs de contenus ayant déjà fait l'objet d'une notification, et donc les bloquer (*notice and stay down*). Si cette interprétation a donné lieu à l'une des pratiques les plus efficaces pour contrer le piratage (*stay down*), celle-ci a néanmoins été invalidée par la Cour de cassation en 2011⁷³, estimant qu'elle contrevenait à la LCEN, qui interdit aux hébergeurs d'effectuer une surveillance générale des contenus stockés sur leurs serveurs. Cette décision judiciaire explique notamment pourquoi la lutte contre le piratage a surtout lieu *a posteriori* sous la forme de sanction⁷⁴.

Si cette procédure fonctionne pour les sites dont les hébergeurs relèvent d'États membres de l'Union européenne, rien ne garantit qu'elle puisse aboutir dans d'autres pays. De plus, les délais de réactivité avant le retrait de contenus notifiés peuvent être conséquents. Caroline Guenneteau, Directrice juridique de BeIN Sports France, s'exprimant sur ce dispositif, a relevé un délai de deux à trois heures entre la notification et le retrait du contenu dans les cas où l'hébergeur tient compte de la notification⁷⁵. Appliquée au *live streaming* sportif, la procédure de *notice and take down* ne permet donc pas d'interrompre la retransmission d'une rencontre sportive dont la durée est moindre que le temps de réaction des intermédiaires.

⁷³ Cour de cassation, *Première chambre civile, Arrêt n°165*, 17 février 2011 (09-67.896).

⁷⁴ « La lutte contre le piratage aujourd'hui et demain », *NPA Conseil [en ligne]*, consulté en mars 2021.

⁷⁵ Kéritch Cayau, « Caroline Guenneteau (beIN SPORTS) : « Les opérateurs de plateforme numérique doivent prendre leur responsabilité sur la diffusion de contenus illégaux » », *Rude Baguette [en ligne]*, 17 avril 2019.

› Blocage DNS : une mobilisation des FAI sur ordonnance du juge

Si l'hébergeur ne tient pas compte de la notification, un ayant droit peut obtenir sur ordonnance du juge, conformément à l'article L.336-2 du CPI, le concours des moteurs de recherche pour déréférencer le contenu, ou des fournisseurs d'accès à Internet (FAI) pour bloquer l'accès au site qui le diffuse⁷⁶. Les ayants droit peuvent également recourir à l'article 6 (I-8) de la LCEN pour ces mêmes finalités. Dans les deux cas, cette voie n'est efficace que si la mesure demandée aux intermédiaires techniques est proportionnée au dommage, ce qui est le cas des sites entièrement dédiés à la contrefaçon.

Dans ce cadre, les FAI effectuent un « *blocage DNS* ». Cette technique consiste à modifier le serveur DNS qu'ils mettent à la disposition de leurs clients pour que ces derniers ne puissent plus accéder aux adresses IP de sites spécifiques, en l'occurrence ceux portant atteinte au droit d'auteur.

Plusieurs technologies et méthodes permettent néanmoins de rendre caducs ces blocages :

- Les VPN, qui permettent aux utilisateurs de masquer leur adresse IP et de changer leur géolocalisation (cf. « *VPN* » dans Annexe 3) ;
- le protocole « DNS over HTTPS » (DoH), qui chiffre les requêtes DNS et s'intègre de plus en plus dans les navigateurs Web ;
- les serveurs DNS alternatifs. Les internautes peuvent recourir à d'autres serveurs DNS que ceux fournis par leurs FAI et ainsi accéder au site bloqué. Ces serveurs alternatifs, appelés « *résolveurs DNS ouverts* », sont facilement accessibles via Google Public DNS, Cisco OpenDNS, etc. ;
- les sites « *miroirs* ». L'administrateur d'un site visé par un blocage DNS peut en créer une copie en utilisant un nouveau nom de domaine, voire en n'en modifiant que l'extension pour ainsi conserver sa « *marque* ». Par exemple, le nom de domaine « *zone-telechargement.com* » a plusieurs fois été modifié : « *zone-telechargement.ws* », « *zone-annuaire.com* »...

Un consommateur de contenus illicites peut ainsi facilement contourner le blocage DNS d'un site pirate. Pour que ce type de mesures techniques soit efficace, l'ordonnance du juge devrait s'appliquer à tous les DNS existants, ce qui nécessiterait la réglementation des DNS alternatifs proposés par des acteurs privés.

Le court délai de réaction à une mise à disposition illicite d'un contenu doit être au cœur de la lutte contre le piratage audiovisuel. Au regard de cet enjeu, les procédures de notification et de retrait de contenu, ainsi que d'assignation des FAI, ne sont désormais plus suffisantes. Elles requièrent trop de temps et de nombreuses techniques de contournement existent.

⁷⁶ Depuis un décret du 8 juillet 2013, l'accès à Internet ne peut plus être coupé.

Des pistes de réformes encourageantes, mais encore insuffisantes

Le projet en l'état de Digital Services Act ne prend pas suffisamment en compte le rôle des hébergeurs dans le piratage

Proposé par la Commission européenne en décembre 2020, le projet de *Digital Services Act* (DSA) révisé la directive e-commerce dont découle la LCEN (cf. p. 34). Ce texte introduit des dispositions dites « *Know your business customer* » (KYBC) visant à lutter contre la contrefaçon sur Internet. Dans ce cadre, les seules plateformes de marché en ligne seront obligées de vérifier l'identité de leurs utilisateurs afin de mieux tracer ceux proposant des biens contrefaits, en plus d'intégrer un dispositif *ad hoc* de signalements. Si ces dispositions « KYBC » présentent un grand intérêt pour faire cesser l'anonymat de certains cybercriminels, elles ne s'appliquent en l'état pas aux hébergeurs de contenus. L'intégration de ces derniers dans le périmètre de ces mesures bénéficierait pourtant grandement à la lutte antipiratage.

En France plus spécifiquement, le gouvernement a initié en décembre 2019 le projet de loi relatif à la « *communication audiovisuelle et à la souveraineté culturelle à l'ère numérique* », amendé par la Commission des affaires culturelles de l'Assemblée nationale en mars 2020. Ses articles 22 et 23 prévoyaient des mécanismes innovants dans la protection en ligne des biens culturels, aussi bien en termes de prérogatives que de moyens. La crise de Covid-19 a néanmoins conduit à un report des échanges parlementaires relatifs à l'article 22 et aux intentions d'évolution de l'Hadopi. Ceux-ci ont été relancés à l'occasion d'un nouveau projet de loi dont la discussion a commencé au Parlement en mai 2021 relatif à « *la protection de l'accès du public aux œuvres culturelles à l'ère numérique* ».



UNE MEILLEURE RÉPARTITION DES RÔLES ENTRE L'AUTORITÉ ADMINISTRATIVE ET LE JUGE

Le projet de loi à venir reprend une disposition du texte avorté et prévoit de fusionner l'Hadopi et le Conseil supérieur de l'audiovisuel (CSA) au sein d'une Autorité de régulation de la communication audiovisuelle et numérique (ARCOM). En cas d'adoption de ce texte, l'ARCOM sera chargée de protéger l'ensemble des œuvres en ligne auxquelles sont attachées un droit d'auteur, un droit voisin ou des droits d'exploitation audiovisuelle. Ses missions consisteront à encourager le développement de l'offre légale, ainsi qu'à réguler et à suivre l'évolution des mesures techniques de protection et d'identification des œuvres. Elle devra également sensibiliser les utilisateurs, notamment les plus jeunes, sur les risques et les conséquences du piratage.

L'ARCOM caractériserait en amont les atteintes aux droits. Plus précisément, des agents assermentés identifieraient les sites et les serveurs reconnus comme contrefaisants, de manière « *grave et répétée* », dans le cadre d'une liste publique (« *liste noire* »). Ce projet de loi, contrairement à la loi Hadopi, ne cible pas un seul mode de piratage en particulier et étend *de facto* le champ d'actions de l'ARCOM à tous ceux existants. Cette liste accélérerait alors les procédures judiciaires. Sur sa base, les créateurs de contenus et leurs ayants droit pourront plus facilement saisir le juge, sans avoir à rassembler de preuves au préalable. En effet, l'anonymat des pirates est aujourd'hui tel qu'il est très difficile pour les ayants droit de collecter des preuves et d'avoir ainsi « *l'accroche* » nécessaire pour initier une procédure pénale.

L'idée de ce type de liste n'est pas nouvelle⁷⁷. Par son établissement, les autorités publiques misent sur les deux principes du « *name and shame* », qui vise à rendre publics les noms de sites et serveurs illicites et à tarir leur offre en jouant sur l'effet de réputation, et du « *follow the money* », qui oblige les régies publicitaires et les intermédiaires de paiement liés à un service inscrit sur la liste noire à communiquer sur l'existence de leurs relations commerciales avec ce dernier. Cette méthode consiste à faire la transparence sur les flux financiers pour renforcer le devoir de vigilance des annonceurs et les dissuader de financer des sites illicites⁷⁸.

L'ARCOM veillerait à ce que la décision prise par le juge judiciaire de bloquer et de déréférencier un site ou un serveur illicite s'applique à tous les sites miroirs qui reprennent en totalité ou en partie le contenu du service initialement ciblé. Les intermédiaires techniques tels que les FAI, les moteurs de recherche, les hébergeurs et les services de navigation pourront alors être impliqués.

Par ses approches « *name and shame* » et « *follow the money* », la problématique centrale de la monétisation des contenus illicites est enfin considérée. Les dispositions prévoient de plus une meilleure optimisation des procédures judiciaires, en favorisant à la fois les saisines du juge par les ayants droit et l'exécution des décisions du juge par une autorité administrative en cas de reprise du contenu visé par des sites de contournement.

Néanmoins, si ce texte propose des avancées, en s'intéressant davantage aux pirates qu'aux consommateurs, il ne prend pas en compte ni la dimension criminelle, ni les réseaux organisés à l'origine du piratage. Pour être efficace sur le long terme, la mission des agents assermentés, en charge de caractériser les atteintes aux droits, doit être complétée par des services d'enquête en mesure d'identifier « à qui profite vraiment le crime » afin de mieux le faire cesser.



UN DISPOSITIF INNOVANT ET ADAPTÉ AUX SPÉCIFICITÉS DU LIVE STREAMING

L'article 23 du projet de loi avorté relatif à la « *communication audiovisuelle et à la souveraineté culturelle à l'ère numérique* » a de son côté été réintroduit en tant qu'article 10 de la proposition de loi visant à « *démocratiser le sport en France* », en cours d'examen par l'Assemblée nationale depuis mars 2021, sur des bases par ailleurs très similaires à celles que l'on retrouve également à l'article 3 du projet de loi relatif à « *la protection de l'accès du public aux œuvres culturelles à l'ère numérique* ».

Les ayants droit et les diffuseurs pourront saisir le président du tribunal judiciaire pour obtenir une ordonnance rendant possible « *des mesures de blocage, de retrait ou de déréférencement* » d'un site ou d'un serveur diffusant illégalement une compétition ou une manifestation sportive. À cet égard, le projet de loi offre un caractère préventif et une plus longue validité à la décision du juge, puisqu'il permet sa mise en œuvre « *pour chacune des journées figurant au calendrier officiel de la compétition ou manifestation sportive, dans la limite d'une durée de douze mois [au lieu de deux mois aujourd'hui]* ». En d'autres termes, une décision peut être appliquée en amont d'une saison sportive et la couvrir dans sa totalité.

La lutte contre le piratage audiovisuel doit être plurielle et puiser dans une « boîte à outils » : elle demande des dispositifs souples de type name and shame, follow the money, mais aussi, évidemment, des mesures de droit dur rapides et efficaces.

Alexandra BENSAMOUN
Professeure de droit à l'Université Paris-Saclay

⁷⁷ Marius François, « Le gouvernement veut bloquer l'accès aux sites de streaming illégal », *Le Figaro* [en ligne], 19 avril 2018.

⁷⁸ *Compte rendu n°42*, Commission des affaires économiques, Assemblée nationale, 25 février 2020.

La proposition de loi, comme d'ailleurs le nouveau projet de loi relatif à l'audiovisuel, donne aux ordonnances judiciaires un caractère dit « *dynamique* ». Elles s'appliqueront également, sans avoir à repasser par une autre procédure judiciaire, aux sites et aux serveurs illicites « *non encore identifiés* » au moment de la décision initiale. Ces « *décisions-cadres* » visent à garantir l'efficacité des ordonnances face aux sites miroirs et autres moyens de contournement.

Dans ce cadre, l'Hadopi (puis potentiellement la future ARCOM) agirait en qualité de tiers de confiance entre les ayants droit et les diffuseurs d'un côté, ainsi que les intermédiaires techniques en mesure de contribuer à l'exécution de l'ordonnance du juge de l'autre. L'autorité s'efforcera d'assurer la « *réactivité nécessaire* » à la lutte contre les mises à disposition illicites de retransmissions sportives, tout en garantissant la « *sécurité juridique* » des mesures de blocage, de retrait ou de déréférencement effectuées *a posteriori* de la décision judiciaire⁷⁹.

La mise en place d'ordonnances à caractère préventif, de longue durée et dynamiques, permet de lutter contre le *live streaming* sportif. Celles-ci garantissent l'efficacité des décisions du juge contre les sites miroirs et permettent d'éviter sa saisine plusieurs fois par an pour la même compétition. Pour aller plus loin, ce dispositif pourrait être complété par la création d'un délit d'atteinte aux droits d'exploitation de l'article L333-1 du Code du sport.

Plusieurs technologies matures visent à lutter contre la violation du droit d'auteur existent déjà. Par leurs effets très ciblés, elles ne permettent néanmoins pas de contrer le piratage de masse :

- ***L'empreinte numérique (fingerprinting) est une technique de filtrage automatique qui consiste à prélever un échantillon d'un contenu lors de son téléversement sur une plateforme. Celui-ci est ensuite comparé à une base de données, puis bloqué s'il est identifié comme contrefaisant.***
- ***Le tatouage numérique (watermarking) imprime une marque unique à un contenu vidéo et permet d'en identifier l'origine, telle que le décodeur TV émetteur, afin de remonter jusqu'au pirate.***

⁷⁹ « Streaming illégal sportif : Constat/Comment lutter contre ce phénomène ? », *Table ronde Hadopi-LFP-ALPA*, Groupe d'études Économie du sport de l'Assemblée nationale, 10 février 2021, p. 6.

L'INDISPENSABLE CONCOURS D'UN RENFORCEMENT DE LA SPHÈRE POLICE-JUSTICE

Les ayants droit orientent aujourd'hui davantage leurs efforts dans la lutte contre le piratage de masse. La fermeture ces dernières années de sites d'envergure témoigne de l'implication croissante de l'action publique à cet égard. Les délais de neutralisation de sites illicites sont néanmoins relativement longs. La SACEM⁸⁰, soutenue par l'Association de lutte contre la piraterie audiovisuelle (ALPA), a par exemple déposé plainte en 2014 contre le site T411 dont les administrateurs n'ont été arrêtés qu'en 2017⁸¹. De la même façon, quasiment trois ans se sont écoulés pour le site zone-téléchargement⁸² (cf. p. 16)

En dépit de leur dimension transnationale, ces exemples attirent l'attention sur le rythme des procédures judiciaires en France. Du fait de sa composante numérique, le piratage audiovisuel fait aujourd'hui l'objet d'un traitement par la justice qui relève de la lutte contre la cybercriminalité. Les procédures s'inscrivent alors dans un contexte marqué par une centralisation des compétences territoriales, de montée en maturité de l'appareil judiciaire⁸³ et de services d'enquêtes qui gagneraient à être étoffés⁸⁴.

⁸⁰ Société des auteurs, compositeurs et éditeurs de musique.

⁸¹ « Angers. Fermeture du site de téléchargement illégal T411 : un Angevin interpellé », *Ouest France* [en ligne], 28 juin 2017.

⁸² « Toulouse. Zone Téléchargement : les deux administrateurs du site placés en détention », *La Dépêche* [en ligne], 1^{er} décembre 2016.

⁸³ Jacques Martinon, « Les défis du traitement judiciaire de la cybercriminalité », *Les risques et l'environnement numérique*, n°59, *INHESJ*, 2019, p. 1.

⁸⁴ Jacques Bigot, Sophie Joissans, « Cybercriminalité : un défi à relever aux niveaux national et européen », *Rapport d'information*, n°613, *Sénat*, 9 juillet 2020.





Une culture cyber à développer sur l'ensemble de la chaîne judiciaire

Les derniers procès médiatisés liés au piratage concerne en réalité des affaires anciennes

Deux types d'infractions cybercriminelles peuvent être distinguées : celles ayant pour objet un système de traitement automatisé de données (STAD) et celles ayant pour vecteur principal un STAD⁸⁵. Portant atteinte aux droits d'auteur par voie numérique, le piratage audiovisuel relève de la seconde catégorie.

La cybercriminalité est un contentieux complexe qui fait l'objet, depuis 2016, d'une spécialisation dans l'appareil judiciaire et d'une centralisation des dossiers les plus techniques en faveur du tribunal judiciaire de Paris. Celui-ci s'est en effet vu attribuer une compétence concurrente nationale, qui a été confiée à la section J3 «*Cybercriminalité*» de son parquet. Celle-ci compte trois magistrats, dédiés en priorité aux atteintes aux STAD et aux affaires à dimension internationale, tandis que les parquets locaux sont compétents pour le reste du contentieux dont les cas d'atteinte au droit d'auteur sur Internet.

Dans ce cadre, le traitement par les parquets de dossiers de piratage revêt une plus grande complexité au regard des enjeux de cybersécurité associés, auxquelles s'ajoutent d'autres problématiques, tant dans les domaines de la fiscalité (blanchiment et fraude) que de la culture. Concrètement, cette complexité se traduit par des délais plus conséquents d'enquête préliminaire, voire d'instruction des plaintes, pour des atteintes à la propriété intellectuelle. Depuis 2019, chaque parquet local se voit affecter un référent cyber, dans le cadre d'un réseau animé par le tribunal judiciaire de Paris, pour appréhender les difficultés techniques. Certains dossiers continuent néanmoins d'être transférés à des services de police spécialisés, tels que la brigade sur les fraudes aux technologies de l'information (BEFTI), pour solliciter une assistance et deviennent *de facto* chronophages. Or, pour être efficace, la lutte contre le piratage requiert une réaction rapide de l'autorité judiciaire.

En comparaison, la réactivité aux contenus haineux repose sur un dispositif plus adapté. En janvier 2021, le tribunal judiciaire de Paris s'est doté d'un pôle spécialisé contre la haine en ligne, surnommé «*parquet numérique*», pour traiter en temps réel toutes les formes de menaces et les apologies du terrorisme sur Internet. Ce pôle s'efforce d'être le pendant judiciaire⁸⁶ de PHAROS⁸⁷, plateforme de signalement de contenus illicites⁸⁸ (ceux piratés n'y sont pas pris en compte), avec laquelle il est en collaboration étroite et permanente. Il ne se limite ainsi pas au retrait rapide de contenus : il cherche aussi à identifier et à «*faire reculer le sentiment d'impunité*» des auteurs jusque là peu poursuivis en raison des délais de procédures⁸⁹. Alors qu'un simple signalement sur PHAROS n'engage pas de poursuite, sa combinaison avec la saisine du «*parquet numérique*» permet de lancer une enquête dans de plus brefs délais⁹⁰.

⁸⁵ *Op. cit.* Jacques Martinon, p. 1.

⁸⁶ Gabriel Thierry, «*Le nouveau pôle spécialisé contre la haine en ligne, une structure très attendue*», *Dalloz Actualité* [en ligne], 3 février 2021.

⁸⁷ Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements.

⁸⁸ Pédophilie, pédopornographie, expression du racisme, de l'antisémitisme et de la xénophobie, incitation à la haine raciale, ethnique et religieuse, terrorisme et apologie du terrorisme, escroquerie et arnaque financières.

⁸⁹ Sébastien Mastrandreas, «*Haine en ligne : le parquet de Paris se dote d'un pôle spécialisé*», *Les Échos* [en ligne], 25 novembre 2020.

⁹⁰ Julien Lausson, «*Ce que l'on sait sur le «*parquet numérique*» censé agir contre les messages haineux*», *Numerama* [en ligne], 2 novembre 2020.

PISTES DE RÉFLEXION POUVANT ACCÉLÉRER LES PROCÉDURES JUDICIAIRES (1/2)

- *Réformer les délais d'enquête et de procédure afin d'accélérer le traitement des atteintes aux droits de la propriété intellectuelle et des infractions connexes.*
- *Doter le « parquet numérique » d'une compétence concurrente nationale pour la poursuite des atteintes aux droits de la propriété intellectuelle et des infractions connexes.*
- *Créer un référent cyber de niveau « magistrat » dans chaque tribunal judiciaire, tant au siège qu'au parquet, afin d'orienter les affaires, communiquer avec les autres référents et mettre en œuvre les actions de coordination sous l'égide du « parquet numérique ».*

Comme les pirates de l'audiovisuel, les « professionnels » de la haine en ligne ont de plus en plus recours à des méthodes cybercriminelles pour rendre difficile voire impossible leur traçabilité⁹¹. Le parquet de Paris, dans la mesure où celui-ci dispose de la section J3 « Cybercriminalité », est particulièrement au fait de ces techniques. Il a par ailleurs su s'imposer en tant que correspondant privilégié de PHAROS⁹² pour identifier les auteurs d'infractions. Le choix d'y loger une compétence concurrente en matière de haine en ligne a alors été le plus naturel.

De la même façon, le traitement des affaires de piratage suppose une importante capacité d'appréciation. L'autorité judiciaire doit pouvoir distinguer la mise en ligne illicite de contenus qui relève de comportements isolés sans lendemain (« Robin des bois »), de celle s'associant à un signal faible de menace à l'ordre public (cybercriminels, crime organisé et terrorisme). Le tribunal judiciaire de Paris est à cet égard le plus disposé par ses compétences concurrentes nationales en matière de lutte contre la cybercriminalité (J3), la criminalité organisée de très grande complexité (JUNALCO) – qui se caractérise par l'internationalisation des réseaux et l'usage de technologies innovantes⁹³ –, et le terrorisme (PNAT). Son parquet, avisé des caractéristiques de tous ces acteurs, est le plus à même de croiser les indices et d'identifier les pirates.

De plus, si le tribunal judiciaire de Paris bénéficie sur le plan civil d'une expertise quant aux demandes de suppression de contenus, du fait de sa proximité avec PHAROS⁹⁴, il est aussi doté sur le plan pénal d'un haut niveau de qualification au regard de son traitement des contentieux de propriété intellectuelle.

⁹¹ « Haine en ligne. Le parquet de Paris va créer un pôle spécialisé », *Ouest France* [en ligne], 23 novembre 2020.

⁹² Ministère de la Justice, Circulaire relative à la lutte contre la haine en ligne, 24 novembre 2020, p. 3.

⁹³ Ministère de la Justice, Circulaire relative à la compétence nationale concurrente du TGI et de la cour d'assises de Paris dans la lutte contre la criminalité organisée de très grande complexité, 17 décembre 2019, p. 6.

⁹⁴ Ministère de la Justice, Circulaire relative à la lutte contre la haine en ligne, 24 novembre 2020, p. 3.

L'Hadopi a par ailleurs appelé à ce que la juridiction parisienne traite l'ensemble du contentieux relatif aux atteintes aux droits d'exploitation de manifestations ou de compétitions sportives au sens de l'article L.333-1 du Code du sport⁹⁵.

L'instruction de plaintes pour piratage peut atteindre jusqu'à 10 ans

Une spécialisation du tribunal judiciaire de Paris permettrait, en cas de compétence concurrente en matière d'atteintes à la propriété intellectuelle, d'apporter une réponse rapide et efficace sur l'ensemble du territoire⁹⁶. Celle-ci pourrait dès lors désengorger d'autres tribunaux, n'ayant pas toujours les capacités ni les moyens techniques d'apprécier ce type d'infractions, et ainsi éviter des délais d'instruction pouvant atteindre jusqu'à 10 ans. Pour autant, à l'image de la justice française, la juridiction parisienne est susceptible de se heurter à la difficulté d'appréhender les auteurs d'infractions, dès lors que ces derniers se situent sur le territoire d'États peu coopératifs⁹⁷. Il est ainsi indispensable de renforcer en complément la coopération judiciaire européenne et internationale.

PISTES DE RÉFLEXION POUVANT ACCÉLÉRER LES PROCÉDURES JUDICIAIRES (2/2)

- *Créer une compétence concurrente nationale du tribunal judiciaire de Paris pour la poursuite, l'instruction et le jugement des infractions en matière d'atteintes aux droits de la propriété intellectuelle et d'infractions connexes. Le procureur de la République, le pôle de l'instruction, le tribunal correctionnel déjà saisis d'une affaire, en vertu des articles 43, 52 et 382 du Code de Procédure pénale, pourraient être dessaisis au profit de la juridiction parisienne.*
- *Former de manière continue et approfondie tous les intervenants de la chaîne pénale (enquêteurs et magistrats du parquet et du siège), incluant des missions d'observations à l'étranger et des rencontres avec leurs homologues européens et internationaux.*

⁹⁵ « Streaming illégal sportif : Constat/Comment lutter contre ce phénomène ? », *Table ronde Hadopi-LFP-ALPA*, Groupe d'études Économie du sport de l'Assemblée nationale, 10 février 2021, p. 5.

⁹⁶ Gordon Choisel, « La nécessité d'un ministère public présent en ligne », *Sécurité globale*, n°15, 2018, p. 40.

⁹⁷ *Op. cit.* Jacques Bigot, Sophie Joissans.



Renforcer les moyens d'investigation à l'échelle nationale et internationale



Au niveau des services d'enquêtes, nous rencontrons une plus grande difficulté à faire traiter des dossiers liés à la contrefaçon sur Internet. Ce type de dossiers, souvent complexes, présentent des particularités juridiques et techniques qui ne peuvent pas toujours être traitées par les services de Police et de Gendarmerie. Il est regrettable que la France n'ait pas, comme dans d'autres pays européens, un service d'enquête spécialisé dédié à la lutte contre cette forme de délinquance.

Frédéric DELACROIX

Délégué général de l'ALPA

En 2017, le colonel Nicolas Duvinage, alors chef du Centre de lutte contre les criminalités numériques (C3N) de la Gendarmerie nationale, interrogé sur la fermeture par son service du site T411, indiquait que les dossiers liés au piratage audiovisuel constituaient des « variables d'ajustement [...] au second plan dans la période de terrorisme⁹⁸ ». En raison d'autres priorités sécuritaires, les forces de l'ordre ne peuvent pas toujours s'impliquer de manière proactive pour appréhender ce type d'infraction, qui n'est finalement traité que lorsqu'elles sont saisies à ce sujet.

Les publications relatives à la pédopornographie et au terrorisme cristallisent naturellement l'attention des autorités. Depuis 2015, ces contenus constitutifs de « grave abus » de la liberté d'expression peuvent déclencher une procédure accélérée de blocage des sites Internet qui les diffusent sur simple décision administrative, plutôt que sur décision d'une autorité judiciaire. De telles images sont en effet suffisamment objectives pour être identifiées directement comme telles. Les contenus audiovisuels portant atteinte aux droits de la propriété intellectuelle sont *a contrario* sujets à diverses interprétations. Le droit d'auteur prévoit en effet plusieurs exceptions à la diffusion légale (parodie, usage strictement familial, exception, musées, etc.). S'ils ne sont évidemment pas à placer sur le même plan, la procédure de lutte contre les contenus pédopornographiques et terroristes peut toutefois ouvrir des pistes de réflexion quant au développement d'outils de protection des contenus piratés.

Pour autant, l'autorité chargée de la procédure accélérée de blocage, l'Office central de lutte contre la cybercriminalité liée aux technologies de l'information et de la communication (OCLCTIC), souffre aussi d'un effectif limité au regard de ses nombreuses sollicitations. En 2019, l'Office comptait 28 enquêteurs pour traiter 228 545 signalements dans l'année. Un effectif jugé comme trop limité par une partie de la classe politique⁹⁹.

⁹⁸ Corentin Durand, « T411 : 7 millions d'euros par an, 6 interpellations, 3 ans d'enquête internationale », *Numerama* [en ligne], 27 juin 2017.

⁹⁹ Alexandre Rousset, « Haine en ligne : la plateforme de signalement Pharos en cinq questions », *Les Échos* [en ligne], 20 octobre 2020.

Par ses missions, la douane contribue fortement à la lutte contre la contrefaçon. Son action s'appuie en effet sur la Direction nationale du renseignement et des enquêtes douanières (DNRED), chargée de cibler les contrôles douaniers par une surveillance des sites et des plateformes de vente en ligne de biens contrefaits¹⁰⁰, et sur le Service national de douane judiciaire (SNDJ), responsable des enquêtes pour démanteler les filières. Sollicitée par un ayant droit, la douane peut engager une procédure de retenue d'une marchandise soupçonnée de porter atteinte à un droit de propriété intellectuelle, afin d'établir la matérialité de l'infraction et de la saisir le cas échéant. Elle est aussi chargée de détecter les biens prohibés. La douane est ainsi compétente, dans le cadre de la lutte contre le piratage, pour la saisie et la confiscation de marchandises illicites telles que des boîtiers IPTV préconfigurés ou des disques Blu-ray copiés.

PISTES DE RÉFLEXION POUVANT RENFORCER LES MOYENS OPÉRATIONNELS (1/2)

- *Renforcer significativement les ressources humaines, techniques et financières des services d'enquête en matière d'atteinte à des droits de propriété intellectuelle et aux droits d'exploitation des manifestations ou compétitions sportives.*
- *Créer une « Brigade anti-cybercriminalité unifiée » (BACU) regroupant les moyens et les ressources de plusieurs services d'enquête (l'OCLCTIC, le C3N, la DNRED-SNDJ, voire la DGSJ suivant l'ampleur de l'organisation criminelle) et compétente en matière d'atteintes aux droits de la propriété intellectuelle.*

¹⁰⁰ « La DGCCRF et la Douane se mobilisent pour la sécurité et la loyauté des produits vendus sur les plateformes numériques », DGCCRF [en ligne], 20 décembre 2018.

En outre, le piratage audiovisuel étant transnational, le renforcement de la coopération *a minima* européenne entre les sphères justice-police augmenterait les chances d'identifier et de démanteler les réseaux organisés. Les intermédiaires techniques et les individus impliqués dans la gestion d'un service illicite sont en effet rarement localisés dans un seul et même pays. Des signes encourageants sont visibles depuis ces dernières années avec des actions récurrentes menées par Eurojust et Europol. En 2020, les deux institutions ont dirigé plusieurs opérations coordonnées dans plusieurs pays.

OPÉRATIONS DE DÉMANTÈLEMENT DE RÉSEAUX ORGANISÉS MENÉES PAR EUROJUST ET EUROPOL

Date	Chiffre d'affaires des organisations (en M euros)	Pays		
		Pirates	Serveurs	Autorités publiques
Septembre 2019 ¹⁰¹	6,5	Grèce	France, Allemagne et Pays-Bas	France, Allemagne, Bulgarie, Grèce, Italie, Pays-Bas
Juin 2020 ¹⁰²	15	Allemagne Danemark Espagne, Suède	Espagne et autres	France, Allemagne, Canada États-Unis, Italie, Pays-Bas, Royaume-Uni, Suède et autres
Novembre 2020 ^{103, 104}	10,7	Italie	France, Allemagne, Bulgarie, Lituanie, Malte, Pays-Bas, Roumanie, Slovaquie, Suède	France, Allemagne, Bulgarie, Grèce, Lituanie, Pays-Bas, Roumanie, Slovaquie, Suède
	1,9+	Suisse	France, Allemagne, Pays-Bas, Suisse	France, Allemagne, Monaco Pays-Bas, Suisse

Ce type de coopération est particulièrement bénéfique, notamment parce qu'il favorise le partage d'informations et l'interopérabilité entre les États membres de l'Union européenne. Néanmoins, l'internationalisation de ces réseaux et l'utilisation de la technologie innovante IPTV sont des indicateurs d'une criminalité organisée de plus en plus complexe, à laquelle l'Europe doit faire face. La France, dans chacun de ces exemples, a accueilli sur son territoire un serveur utilisé à des fins de piratage et a mobilisé ses forces de l'ordre. Ces dernières, pour demeurer efficaces face à cette complexité croissante, pourraient adopter les techniques d'enquête spécifiquement consacrées par le Code de procédure pénale pour la délinquance et la criminalité organisées « classiques » (infiltration, enquête sous pseudonyme, interceptions de correspondances, etc.).



Les sites et les services illicites les plus utilisés par les internautes français sont pour la plupart administrés dans des pays d'Afrique du Nord

Frédéric DELACROIX
Délégué général de l'ALPA

¹⁰¹ « Eurojust helps unravel massive trans-European pay-TV fraud », *Eurojust* [en ligne], 18 septembre 2019.

¹⁰² « Illegal streaming service with over 2 million subscribers worldwide switched off », *Europol* [en ligne], 10 juin 2020.

¹⁰³ « Eurojust coordinates action in Italy and ten other countries », *Eurojust* [en ligne], 11 novembre 2020.

¹⁰⁴ « Widely used illegal streaming platform switched off from Switzerland », *Europol* [en ligne], 11 novembre 2020.

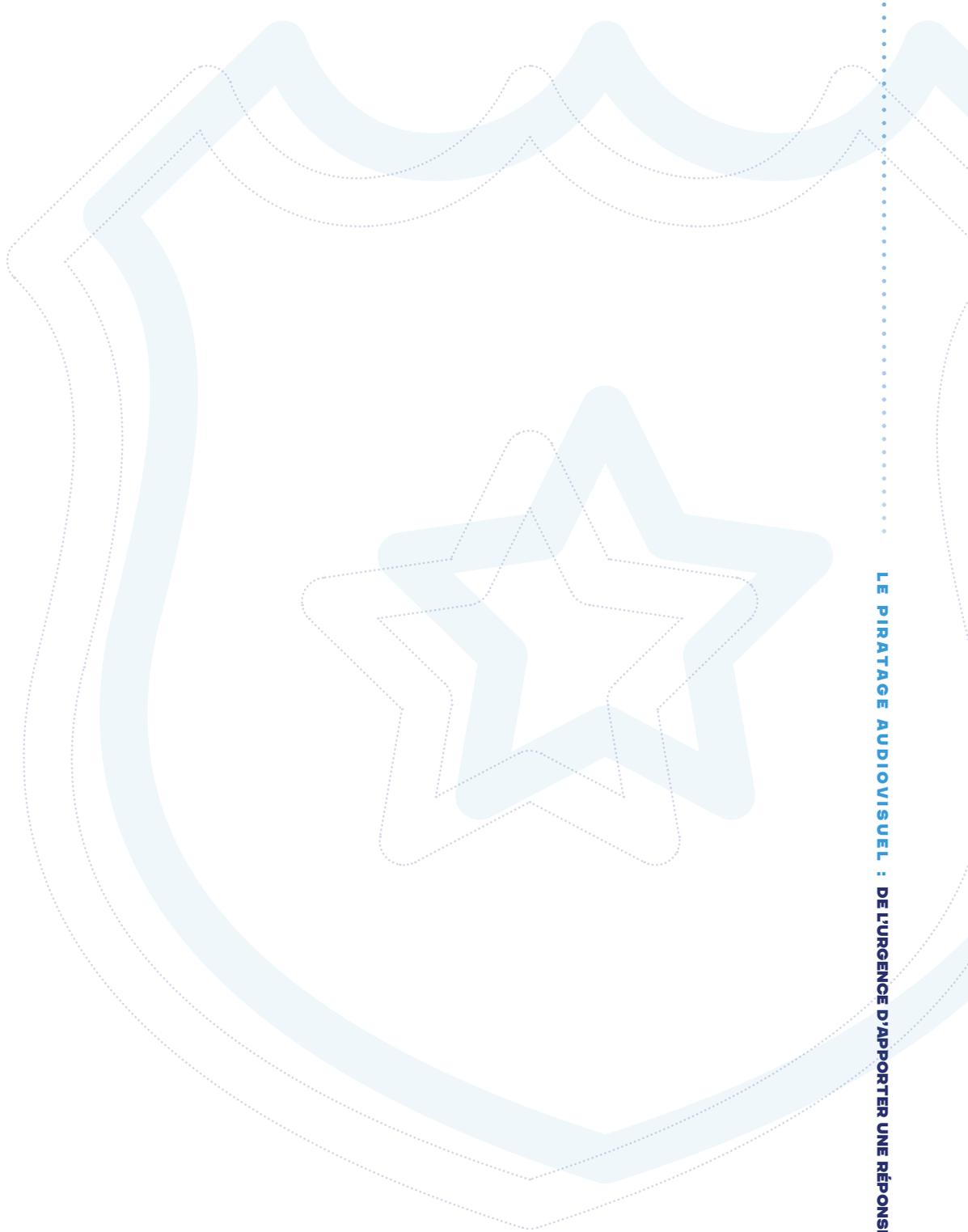
En parallèle, la France pourrait s'efforcer de renforcer sa coopération en la matière avec d'autres pays, et plus particulièrement ceux d'Afrique du Nord. Un nombre important de services illicites basés dans la région s'appuient en effet sur des serveurs français¹⁰⁵.

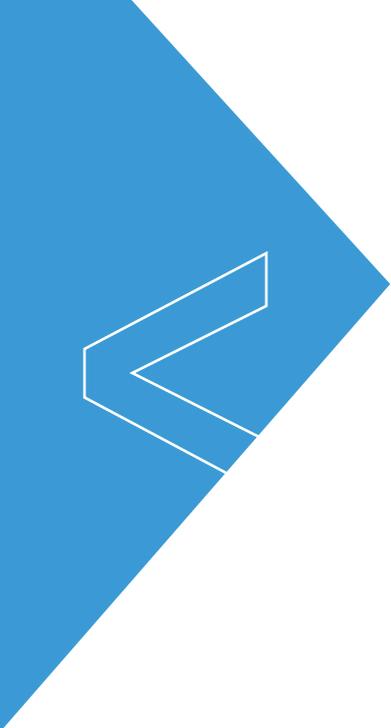
PISTES DE RÉFLEXION POUVANT RENFORCER LES MOYENS OPÉRATIONNELS (2/2)

- *Étendre les pouvoirs d'enquête prévus pour la délinquance et la criminalité organisées, disposés par les articles 706-80 à 706-87 (surveillance et infiltration), 706-89 à 706-94 (perquisitions) et 706-95 à 706-103 (accès à distance aux correspondances, recueil des données techniques de connexion et des interceptions de correspondances, sonorisation, captation des données informatiques) du Code de procédure pénale, aux infractions en matière de droits de la propriété intellectuelle et de droits similaires.*
- *Renforcer significativement la coopération internationale entre les services d'enquête à des fins de collecte des preuves.*



¹⁰⁵ Abderrafiq Khenifsa, « Le piratage des TV payantes en Europe devra connaître des temps durs en Europe et par ricochet en Algérie », *Medium [en ligne]*, 19 septembre 2016.





CONCLUSION

La crise du Covid-19 a montré les limites des actions initiées ces dernières années par les autorités publiques et les ayants droit pour lutter contre le piratage audiovisuel.

En mars 2020, les consommateurs illicites étaient ainsi 13,6 millions, contre 12 millions en 2016. Bien que cette hausse soit certainement le fruit spontané d'un contexte sanitaire singulier, il démontre de manière inquiétante que le piratage reste un recours solidement ancré chez beaucoup de Français.

Examiné à l'Assemblée nationale ce mois de juin, après une adoption en première lecture au Sénat en mai dernier, le projet de loi relatif à « *la protection de l'accès du public aux œuvres culturelles à l'ère numérique* », apporte des réponses encourageantes et nécessaires mais encore insuffisantes. Le texte se concentre en effet sur les conséquences du piratage, lorsque le « *mal est déjà fait* », et ne prend pas en compte les origines structurelles – bien souvent sous-estimées – sur lesquelles celui-ci se fonde et se développe.

D'une part, un écosystème opaque d'acteurs recourant à diverses techniques numériques pour préserver leur anonymat, les rendant dès lors difficilement traçables. Les « *Robins de bois* » des premières heures d'Internet, qui assortissaient le piratage d'un idéal de partage, se sont largement fait supplanter par une criminalité qui s'est peu à peu déportée sur la toile. Le piratage apparaît pour ces réseaux criminels comme une activité lucrative et peu risquée sur le plan pénal. Leur structuration transnationale facilitée par Internet, conjuguée à l'utilisation de technologies sophistiquées, rendent cette criminalité organisée très complexe et difficile à appréhender. Une connaissance plus fine de cet environnement permettrait dès lors d'avoir une réponse globale plus adaptée.

D'autre part, une législation et des moyens opérationnels qui ne permettent ni d'identifier ces pirates, ni de réagir rapidement contre des modes de piratage qui ne cessent de s'industrialiser. Si le *peer-to-peer* a diminué, d'autres modes de piratage se maintiennent quant à eux à des niveaux élevés (*streaming*, le téléchargement direct...) ou montent en puissance (IPTV et *live streaming*). En l'état, les délais de retrait de contenus ou de blocage de sites pirates ne peuvent endiguer ce phénomène.

Face à la temporalité des procédures judiciaires, ainsi qu'au manque de moyens humains et techniques des services d'enquête, les contenus portant atteinte à la propriété intellectuelle ont largement le temps d'être consommés, voire copiés pour alimenter d'autres services pirates. Afin de maximiser l'efficacité des autorités, celles-ci doivent pouvoir exiger la coopération des intermédiaires techniques (fournisseurs d'accès à Internet, moteurs de recherche, hébergeur de fichiers...).

Facteur de déstabilisation de l'ordre public numérique, le piratage entraîne également des conséquences directes dans la vie « hors-ligne », avec un manque à gagner réel pour l'État et les ayants droit (1,03 milliard d'euros en 2019). Celui-ci se concrétise notamment par une réduction des moyens économiques des métiers de l'audiovisuel, en affectant de bout-en-bout la chaîne de valeur de la filière, et par un rayonnement *de facto* moindre des productions françaises dans le monde. Le manque à gagner impacte aussi le domaine du sport, le piratage des retransmissions sportives affectant le financement, avec la taxe dite « Buffet », de la pratique, aussi bien professionnelle qu'amateur.

La lutte contre le piratage revêt par ailleurs un enjeu de santé publique. En cause, les publicités, bien souvent à caractère pornographique, finançant la majeure partie des sites illégaux de *streaming* et de téléchargement. Celles-ci, relayées par des régies publicitaires étrangères et peu scrupuleuses, sont en effet susceptibles d'avoir un impact psychologique sur les plus jeunes. Côté cybersécurité, ces bannières peuvent par ailleurs contenir des *malwares* conçus pour infecter tout type de terminal (ordinateurs, smartphones, tablettes, etc.), et entraîner ainsi des vols de données voire des usurpations d'identité des consommateurs illicites.

Ni « crime sans victime », ni « concurrent sans visage », le piratage audiovisuel est aujourd'hui un crime organisé et doit être traité comme tel. Cette menace transversale doit dès lors être appréhendée avec une myriade de solutions, dans le cadre d'une stratégie interministérielle globale. Celles-ci devront notamment reposer sur une sensibilisation quant aux menaces inhérentes à cette pratique pour limiter les comportements irresponsables, une réaction quasi-instantanée des autorités à la mise en ligne de contenus piratés, fondée sur une sphère police-justice avisée, ainsi que sur des coopérations proactives sur les plans « public-privé » et international. Des objectifs qui ne seront atteints que sous l'impulsion d'une volonté politique forte et ambitieuse.

SPÉCIFICITÉ DE LA LUTTE CONTRE LE PIRATAGE DANS LES PAYS VOISINS

LES ÉTATS MEMBRES DE L'UNION EUROPÉENNE ONT ADOPTÉ DES APPROCHES DIFFÉRENTES EN MATIÈRE DE LUTTE CONTRE LE PIRATAGE AUDIOVISUEL. OUTRE DES MESURES LÉGISLATIVES ET RÉGLEMENTAIRES¹⁰⁶, CERTAINS PAYS SE DISTINGUENT PAR UNE VOLONTÉ AFFIRMÉE D'INCLURE LES INTERMÉDIAIRES TECHNIQUES ET DES SERVICES D'ENQUÊTE.

ITALIE

UN DISPOSITIF DE LUTTE PROACTIVE CONTRE LES SITES MIROIRS¹⁰⁷

Autorité administrative indépendante, l'Autorità per le garanzie nelle comunicazioni (AGCOM) peut ordonner, aux fournisseurs d'accès à Internet (FAI), le blocage de sites de *streaming* et de *live streaming* diffusant illégalement des œuvres culturelles ou sportives. Les événements sportifs sont en effet protégés au même titre que les biens culturels en vertu d'un droit voisin introduit en 2008.

Concernant les sites illicites basés en Italie, l'AGCOM peut enjoindre à leurs hébergeurs de procéder au retrait d'œuvres préalablement notifiées par les ayants droit. Cette procédure de notification et de retrait varie entre 3 et 35 jours, mais peut être accélérée en cas de violations massives.

En juillet 2018, la justice italienne, saisie d'un cas de réapparition d'un site bloqué sous la forme de site miroir, a ordonné la mise en place d'un système de blocage « *proactif* ». Les FAI doivent depuis empêcher l'accès aux contenus illicites sur demande des ayants droit, y compris lorsqu'il s'agit d'un site qui, indépendamment du nom de domaine en cause, conduit aux mêmes violations constatées dans la décision initiale de blocage. Les frais sont à la charge des ayants droit.



¹⁰⁶ « La lutte contre le piratage aujourd'hui et demain », *NPA Conseil* [en ligne], consulté en mars 2021.

¹⁰⁷ Hadopi, *Stratégies de lutte contre le piratage des contenus culturels et sportifs*, Rapport de veille internationale, 2019, p. 9.

PORTUGAL

UN SYSTÈME DE COLLABORATION ENTRE L'ÉTAT, LES AYANTS DROIT ET LES FAI¹⁰⁸



En 2015, l'Inspeção Geral Das Actividades Culturais – IGAC (ministère de la Culture) a signé un mémorandum avec les FAI (réunis au sein de l'APRITEL) et les ayants droit (regroupés dans la MAPINET). En vertu de cet accord, la MAPINET peut obtenir chaque mois le blocage DNS de cent sites portant atteinte à la propriété intellectuelle, qu'elle a identifiés préalablement.

La MAPINET doit pour cela notifier, preuves à l'appui, des sites dont les deux tiers des contenus sont piratés ou ceux proposant plus de 500 liens illicites. Après vérification, l'IGAC demande aux FAI, à l'occasion de deux créneaux mensuels prévus à cet effet, de procéder aux blocages DNS sous 48h.

Comme les événements sportifs sont protégés par la propriété intellectuelle, ce dispositif administratif s'étend au *live streaming* et favorise ainsi le blocage en direct de matchs diffusés illégalement.

¹⁰⁸ *Ibid.*

ROYAUME-UNI

UNE UNITÉ D'ENQUÊTE SPÉCIALISÉE DANS LA PROPRIÉTÉ INTELLECTUELLE¹⁰⁹

Créée en 2013, la Police Intellectual Property Crime Unit (PIPCU) est une unité de police de Londres, financée par l'Intellectual Property Office (département des Affaires, de l'Énergie et des Stratégies industrielles). Elle enquête et prévient les délits graves et organisés liés à la propriété intellectuelle au Royaume-Uni. La PIPCU présente la particularité de ne pas être soumise aux autorisations d'un juge.

Comptant une vingtaine de policiers (dont enquêteurs et détectives), la PIPCU se concentre sur les délits de propriété intellectuelle ayant des implications pour la sécurité publique. Elle a ainsi enquêté sur des infractions de contrefaçon et de piratage numérique d'une valeur de plus de 100 millions de livres sterling. L'unité a notamment suspendu plus de 30 000 sites Web vendant de la contrefaçon.

Lorsqu'elle identifie un site pirate, la PIPCU adresse un courrier au registraire de nom de domaine associé en lui demandant de suspendre le site. Face au manque fréquent de répondant des acteurs situés hors du Royaume-Uni, la police britannique s'efforce de conclure des accords internationaux avec des organismes de gestion des noms de domaine étrangers, ainsi que des bureaux d'enregistrement.



MODES DE FINANCEMENT DU PIRATAGE AUDIOVISUEL

La publicité comme source principale de revenus

Les hébergeurs et les sites de référencement de contenus illicites valorisent leurs audiences par la monétisation publicitaire. Ces acteurs privilégient des types spécifiques de piratage (*streaming*, *peer-to-peer*, téléchargement direct) qui se sont pérennisés avec la numérisation accrue des espaces publicitaires et le développement du numérique (réduction des coûts de stockage, augmentation des niveaux de compression vidéo et de débit Internet).



LE STREAMING : LE MOYEN LE PLUS RÉPANDU DE CONSOMMATION ILLICITE

Ce mode de transmission de données en flux continu permet à un internaute de visionner directement des vidéos à partir d'un site Internet, notamment des films et des séries. Bien qu'offrant des niveaux de qualité variables, le *streaming* présente l'avantage d'être facile d'accès, simple d'utilisation, et ne requiert pas le téléchargement complet d'un contenu audiovisuel.

**1 individu sur 2
a recours
au streaming
pour accéder à
du contenu piraté**

Le *streaming* est la pratique la plus répandue pour visionner des contenus illégaux. Sa popularité s'explique entre autres par l'individualisation des consommations sur des supports mobiles (*smartphones* et tablettes)¹¹⁰.

La navigation sur un site connu de streaming illégal qui hébergeait plus de 480 séries et attirait jusqu'à 700 000 visiteurs par mois était « agrémentée à chaque clic de fenêtres publicitaires intempestives¹¹¹ ».

¹¹⁰ EY, *Piratage en France*, Février 2017, p. 7.

¹¹¹ « Site illégal de streaming : 8 mois de prison avec sursis requis contre le jeune pirate informatique franc-comtois », *franceinfo* [en ligne], 13 novembre 2019.



LE PEER-TO-PEER (P2P) : UNE PRATIQUE QUI DURE

Le *peer-to-peer* permet le téléchargement d'un fichier partagé sur un réseau d'ordinateurs de particuliers. Il met directement un internaute en liaison avec un ou plusieurs autres internautes pour l'obtention d'un fichier spécifique. Ce protocole est le seul visé par la « réponse graduée » de l'Hadopi en vigueur depuis 2010, qui consiste à envoyer des messages de prévention avant de sanctionner les consommateurs.

Le périmètre d'action de l'Hadopi ne se limite qu'au P2P. Il est inadapté aux enjeux du piratage tant la tendance est aujourd'hui au streaming et au DDL.

En déclin, le P2P présente quelques contraintes techniques, car il nécessite notamment l'installation d'un logiciel. Ses adeptes y ont néanmoins recours de manière fréquente.



LE TÉLÉCHARGEMENT DIRECT (DDL) : UN PROTOCOLE POPULAIRE

Le téléchargement direct (*direct download*) est la mise à disposition d'un fichier sur un serveur de stockage accessible depuis un site Web. Suivant un modèle « *client-serveur* », cette pratique propose des contenus souvent de bonnes qualités et concerne aussi bien les films, les séries télévisées, que les dessins animés.



Pour accéder au contenu audiovisuel recherché, l'internaute doit passer par un site de référencement de liens qui le redirige ensuite vers un autre site d'hébergement de fichiers (1fichier, Rapidgator, Uptobox, etc.), après avoir été très souvent exposé à plusieurs fenêtres intempestives de publicité.

Le DDL a bénéficié du départ des utilisateurs du P2P inquiétés par la réponse graduée de l'Hadopi (cf. *supra*).

Pour la première fois, un responsable de site français d'hébergement a été poursuivi en 2021. Des débats sont en cours pour déterminer sa responsabilité dans la circulation de contenus illicites¹¹²

La publicité finance en grande partie les sites de piratage de contenus non linéaires (*streaming*, DDL et P2P). Ces derniers peuvent toutefois percevoir des revenus complémentaires en proposant des options spécifiques telles que la suppression du délai d'attente entre plusieurs téléchargements. Si la pratique du P2P a diminué ces dernières années, celles du *streaming* et du DDL se maintiennent à des niveaux élevés.

¹¹² Maxime Arnoult, Procès contre 1fichier.com : « On essaye de le présenter comme le plus grand pirate de France », *L'Est républicain [en ligne]*, 22 janvier 2021.

L'organisation d'offres illégales d'abonnement



LE CARD SHARING : UNE PRATIQUE EN COURS DE TRANSFORMATION

Protocole ancien, le *card sharing* consiste à partager illégalement un abonnement à des chaînes de télévision payante avec plusieurs utilisateurs. Il permet l'accès gratuit et en qualité haute définition (HD) à des bouquets payants sur un écran de télévision. Ce mode de consommation illicite, outre la vente via Internet d'abonnements pirates, nécessite l'achat au préalable d'un décodeur et d'une parabole.

Réservé à un public averti étant donné la relative complexité d'installation matérielle, le *card sharing* comptait un nombre estimé à plusieurs dizaines de milliers d'utilisateurs français en 2017. Cette pratique laisse peu à peu la place à l'IPTV en raison notamment d'un renforcement du chiffrement du signal¹¹³.

En France, le détournement des boîtiers multimédias (box TV) et des téléviseurs connectés (*smart TV*) se substitue progressivement au modèle du *card sharing*, tout en présentant l'avantage de ne pas nécessiter d'infrastructure importante. Le principe est le même : l'utilisateur peut accéder gratuitement à des services de vidéo à la demande (SVOD) payants, par le biais d'un compte qui peut soit avoir été piraté ou soit faire l'objet d'un partage abusif et contraire aux conditions d'utilisations. En 2019, les SVOD auraient enregistré un manque à gagner de 9,1 milliards d'euros dans le monde en raison de cette pratique¹¹⁴.

**En recul
en France,
le card
sharing reste
populaire au
Maghreb et
en Amérique
latine**

¹¹³ *Ibid.*

¹¹⁴ « Piracy and account sharing cost US pay-TV and OTT operators more than \$9 billion in 2019 and forecasted to reach \$66 billion worldwide by 2022 », *Park Associates* [en ligne], 15 janvier 2020



L'IPTV : LE DÉVELOPPEMENT DU PIRATAGE D'OFFRES INTÉGRALES

L'IPTV (*Internet Protocol Television*) désigne un mode de consommation de flux de télévision via un protocole Internet plutôt que par câble ou par satellite. Il propose par extension des services de télévision en direct, de vidéo à la demande et de *replay*. La désignation IPTV couvre ainsi le visionnage de ces flux TV à partir d'Internet et ce quel que soit le support (ordinateur, télévision, *smartphones*, etc.).

Un service IPTV consiste en un logiciel qui permet à l'utilisateur d'accéder à un serveur dans lequel des contenus illicites sont stockés et par lequel des flux de *live streaming* transitent. Cette application peut être directement installée sur un boîtier à connecter à une télévision ou à d'autres terminaux.

L'IPTV est une technologie légale de diffusion, mais elle fait l'objet de détournements à des fins illicites¹¹⁵. Beaucoup d'offres IPTV ont profité de l'émergence d'acteurs de vidéo à la demande – VOD (Amazon Prime Video, Disney+, Netflix...), ainsi que de l'éclatement des droits de retransmission des événements sportifs entre plusieurs diffuseurs (beIN Sports, Canal+ et RMC Sport), pour étoffer leurs propres catalogues de contenus piratés. Certaines proposent même des milliers de chaînes TV (dont celles payantes) et de contenus VOD pour une centaine d'euros par an.

Pour la France, une étude avance le chiffre de 2,3 millions d'utilisateurs d'offres IPTV illégales en 2018¹¹⁶. Ces derniers auraient ainsi contribué, considérant un abonnement en moyenne de 6,78 euros par mois, à un chiffre d'affaires évalué à 181 millions d'euros. L'IPTV attire surtout une communauté stable d'utilisateurs initiés.

L'Hadopi appelle à davantage de vigilance quant à son utilisation accrue, tant ce mode de consommation est relativement récent. En décembre 2020, la justice, qui avait jusque-là peu appréhendé ce piratage, a décidé le blocage inédit de huit services IPTV sous l'impulsion notamment des ayants droit¹¹⁷.

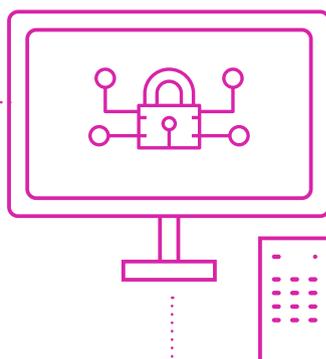
¹¹⁵ Manuel Alaver, « IPTV : cette pratique illégale qui permet de regarder Canal+ ou beIN Sports à moindre frais », *Capital* [en ligne], 24 mai 2019.

¹¹⁶ European Union Intellectual Property Office, *Illegal IPTV in the European Union*, Novembre 2019, p. 50.

¹¹⁷ « La France bloque l'accès à 8 services IPTV illégaux », *presse-citron* [en ligne], 26 janvier 2021.



Une fois les bons plug-ins installés, le lecteur multimédia Kodi permet d'accéder, illégalement et en permanence, à une source illimitée de vidéos de rencontres sportives. Il est possible de s'en procurer pour une trentaine d'euros sur des sites marchands tels que Alibaba, Gearbest ou Aliexpress¹¹⁸.



amazonPrime

Disney+

NETFLIX

RMC
SPORT

beIN
SPORTS

CANAL+

¹¹⁸ Fabien Soyez, « Comment les sites (illégaux) de streaming de football font leur beurre sur le dos des diffuseurs », CNET France [en ligne], 14 août 2020.



LE CAS SPÉCIFIQUE DU LIVE STREAMING : DES CONTENUS À HAUTE VALEUR INSTANTANÉE



**Une question.
Pourquoi payer 25 €,
pour la même chose
en accès libre sur
Internet ?**

Anonyme
Cité par Ouest France¹¹⁹

Le *live streaming* désigne un mode de consommation d'un contenu linéaire diffusé en direct depuis un site Internet. Il présente la particularité de se financer aussi bien par la publicité que par la vente d'abonnements. Ce moyen est particulièrement privilégié pour le visionnage de rencontres sportives, car il permet de contourner les offres de la télévision payante. Les liens d'accès aux contenus de *live streaming* sont de plus en plus communiqués peu de temps avant le début des événements, rendant leur déréférencement des moteurs de recherche plus difficile. Si le football apparaît comme la discipline la plus touchée par ce piratage, le tennis, le rugby, le basket-ball et la formule 1 le sont également.

Ce protocole repose sur le piratage d'offres légales, plus précisément des flux entrants et sortants des décodeurs et des boîtiers connectés à une télévision par câble HDMI. La qualité et la stabilité des flux piratés ont progressé ces dernières années, car les pirates se soucient aujourd'hui davantage de l'expérience utilisateur, dans le but de fidéliser leurs audiences. Ils investissent ainsi massivement dans l'encodage et dans des infrastructures, car streamer à grande échelle nécessite un certain niveau technique¹²⁰. Le piratage de ces flux s'effectue souvent dans des centres dédiés, notamment en Asie du Sud-Est¹²¹, témoignant dès lors de la structuration à l'échelle mondiale d'un véritable commerce illicite autour du *live streaming* sportif.

En raison de la suspension des compétitions sportives pendant la crise Covid-19, le taux de recours au *live streaming* a diminué entre 2019 et 2020¹²². Ce type de piratage demeure pourtant largement employé puisque 3,4 millions d'internautes y ont eu recours en septembre 2020¹²³.

**Lancé en
août 2020, Téléfoot
n'a pas atteint
les 3,5 millions
d'abonnés escomptés
pour rentabiliser
l'investissement de
800 millions d'euros.
Plusieurs facteurs y
ont contribué dont la
concurrence des sites
de streaming gratuits.
La chaîne a fermé moins
de six mois plus tard.**

¹¹⁹ Pierre Guyon, « Droits TV. « Trop cher », la concurrence du streaming », *Ouest France* [en ligne], 27 janvier 2021.

¹²⁰ *Op. cit.* Fabien Soyez, *CNET France*, 14 août 2020.

¹²¹ Damien Licata, « Rojadirecta, LiveTV Qui se cache derrière les sites de streaming de foot ? », *Le Parisien* [en ligne], 12 février 2019.

¹²² Hadopi, *Baromètre de la consommation de biens culturels dématérialisés*, Février 2021, p. 37.

¹²³ Hadopi, *Étude de l'impact économique de la consommation illicite en ligne de contenus audiovisuels et de retransmissions*, Décembre 2020, p. 32.

LES CONTENUS PIRATÉS AU CŒUR D'UNE VASTE CHAÎNE D'ACTEURS LÉGAUX

Accès aux contenus piratés



Les **MOTEURS DE RECHERCHE** (Bing, Google, etc.) demeurent la principale porte d'entrée vers les contenus illicites. Une requête peu approfondie contenant le terme «*streaming*» en complément du titre d'un film ou d'une série, voire d'une rencontre sportive, suffit à se voir proposer plusieurs sites illicites diffusant le contenu recherché.

Dans le cas de l'IPTV, la simple saisie des mots-clés «*abonnement IPTV*» oriente vers des dizaines de sites frauduleux commercialisant des abonnements illicites, mais aussi vers des liens sponsorisés redirigeant vers des sites de commerce en ligne (de type AliExpress ou eBay) pour l'achat de boîtiers.

Si la visibilité des sites pirates a été réduite ces dernières années, en raison des demandes de déréférencement des ayants droit au profit d'une meilleure indexation de l'offre légale¹²⁴, il demeure aisé d'en trouver à la première page des résultats d'une requête.



Les **FOURNISSEURS D'ACCÈS À INTERNET (FAI)** (Bouygues, Free, Orange, SFR, etc.) occupent une place importante aussi bien dans l'accès que dans la lutte contre le piratage audiovisuel. Ces derniers permettent en effet à leurs clients de se connecter à Internet et d'accéder à un certain nombre de contenus parmi lesquels ceux illicites.

Les FAI mettent à disposition des internautes un serveur DNS chargé de traduire le nom d'un site Internet (nom de domaine) en une adresse IP, qui permet aux machines de «*communiquer*» entre elles. Lorsqu'un individu souhaite accéder à un site Internet, il en saisit le nom de domaine dans un navigateur, puis le serveur DNS effectue une requête pour trouver l'adresse IP associée. Une connexion entre le navigateur et le serveur qui héberge le site Internet est alors établie afin de charger la page Web.

¹²⁴Ernesto Van der Sar, « Pirate Site Search Traffic Tanked Following Google Updates », *TorrentFreak* [en ligne], Janvier 2021.



VIRTUAL PRIVATE NETWORK (VPN) Un permet d'accéder de manière sécurisée à des réseaux privés et de protéger l'anonymat de son utilisateur. Il permet de masquer son adresse IP en en utilisant une autre associée à une autre localisation. Par exemple, un individu connecté à Internet via un VPN localisé aux États-Unis sera perçu comme étant physiquement dans le pays du fait de son adresse IP américaine, alors qu'il est en réalité en France. Si ce même individu est abonné à une offre légale qui diversifie ses contenus en fonction de la zone géographique, il pourra alors accéder au catalogue américain, normalement inaccessible ailleurs.

Les VPN sont souvent utilisés pour télécharger en *peer-to-peer* et échapper ainsi à la détection de l'Hadopi¹²⁵. Des solutions proposent même des serveurs optimisés spécialement dédiés à cet usage, comme entre autres ExpressVPN¹²⁶ (établi aux îles Vierges Britanniques) et NordVPN¹²⁷ (Panama).

Hébergement et diffusion



Les **REGISTRAIRES DE NOM DE DOMAINE** créent et fournissent des noms de domaine aux administrateurs de sites Web pour une durée déterminée. Ceux établis à l'étranger, notamment dans des paradis réglementaires, sont plus enclins à ne pas coopérer avec des autorités publiques qui cherchent à identifier les responsables de sites dont ils ont la charge. Les données d'identification de leurs clients sont en effet généralement plus difficiles à obtenir¹²⁸.

Les propriétaires de noms de domaine de sites illicites privilégient des registraires à l'étranger dont ils peuvent en plus fournir des coordonnées anonymisées, voire fictives. Ils passent à cet égard par des sociétés-écrans, souvent localisées dans des paradis réglementaires, qui ajoutent une couche d'opacité susceptible d'empêcher les ayants droit ou les autorités publiques de remonter jusqu'à eux.

¹²⁵ Roméo Arnault, « Est-ce qu'un VPN permet vraiment d'échapper à Hadopi ? », *clubic* [en ligne], 4 novembre 2020.

¹²⁶ « Le Guide du torrenting avec ExpressVPN », *pypo* [en ligne] 12 novembre 2020.

¹²⁷ « Quel est le meilleur VPN pour le téléchargement en P2P ? », *Android MT* [en ligne], 11 septembre 2020.

¹²⁸ Hadopi, *L'écosystème illicite de biens culturels dématérialisés*, Janvier 2019, p. 44.



Les **HÉBERGEURS WEB** mettent à disposition des serveurs pour héberger des sites Internet. Outre l'hébergement de sites partageant des contenus piratés, ils stockent les flux de *live streaming* et des services IPTV. Les hébergeurs Web stockent des milliers de flux illicites qui font l'objet chaque mois de demandes de retraits. Pour autant, la majorité n'y procède qu'avec réticence et dans des délais parfois très longs. Beaucoup de ces hébergeurs sont en effet peu enclins à sanctionner les utilisateurs qui y téléversent massivement des contenus illicites, en les bannissant via leurs adresses IP par exemple.

Ces hébergeurs mettent à la disposition deux types de serveurs :

- Les serveurs « *mutualisés* », qui peuvent héberger de nombreux sites Internet différents, pour une multitude de clients. L'hébergeur garde la main sur ces serveurs et peut ainsi suspendre assez facilement tel ou tel site en cas de signalement d'infractions par des plaignants ;
- Les serveurs « *dédiés* », à la disposition entière du client qui en fait ce qu'il veut (et peut par exemple légalement le sous-louer à des sous-clients). De ce fait, la responsabilité de l'hébergeur est transférée d'office à son client, car il ne peut intervenir de manière directe ou chirurgicale sur ce type de serveurs (à moins de le « *couper* » entièrement en dernier recours).

Les administrateurs de sites pirates de taille importante, ainsi que les opérateurs de services illicites IPTV, utilisent généralement des serveurs dédiés. D'une part, ils peuvent les configurer à leur guise et d'autre part, ce système ajoute des couches de complexités intermédiaires. Il devient ainsi plus difficile pour les ayants droit de faire fermer les sites et les services illicites qui y sont stockés. Si un hébergeur Web reçoit une plainte concernant l'un de ses serveurs dédiés, il peut la transférer à son client qui aura la charge d'agir ou qui la fera lui-même suivre à son sous-client, empêchant tout processus de résolution rapide des litiges.



Les **SITES D'HÉBERGEMENT DE FICHIERS** tels que 1fichier, Rapidgator et Uptobox font partie intégrante du piratage audiovisuel. Ils permettent à des utilisateurs d'héberger du contenu sur des serveurs à des fins de téléchargement, de *streaming*, voire les deux. L'accès à ce type de service s'effectue souvent par le biais d'un lien hypertexte référencé par des sites pirates. Bien que légaux, les sites d'hébergement de fichiers sont utilisés pour partager des contenus enfreignant le droit d'auteur¹²⁹.

Certains sites d'hébergement de fichiers ont une politique de rémunération visant à récompenser les utilisateurs dont les contenus ont été vus ou téléchargés un certain nombre de fois. Si la plupart de ces sites appliquent les demandes de retrait de contenu, certains n'y consentent pas au motif du régime de responsabilité des hébergeurs prévu par le droit français et européen¹³⁰ (cf. p. 34). Des contenus retirés peuvent par ailleurs réapparaître sous un lien hypertexte différent.

¹²⁹ Marc Rees, « 1Fichier.com assigne en justice le ministère de la Culture et Bercy », *Next INpact* [en ligne], 21 juin 2018.

¹³⁰ Maxime Arnoult, Procès contre 1fichier.com : « On essaye de le présenter comme le plus grand pirate de France », *L'Est républicain* [en ligne], 22 janvier 2021.



Les **PLATEFORMES DE CONTENU GÉNÉRÉ PAR LES UTILISATEURS (UGC)¹³¹** telles que Facebook et YouTube permettent de publier des contenus produits par les internautes. Cependant, elles ont rapidement été détournées dans le but de diffuser illégalement des contenus audiovisuels protégés par le droit d'auteur.

En dépit de l'adoption d'outils de reconnaissance destinés à identifier les contenus piratés, les plateformes UGC continuent d'en héberger, ainsi que des flux «live» d'événements sportifs et des tutoriels expliquant comment accéder ou utiliser des services illicites.



FABRICANTS DE LECTEURS MULTIMÉDIAS Pour la plupart chinoise, les entreprises à l'origine de dispositifs de diffusion multimédias (de type Kodi) participent indirectement au développement du piratage audiovisuel. Ces équipements, légaux, consistent en des boîtiers à brancher à une télévision ou autre terminal. Leurs utilisateurs peuvent néanmoins les configurer à l'aide d'un plug-in de sorte à faciliter leur accès à un service illégal IPTV spécifique. Par une décision du 26 avril 2017, la Cour de justice de l'Union européenne (CJUE) a statué que la vente de ces boîtiers déjà préconfigurés par leurs constructeurs, à des fins illicites, constituait une atteinte au droit d'auteur.

Promotion et commercialisation



Les **RÉSEAUX SOCIAUX** (Facebook, Vkontakte, etc.) contribuent à banaliser le piratage audiovisuel. Il y existe des comptes, des pages et des groupes promouvant des sites ou des services illicites^{132, 133}. Sur ces différents supports, les utilisateurs peuvent accéder à des contenus portant atteinte au droit d'auteur publiés en natif, accéder à des liens renvoyant vers des hébergeurs de fichiers ou s'en échanger directement¹³⁴. Les réseaux sociaux fédèrent par ailleurs des communautés d'utilisateurs en quête de contenus piratés.



Les **SITES DE COMMERCE EN LIGNE** (*marketplaces*) ont permis aux contrefacteurs d'étendre la portée de leurs activités dans le monde¹³⁵. Certaines boutiques en ligne, essentiellement hébergées en Asie, y commercialisent des offres d'abonnement et des boîtiers pirates préconfigurés capables de capter des flux IPTV¹³⁶. Elles promeuvent leurs services et leurs produits par le biais d'annonces, notamment référencées en Chine, rédigées en français de sorte à atteindre une audience.

¹³¹ User Generated Content.

¹³² Chaim Gartenberg, « Facebook has a movie piracy problem, but it can't (or won't) do anything about it », *The Verge* [en ligne], 13 juillet 2018.

¹³³ *Counterfeit and Piracy Watch List*, European Commission, 14 décembre 2020, p. 34.

¹³⁴ Hadopi, *Baromètre de la consommation de biens culturels dématérialisés*, Février 2021, p. 37.

¹³⁵ Unifab, *Contrefaçon et terrorisme*, 2017, p. 24.

¹³⁶ EY, *Piratage en France*, Février 2017, p. 10.

Monétisation



RÉGIES PUBLICITAIRES La principale source de financement des sites illégaux de téléchargement direct, de *streaming* et de *live streaming*, est la publicité. Bénéficiant d'un trafic parfois très élevé, ces sites agissent comme des éditeurs de contenus commercialisant des espaces publicitaires sur leurs pages Web à des annonceurs, pour leur assurer de l'exposition. La relation entre ces derniers se fait par l'intermédiaire de régies publicitaires dites externes. Les régies fournissent aux éditeurs de contenus un code informatique à intégrer au script du site pour y afficher les publicités¹³⁷.

Les annonces publicitaires publiées sur les sites illicites se déclinent en formats image, vidéo et semi-animé. Souvent suffisamment intrusives pour contourner les logiciels antipubs, elles s'intègrent en surimpression au contenu vidéo recherché, sous la forme de bannière ou de fenêtre *pop-up*. La publicité peut intervenir dès l'entrée de l'internaute sur le site, lorsqu'il y navigue de page en page, ou lors de la consommation d'un contenu. Dans le cas du *streaming* et du *live streaming*, elle s'intègre à la vidéo et sa fermeture entraîne l'apparition d'autres fenêtres publicitaires¹³⁸.

Certaines régies publicitaires étrangères ne sont pas regardantes des sites avec qui elles collaborent, dont en premier lieu ceux de streaming illégal

En 2015, le ministère de la Culture a lancé une «*Charte des bonnes pratiques dans la publicité pour le respect du droit d'auteur et des droits voisins*», signée par des ayants droit, des régies publicitaires sur Internet et des annonceurs. Celle-ci vise à empêcher les annonceurs de bonne foi de retrouver à leur insu leurs publicités sur des sites douteux et de financer ainsi la consommation illicite de biens protégés. En d'autres termes, le but est d'éviter des incidents pouvant porter atteinte à l'image des annonceurs et d'assécher les revenus des sites illicites¹³⁹. Les résultats demeurent toutefois sujets à caution.

Les sites pirates diffusent désormais généralement des publicités à caractère pornographique ou promouvant des sites de rencontre, des jeux d'argent ou érotiques, et des fausses solutions antivirus. Certaines de ces publicités inappropriées sont aussi elles-mêmes porteuses de virus informatiques (*malvertising*).



EXEMPLE D'ANNONCES LÉGALES QU'IL EST ENCORE POSSIBLE DE TROUVER SUR DES SITES ILLICITES DE STREAMING

¹³⁷ « Comment fonctionne la publicité sur Internet et quels risques », *Le Blog du Hacker* [en ligne], 8 juillet 2018.

¹³⁸ Hadopi, *L'écosystème illicite de biens culturels dématérialisés*, Janvier 2019, p. 47-48.

¹³⁹ Ministère de la Culture, *Signature de la charte des bonnes pratiques dans la publicité en ligne pour le respect du droit d'auteur et des droits voisins*, Mars 2015.



INTERMÉDIAIRES DE PAIEMENT En 2015, le ministère de la Culture a mis en place un comité de suivi destiné à limiter les moyens de paiement des sites pirates afin d'assécher leurs ressources financières. Composé d'intermédiaires de paiement dont MasterCard, PayPal et Visa Europe, ce comité a indiqué l'année suivante que tous les moyens de paiement «classiques» avaient été supprimés des sites illicites¹⁴⁰. Pour autant, une enquête effectuée en 2018 indique que les trois cités auraient toujours été impliqués dans l'écosystème du téléchargement illégal¹⁴¹.

Cette initiative a néanmoins certainement poussé des sites pirates à se tourner davantage vers d'autres systèmes de paiement (comme alloPass, Skrill, etc.) voire des portefeuilles de cryptomonnaie. Ils en font divers usages, dont la récolte de dons des internautes, ainsi que le règlement des régies publicitaires et des coûts d'infrastructures techniques (hébergement, noms de domaine, etc.). Ces services sont également utilisés par les offres IPTV comme moyens de paiement pour permettre aux utilisateurs de régler leurs abonnements de façon rapide et sécurisée.

¹⁴⁰ Ministère de la Culture, *Charte de bonnes pratiques dans la publicité pour le respect du droit d'auteur et des droits voisins*, Rapport 2015-2016, p. 3.

¹⁴¹ « Téléchargement illégal : PayPal, Visa et Master Card impliqués ? », *Rude Baguette* [en ligne], 6 septembre 2018.

REMERCIEMENTS

Forward Global remercie toutes les personnes auditionnées
dans l'élaboration de ce livre blanc :

- **Alexandra Bensamoun**, professeure de droit à l'Université Paris-Saclay
- **Pauline Blassel**, secrétaire générale de l'Hadopi
- **Frédéric Delacroix**, délégué général de l'Association de lutte contre la piraterie audiovisuelle (ALPA)
- **Général de brigade Éric Freyssinet**, chef du Pôle national de lutte contre les cybermenaces de la Direction générale de la Gendarmerie nationale
- **Alexandra Laffitte**, responsable Contenus à la Fédération française des Télécoms
- **Delphine Sarfati-Sobreira**, directrice générale de l'Union des Fabricants (UNIFAB)
- **Didier Wang**, expert en protection des contenus et lutte contre le piratage à l'Hadopi
- **Général d'armée (2S) Marc Watin-Augouard**, fondateur du Forum international de la cybersécurité

Les opinions exprimées dans ce livre blanc n'engagent ni les personnes précédemment citées, ni les institutions qu'elles représentent.





Forward 

17, avenue Hoche
75008 PARIS

forwardglobal.com