CYBER- CONTREFAÇON :

ÉTAT DES LIEUX

LAURE BOUCHARD

AVOCAT AU BARREAU DE PARIS,
CABINET HOFFMAN

EMMANUELLE HOFFMAN

AVOCAT AU BARREAU DE PARIS, AMCO
CABINET HOFFMAN

La cyber-contrefaçon est une préoccupation contemporaine majeure, qui recouvre des réalités les plus diverses et soulève des questions souvent controversées.

La cyber-contrefaçon désigne premièrement la vente sur Internet de produits réels contrefaisants.

Cela touche tous les secteurs, de la maroquinerie de luxe aux produits pharmaceutiques (selon SANOFI, 94% de la vente de produits médicamenteux sur Internet serait illégale). Cette forme de cyber -contrefaçon représente un danger, que ce soit en termes de santé publique (médicaments), de sécurité (jouets), et d'atteinte aux droits de propriété intellectuelle.

Il s'agit là de contrefaçon « classique », liée le plus souvent au crime organisé, dans laquelle Internet joue ici le rôle de simple vecteur.

La cyber-contrefaçon recouvre aussi d'autres formes d'atteintes cette fois-ci propres à la technologie Internet, qui ne sont pas nécessairement liées à la vente de produits réels contrefaisants.

C'est par exemple le cas du « phishing », cette forme d'escroquerie consistant à conduire les internautes, au moyen d'un courriel frauduleux, à se connecter à un site Internet imitant trait pour trait celui d'une société bien connue et ce, afin d'établir une connexion avec l'ordinateur du consommateur et puiser ainsi ses données, notamment bancaires.

Le faux site (« phisher ») contrefait de nombreux éléments appartenant à la société copiée (marques, identité visuelle...), de sorte que cette pratique constitue bel et bien un acte de contrefaçon de droits de propriété intellectuelle.

Autre pratique contrefaisante propre à Internet, celle du « cybersquatting », qui consiste pour une personne mal intentionnée à réserver des noms de domaine correspondant à des marques, dans un but de spéculation ou dans celui de diriger l'internaute vers des faux produits sur une fausse boutique en ligne imitant celle de la marque faisant l'objet de l'attaque.

Il s'agit là de formes d'atteintes tout à fait inédites et spécifiques à ce media.

On ne peut évoquer également la cyber-contrefaçon sans mentionner le téléchargement ou streaming illégal, bien que ces pratiques n'aient pas tendance à être considérées socialement comme de la cyber-criminalité, à l'inverse des autres exemples mentionnés ci-dessus.

Si le téléchargement ou streaming illégal est plus accepté socialement, il n'en demeure pas moins un problème majeur pour les titulaires de droits, et pour toute l'industrie culturelle.

Aujourd'hui, les tentatives des pouvoirs publics se multiplient à l'échelon national et communautaire pour tenter d'endiguer ces différentes pratiques et défendre les intérêts des titulaires de droits, tout en préservant ceux des consommateurs et ceux des acteurs de l'Internet, étant précisé que ces intérêts sont parfois contradictoires.

En effet, l'intervention du juge et l'instauration d'un contrôle, voire d'une censure sur Internet touche à des problématiques plus globales liées aux libertés fondamentales.

Les outils pour lutter contre la cyber-contrefaçon ont sensiblement évolué ces dernières années, avec des moyens d'action mis en place à chaque étape de la chaîne Internet (titulaire de

droits, intermédiaire, pirate, consommateur) (II), l'accent étant mis sur le rôle des intermédiaires qui assument, de plus en plus, leur part de responsabilité dans ce combat (I).

La cyber-contrefaçon est une problématique vaste, qui touche tous les droits de propriété intellectuelle et soulève des questions juridiques très diverses.

Le présent article ne prétend pas donner une analyse exhaustive de l'ensemble de ces problématiques, mais entend dresser un état des lieux global des réponses juridiques actuellement apportées en France aux problèmes de la contrefaçon sur Internet.

I. Le rôle accentué des intermédiaires

Les intermédiaires de l'Internet (fournisseurs d'accès, moteurs de recherche, plateformes de communication, sociétés de paiement en ligne, annonceurs de publicité en ligne...) sont de plus en plus sollicités dans la lutte contre la cyber-contrefaçon, parce qu'ils jouent un rôle concret dans la diffusion de la contrefaçon sur Internet, mais aussi parce qu'il est plus aisé d'agir avec/ contre de grandes sociétés multinationales solvables que contre des « pirates » à l'identité camouflée.

Ces intermédiaires sont sollicités par la loi et les tribunaux (A), mais jouent aujourd'hui un rôle proactif en mettant en place des outils destinés à lutter contre la contrefaçon (B et C).

A. Une mise à contribution accrue des intermédiaires par le législateur

La responsabilité des intermédiaires de la chaîne Internet a pu paraître à l'origine assez décevante pour les titulaires des droits.

La loi « LCEN » du 21 juin 2004[1], transposant en droit français la Directive 2000/31 du 8 juin 2000[2], a aménagé un régime de responsabilité spécial pour les « *personnes physiques ou morales qui assurent, même à titre gratuit, par mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* ».

Ces intermédiaires se voyaient épargnés d'une mission de contrôle *a priori* des contenus mis en ligne, leur responsabilité ne pouvant être engagée qu'*a posteriori*, à défaut pour eux de retirer des contenus qui leur seraient signalés comme illicites.

La loi dite « LCEN » du 21 juin 2004 a imposé certaines obligations aux intermédiaires techniques : conservation des données d'identification des clients, communication aux autorités judiciaires, et obligation de retrait de contenu illicite.

Cette loi, qui fonde encore aujourd'hui le régime de responsabilité des intermédiaires sur Internet (avec la fameuse dichotomie hébergeurs/ éditeurs de contenus), a donné naissance à la pratique des « notifications LCEN » qui consistent, pour les ayants droits, à notifier aux intermédiaires (type Youtube) la présence d'un contenu illicite, en sollicitant son retrait.

Ce système, qui fonctionne assez efficacement en pratique, est parfois considéré comme un puits sans fond, puisque rien n'empêche aujourd'hui le contenu de réapparaître sur une autre page.

L'intérêt de l'action ciblant le contenu lui-même est par conséquent limité, outre qu'elle représente une tâche considérable pour les titulaires de droits contraints de procéder à un nombre infini de notifications.

Le législateur a donc mis en place un autre outil afin de toucher, non plus seulement le contenu contrefaisant lui-même, mais le site entier abritant des contenus contrefaisants.

La Directive 2001/29[3] mettait déjà l'accent sur cette responsabilité, notamment en son considérant 59 : « *Les services d'intermédiaires peuvent, en particulier dans un environnement numérique, être de plus en plus utilisés par des tiers pour porter atteinte à des droits. Dans de nombreux cas, ces intermédiaires sont les mieux à même de mettre fin à ces atteintes. Par conséquent, sans préjudice de toute autre sanction ou voie de recours dont ils peuvent se prévaloir, les titulaires de droits doivent avoir la possibilité de demander qu'une ordonnance sur requête soit rendue à l'encontre d'un intermédiaire qui transmet dans un réseau une contrefaçon commise par un tiers d'une oeuvre protégée ou d'un autre objet protégé* ».

Le dispositif législatif français a donc été renforcé en 2009[4], avec l'introduction d'une procédure de blocage de sites litigieux abritant massivement du contenu contrefaisant des droits d'auteur (par exemple les sites de streaming permettant l'accès gratuit à un catalogue fourni de films ou séries sans autorisation des titulaires de droits).

L'article L 336-2 ainsi introduit au sein du Code de la propriété intellectuelle dispose que : « *En présence d'une atteinte à un droit d'auteur ou à un droit voisin occasionnée par le contenu d'un service de communication au public en ligne, le tribunal de grande instance, statuant le cas échéant en la forme des référés, peut ordonner à la demande des titulaires de droits sur les oeuvres*

et objets protégés, de leurs ayants droit, des sociétés de perception et de répartition des droits (...) ou des organismes de défense professionnelle (...), toutes mesures propres à prévenir ou à faire cesser une telle atteinte à un droit d'auteur ou un droit voisin, à l'encontre de toute personne susceptible de contribuer à y remédier ».

Cette disposition a donné lieu à un jugement exemplaire rendu le 28 novembre 2013 par le Tribunal de grande instance de Paris[5].

Dans cette affaire, l'association des producteurs de cinéma (APC), la fédération nationale des distributeurs de films (FNDF) et le syndicat de l'édition vidéo numérique avaient assigné, sur le fondement de l'article L 336-2 du Code de la propriété intellectuelle, les sociétés Numéricâble, Orange, France Télécom, SFR, Free, Bouygues Télécom, Darty Télécom et Auchan Télécom pour voir ordonner diverses mesures de nature à empêcher l'accès à partir du territoire français au contenu des sites www.allostreaming.com, www. alloshowtv.com, www. alloshare.com et www.allomovies.com.

Les demandeurs avaient également assigné les sociétés Yahoo Inc., Microsoft corp. Et Google, pour voir ordonner à ces moteurs de recherche de supprimer toutes réponses et résultats renvoyant vers les sites en cause.

Le tribunal a donné raison aux demandeurs en estimant que : « *Ainsi en procurant aux internautes la possibilité de visionner les oeuvres à partir de liens hypertextes présentés sur les sites litigieux, et ce même si les contenus sont stockés auprès de serveurs tiers ou sur des plateformes tierces, ces opérateurs ont procédé à des actes de représentation des oeuvres litigieuses en fournissant la mise à disposition des contenus.* »

Le tribunal a donc ordonné aux fournisseurs d'accès à Internet de mettre en oeuvre toute mesure pour empêcher l'accès à ces sites, notamment en utilisant le blocage de noms de domaine. Parallèlement, le tribunal a condamné les moteurs de recherche à prendre toute mesure pour empêcher l'apparition de réponse renvoyant vers ces pages.

L'application de l'article L 336-2 du Code de la propriété intellectuelle a récemment donné lieu à une nouvelle décision du Tribunal de grande instance de Paris, ayant ordonné aux principaux fournisseurs d'accès à Internet le blocage des sites illicites « The Pirate Bay » pour une durée de douze mois, toujours en laissant le choix des mesures les plus appropriées pour empêcher l'accès à ce site à partir du territoire français[6].

Ces dossiers ont vraisemblablement sollicité un gros travail en amont de la part des titulaires des droits et de leurs conseils pour la démonstration de la matérialité des atteintes, notamment par la multiplication de constats (pas moins de quinze constats d'huissier avaient été versés aux débats dans l'affaire Pirate Bay) destinés à prouver la multitude d'oeuvres contrefaisantes diffusées sur ces sites, et permettant l'identification de toutes les extensions des sites litigieux (dans cette même affaire avaient été identifiés : un site d'origine, dix-huit sites de redirection, trois sites miroirs, cinquante-et-un proxies).

C'est pourquoi ces actions sont majoritairement menées par les sociétés d'auteurs et/ou les syndicats du secteur culturel.

En mai 2014, Madame Mireille IMBERT-QUARETTA, conseillère d'État, a remis à Madame la Ministre de la Culture et de la Communication un rapport intitulé « *Outils opérationnels de prévention et de lutte contre la contrefaçon en ligne* »[7].

Ce rapport propose notamment la création d'une injonction de retrait prolongé, ayant un champ d'application plus restreint que l'article L 336-2 du Code de la propriété intellectuelle, dont le but serait d'éviter la réapparition de contenus supprimés sur demande des titulaires de droits. S'inspirant de dispositifs actifs à l'étranger, cette injonction extrajudiciaire serait prononcée par une autorité administrative à l'encontre d'un site de communication en ligne sur demande d'un titulaire de droits. Elle obligerait le site en question à faire cesser et prévenir, pendant une durée maximale de 6 mois, la réapparition de contenus qui lui auraient été signalés comme constituant une atteinte aux droits d'auteur ou aux droits voisins.

Le caractère limité de cette injonction assurerait sa compatibilité avec le droit communautaire. En effet, l'article 15 de la directive communautaire du 8 juin 2000 interdit aux États membres que soit imposée aux hébergeurs une « *obligation générale de surveiller les informations* » stockées[8].

La Cour de Justice de l'Union Européenne a par la suite précisé que si les États pouvaient prévoir des mesures de filtrage avec l'aide des intermédiaires, celles-ci ne devaient pas avoir pour effet de porter atteinte de façon disproportionnée à la liberté d'entreprendre[9], d'où leur caractère nécessairement limité.

Cette procédure d'injonction, qui viendrait compléter le dispositif législatif existant, a notamment pour but d'éviter aux titulaires de droits de réitérer sans arrêt leurs demandes de retraits

de contenus, et d'empêcher la persistance des contenus contrefaisants.

Le législateur a donc introduit des moyens d'actions permettant aux titulaires de droits d'agir sur les intermédiaires du secteur de l'Internet (plateformes communautaires, fournisseurs d'accès) afin de supprimer certains contenus, voire de bloquer l'accès à des sites entiers.

Les intermédiaires, souvent pointés du doigt, ont pris le parti le plus souvent de devancer les demandes des pouvoirs publics en mettant en place leurs propres outils techniques permettant de lutter contre la cyber-contrefaçon.

B. Les initiatives personnelles des intermédiaires pour lutter contre la cyber -contrefaçon

Les intermédiaires du monde de l'Internet, et notamment les moteurs de recherche ou plateformes de vente en ligne, communiquent abondamment sur leurs propres initiatives techniques dédiées à lutter contre la piraterie en ligne.

Youtube, par exemple, a mis en place un outil dénommé « Content ID », permettant aux internautes mettant régulièrement en ligne du contenu de gérer eux-mêmes ce contenu, en autorisant, limitant, ou prohibant sa reproduction.

Google, quant à lui, publie chaque année son rapport dédié à la lutte contre la contrefaçon[10] et insiste sur sa réactivité quant aux réponses apportées aux notifications qui lui sont adressées par les titulaires de droits.

Le système d'annonce publicitaire « Google Adwords » est particulièrement concerné par les actes contrefaisants.

Cet outil permet d'afficher des liens commerciaux en marge et en haut de la liste des résultats naturels du moteur de recherche Google, à travers l'achat de mots-clefs. Il est utilisé à grande échelle par les pirates pour attirer les consommateurs sur les sites vendant des contrefaçons, en utilisant comme « mot-clef » la marque contrefaite.

Google avait été, un temps, inquiété du fait de cette activité consistant à proposer aux annonceurs des mots-clefs Adwords composés de marques déposées. Il a cependant été jugé que Google ne se rendait pas coupable à travers cette pratique d'actes de contrefaçon de marque[11].

Les annonceurs peuvent donc réserver des marques déposées par des tiers en tant que mot-clef « Adwords » pour proposer leurs propres produits et rediriger l'internaute vers leur propre site.

Toutefois, l'annonceur ne peut bien évidemment pas entretenir de confusion avec les produits de la marque déposée, et rediriger l'internaute vers un site commercialisant des contrefaçons.

Dans de tels cas, Google affirme pratiquer la tolérance zéro et fermer les comptes Adwords renvoyant à des sites de contrefaçons lorsque ceux-ci lui sont signalés.

Google joue alors ici le rôle d'hébergeur qui lui a été reconnu par la jurisprudence pour ce service Adwords[12].

Mais les sites contrefaisants n'apparaissent pas uniquement à travers le service Google Adwords. Ils sont, de fait, référencés naturellement sur le moteur de recherche global de Google.

Google a donc récemment adopté une démarche pour limiter le référencement des sites qui lui seraient signalés comme abritant des contenus contrefaisants.

Google a ainsi mis en place un algorithme permettant de rétrograder naturellement dans les résultats de recherche les sites ayant fait l'objet de notifications trop fréquentes de la part des titulaires de droits.

Plus le site fait l'objet de notifications pour contrefaçon, moins celui-ci sera visible dans les résultats de recherche naturels, le but étant de limiter la fréquentation de ce site et ses revenus.

On pourra constater que ces démarches, si louables soient-elles, sollicitent toujours des actions systématiques et une réactivité accrue des titulaires de droits.

Cette charge pesant sur les titulaires de droits résulte bien entendu de la qualification d'hébergeur retenue presque systématiquement pour les plateformes de partage et autres sites intermédiaires.

Du fait de ce statut, aucune obligation de contrôle *a priori* ne pèse sur ces plateformes qui n'engagent leur responsabilité que si, dès le moment où ils ont eu connaissance du contenu illicite, ils n'agissent pas promptement pour le retirer.

C. « Follow the money »

D'autres intermédiaires sont aujourd'hui sollicités pour lutter contre la cyber-contrefaçon, en vertu de la doctrine « *Follow the money* ».

Face aux difficultés rencontrées pour lutter frontalement contre les pirates d'Internet, il est devenu évident qu'il fallait s'attaquer à leurs ressources financières afin de les assécher et

mettre un terme à leur activité.

Cela concerne principalement les sites de paiement en ligne (type Visa, MasterCard, Paypal) puisque de nombreux sites, notamment en matière de téléchargement, proposent des abonnements aux internautes, ce qui nécessite inévitablement un paiement en ligne, tout comme l'acquisition de produits contrefaisants sur Internet.

Les acteurs de la publicité en ligne sont les autres acteurs concernés, puisque la publicité constitue la source de revenus majeure des sites Internet.

Le rapport précité de Madame IMBERT QUARETTA[13] remis récemment à Madame la Ministre de la Culture et de la Communication rappelle le rôle primordial des acteurs de la publicité et du paiement en ligne dans la lutte contre la cyber-contrefaçon.

Des outils techniques existent afin que les acteurs de la publicité puissent vérifier, par exemple, que la publicité diffusée ne se trouve pas associée à un contenu illégal (filtrage *a priori* ou contrôle *a posteriori*).

Le rapport préconise de se placer, concernant ces acteurs, sur les terrains de l'autorégulation et du droit souple, en soutenant la signature de chartes permettant d'étendre, de formaliser et de systématiser le recours à des actions techniques permettant de lutter contre la contrefaçon sur Internet.

L'idée serait de confier à une autorité publique (qui pourrait être par exemple la HADOPI, Haute Autorité pour la diffusion des oeuvres et la protection des droits sur Internet) la mission de recouper des informations sur l'activité d'un site. En cas d'activité massivement contrefaisante, les acteurs du paiement en ligne et de publicité en ligne pourraient être informés et sollicités afin de prendre des mesures volontaires, « *allant du simple rappel des obligations contractuelles jusqu'à la rupture du contrat* ».

Avec cet autre type d'intermédiaires, la démarche est donc moins directe qu'avec les fournisseurs d'accès ou les plateformes communautaires, même si leur rôle est aujourd'hui tout aussi important dans la chaîne de la cyber-contrefaçon.

Les intermédiaires ont beau être en première ligne de la lutte anti-contrefaçon sur Internet, du moins devant les tribunaux, les actions menées directement contre les cyber-contrefacteurs n'en sont pas moins cruciales.

II. Une lutte laborieuse conte les cyber-contrefacteurs

La responsabilisation et la condamnation des auteurs directs de la cyber-contrefaçon ne sont pas pour autant délaissées, loin de là (A).

La justice et les services de l'État redoublent d'efforts pour tenter de retrouver et sanctionner les auteurs de piraterie sur Internet (B), même si cette lutte s'avère difficile dans un univers où la dissimulation et l'éphémère sont rois.

Enfin, il ne faut pas oublier les consommateurs, qui parfois eux aussi sont responsables de cyber-contrefaçon, que ce soit à travers l'acquisition de produits contrefaisants sur Internet ou du fait d'un téléchargement de contenu illégal (C).

A. Des « pirates » sanctionnés sur le fondement du Code de la propriété intellectuelle

La contrefaçon sur Internet est sanctionnée, au même titre que la contrefaçon « classique », sur le fondement du Code de la propriété intellectuelle, que ce soit par les juridictions civiles ou pénales.

La voie pénale est d'ailleurs souvent négligée, notamment du fait d'un certain désintérêt des juridictions pénales pour les problématiques liées à la contrefaçon.

Sur ce terrain, une sensibilisation et une spécialisation sont souhaitables, les pouvoirs d'enquête ainsi que les sanctions pénales pouvant être d'une grande efficacité dans la lutte contre les réseaux mafieux de cyber-contrefaçon.

Les textes actuels peuvent aisément s'appliquer à ces nouvelles formes de contrefaçon, sans qu'il soit nécessairement besoin de produire un arsenal législatif spécifique.

C'est le cas notamment du « phishing » et du « cybersquatting » qui étaient évoqués en introduction, et que la jurisprudence a déjà eu l'occasion de sanctionner sur le fondement du Code de la propriété intellectuelle.

En ce qui concerne le phishing, les décisions de justice demeurent rares, sans doute du fait des difficultés rencontrées pour identifier les auteurs de telles attaques.

En 2005, la 31ème chambre du Tribunal de grande instance de Paris a eu l'occasion de condamner une personne poursuivie pour avoir réalisé sur un site Internet personnel une imitation de la page de connexion à Microsoft MSN messenger, sur laquelle les personnes étaient invitées à livrer leurs données personnelles, récoltées par email par le prévenu[14].

La société Microsoft corporation s'était portée partie civile.

Toutefois, la peine prononcée fut modeste (500 euros d'amende

avec sursis et 700 euros de dommages-intérêts), le tribunal ayant relevé que le dispositif était de mauvaise qualité, que le dossier ne démontrait pas que des données personnelles avaient effectivement été frauduleusement obtenues, que le site avait rapidement fermé, et que les faits n'avaient donc que modestement porté atteinte aux intérêts de la société Microsoft.

Le cybersquatting fait quant à lui l'objet de condamnations plus abondantes et plus sévères.

En pratique, face à un cybersquatting, les titulaires de droits préfèrent oeuvrer en vue du transfert du nom de domaine à leur profit, à travers une procédure UDRP (procédure non contentieuse devant l'OMPI). Cependant, de telles procédures ne permettent pas de sanctionner directement l'auteur du cybersquatting.

L'exercice d'une procédure judiciaire peut toutefois se révéler plus efficace, notamment d'un point de vue dissuasif.

En 2010, le Tribunal de grande instance de Paris a condamné, à la demande de la SNCF, un cybersquatteur qui avait enregistré les noms de domaine sncfu-sa.com et eurotgv.org, pour contrefaçon de marque, atteinte au nom de domaine et pratiques commerciales trompeuses[15].

Le tribunal avait alors précisé qu'il importait peu que le site litigieux ait ou non été exploité, « *dès lors que le simple enregistrement du nom de domaine imitant une marque notoire suffisait à engager la responsabilité de son auteur* ».

Outre des mesures d'interdiction, une condamnation de 20 000 euros à titre de dommages-intérêts fut prononcée à l'encontre du défendeur.

Même chose pour le cybersquatting de la marque Chérie FM. Un contrefacteur avait réservé les noms de domaine cherihd.net, cherie-hd.com, cherie-hd.net, cheriehd.fr et cherie-hd.fr, deux jours après la publication d'un communiqué de presse du groupe NRJ relatif au lancement de la chaîne CherieHD. Ces noms de domaine étaient exploités via des pages parking, puis proposés aux enchères.

Là encore, la contrefaçon de marque fut reconnue par le Tribunal de grande instance de Nanterre dans un jugement du 28 juin 2012, en même temps que l'atteinte à la dénomination sociale, au nom commercial et à l'enseigne[16]. Le contrefacteur fut condamné à verser la somme de 6 000 euros à titre de dommages intérêts.

La condamnation des auteurs de contrefaçon commise via Internet est donc possible sur le fondement de l'actuel Code de la propriété intellectuelle.

Cependant, les difficultés résident souvent dans l'appréhension de l'identité du contrefacteur et de la source de la contrefaçon.

B. La « traque » des cyber-contrefacteurs, une difficulté majeure

Sites hébergés à l'étranger dans des paradis numériques, adresses IP masquées, darknet, réseaux sociaux, sites éphémères... autant d'obstacles à ce que les titulaires de droits, victimes d'une contrefaçon sur Internet, puissent remonter à la source de la contrefaçon et agir efficacement afin de faire cesser les actes litigieux.

Les réseaux de cyber-contrefaçon sont souvent structurés autour de sites satellites éphémères, qui ramènent vers les têtes de réseaux où le paiement est effectué. Or, il est extrêmement difficile de remonter jusqu'à la tête de réseau, et la durée de vie des sites satellites est quant à elle extrêmement courte (37 jours en moyenne).

Ces structures et leur rapidité d'évolution sont en décalage avec la temporalité de la justice.

Les pouvoirs publics tentent aujourd'hui de s'adapter à cette réalité, notamment à travers la cellule Cyberdouane auprès de qui les titulaires de droits peuvent déposer des dossiers afin de déclencher une veille des services sur le réseau Internet.

La gendarmerie forme également des enquêteurs spécialisés en cyber-criminalité pour tenter de remonter ces réseaux.

Les services publics et le secteur privé doivent oeuvrer ensemble pour combattre la cyber-contrefaçon.

De nombreuses initiatives existent déjà en ce sens, comme le service «Digital Crime Unit » de Microsoft, qui travaille avec le FBI pour identifier des attaques Internet et les combattre.

L'opération PANGEA dans le domaine de la contrefaçon de médicament est également un exemple à suivre, puisque cette coopération ponctuelle entre Interpol, les douanes, et des entreprises privées du monde entier du secteur pharmaceutique aboutit à chaque fois à la fermeture de plusieurs milliers de sites Internet.

Les services qui participent à la lutte contre la cyber-contrefaçon doivent aujourd'hui coopérer avec des experts techniques formés spécifiquement sur ces problématiques.

De telles entités existent déjà en France, et on ne peut qu'encourager leur développement face à l'ampleur du phénomène.

C. Les consommateurs, cyber-contrefacteurs ?

On ne peut envisager la notion de cyber-contrefacteur sans questionner le rôle et la responsabilité du consommateur. En effet, le consommateur, comme pour la contrefaçon classique, est lui aussi contrefacteur lorsqu'il acquiert un produit contrefaisant sur Internet.

La consommation de produits contrefaisants se trouve facilitée, voire banalisée lorsqu'elle est faite au travers d'un site Internet.

Or, l'acquisition et la détention d'un produit contrefait constituent en soi des actes de contrefaçons punis par la loi (3 ans d'emprisonnement et 300 000 euros d'amende[17]) et ces achats peuvent être interceptés dans le cadre de contrôles douaniers.

Un travail de sensibilisation et de responsabilisation des consommateurs est donc nécessaire.

Mais le consommateur contrefacteur est aussi celui qui télécharge ou échange des oeuvres illégalement.

La loi HADOPI a introduit au sein du Code de la propriété intellectuelle un article L 336-3 qui dispose que : *« La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'oeuvres ou d'objets protégés par un droit d'auteur ou par in droit voisin sans l'autorisation des titulaires de droits prévus aux livres Ier et II lorsqu'elle est requise ».*

Le défaut de surveillance de son réseau est sanctionné à travers le dispositif de la « réponse graduée » appliquée par la HADOPI.

Le choix du législateur s'est donc porté sur une vraie responsabilisation du consommateur, pour combattre le fait que ce type de comportement contrefaisant était, et est toujours, socialement accepté malgré l'atteinte manifeste aux droits de propriété intellectuelle.

A l'heure actuelle, l'avenir de ce dispositif et de la HADOPI est incertain.

Le dernier rapport annuel publié par la HADOPI fait mention, au 30 juin 2014, de 3 249 481 premières recommandations adressées à des internautes, ayant abouti à 116 transmissions au procureur de la République[18].

Dans un entretien accordé le 28 janvier 2015, la Ministre de la Culture et de la Communication, Fleur Pellerin, affirmait que HADOPI continuait de *« mettre en oeuvre la réponse graduée, mission qu'elle a les moyens d'assurer pleinement »*[19].

La ministre concédait cependant vouloir mettre davantage l'accent sur le développement de l'offre légale, ainsi que sur le rôle des intermédiaires.

Il semble donc que ce système soit amené à perdurer pour l'instant, ce que souhaitent les titulaires de droits qui jugent positive l'action menée par la HADOPI.

Conclusion

Si de nombreux outils ont déjà été mis en place, des efforts doivent encore être faits pour assurer l'efficacité de la lutte contre la contrefaçon sur Internet et la protection des droits de propriété intellectuelle.

La tendance contemporaine pour endiguer la cyber-contrefaçon est à la coopération : coopération inévitable avec les intermédiaires de tous types, qui possèdent un pouvoir concret et des outils techniques, mais coopération également entre les pouvoirs publics et les entreprises du secteur privé afin de mettre en place des process de pointe pour remonter les réseaux et identifier les sources de la cyber -contrefaçon.

La limite à cette action d'ampleur mondiale réside dans le respect des libertés individuelles, qui sont évidemment menacées chaque fois que se ressent le besoin pour les pouvoirs publics de contrôler plus sévèrement les contenus mis en ligne.

Notes :

1 Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

2 Directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique dans le marché intérieur

3 Directive 2001/29/CE du Parlement européen et du conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information

4 Loi n°2009-669 du 12 juin 2009, dite « HADOPI I »

5 TGI Paris 28 novembre 2013, RG n° 11/60013

6 TGI Paris 4 décembre 2014, The Pirate Bay

7 « Outils opérationnels de prévention et de lutte contre la contrefaçon en ligne », Rapport à Madame la ministre de la culture et de la communication, Mireille IMBERT-QUARETTA, conseillère d'Etat, Mai 2014

8 Voir note 2 supra

9 CJUE 24 novembre 2011 aff. C70/10 et CJUE 16 février 2012 aff. C 360-10

10 « How Google Fights piracy », dernier rapport publié le 17 octobre 2014

11 CJUE 23 mars 2010, aff. C 236/08 à C 238/08 et en France CA Paris, Pôle 5 Chambre 2, 19 novembre 2006 ; CA Paris, Pôle 2 Chambre 7, 11 décembre 2013 ; CA Paris Pôle 5 Chambre 1, 9 avril 2014, RG n° 13/05025

12 Voir note 11 supra

13 Voir note 7 supra

14 TGI Paris 31ème chambre /2, 21 septembre 2005

15 TGI Paris 3ème chambre, 2ème section, 29 octobre 2010, Sncf / Benoît M.

16 TGI Nanterre 28 juin 2012, Chérie FM./ Mohamed E.

17 Articles L 335-2, L 521-10 et L 716-10 du Code de la propriété intellectuelle

18 HADOPI, Rapport annuel 2013/2014

19 Les Echos, 28 janvier 2015