

Comité consultatif sur l'application des droits

Douzième session
Genève, 4 – 6 septembre 2017

MÉCANISMES INSTITUTIONNELS ASSOCIÉS AUX POLITIQUES ET SYSTÈMES D'APPLICATION DES DROITS DE PROPRIÉTÉ INTELLECTUELLE DANS LE DOMAINE DE LA LUTTE CONTRE LES ATTEINTES À LA PROPRIÉTÉ INTELLECTUELLE COMMISES EN LIGNE

Contributions établies par l'Italie, la République de Corée, le Royaume-Uni, la Thaïlande, Europol et la Motion Picture Association of America, Inc.

1. À sa onzième session, le Comité consultatif sur l'application des droits (ACE) est convenu de poursuivre l'examen du thème suivant : "échange de données d'expérience nationales relatives aux mécanismes institutionnels associés aux politiques et systèmes d'application des droits de propriété intellectuelle, notamment les mécanismes permettant de régler les litiges de propriété intellectuelle d'une manière équilibrée, globale et efficace".

2. Le présent document contient les contributions établies par quatre États membres (Italie, République de Corée, Royaume-Uni et Thaïlande), un autre membre et une organisation ayant le statut d'observateur, relatives aux mécanismes d'application des droits visant à freiner la croissance du commerce en ligne de produits portant atteinte à des droits de propriété intellectuelle et notamment à lutter contre l'anonymat des auteurs de ces atteintes, la rapidité avec laquelle ces atteintes sont commises et le caractère transnational de ces atteintes. Les mécanismes examinés prévoient la création de services de police spécialisés, des enquêtes fondées sur les connaissances, des plateformes informatisées facilitant le suivi en ligne et la collecte de données, l'application de la méthode consistant à "suivre la piste de l'argent" pour contrôler les mouvements d'argent liquide, le blocage de sites Web, le ciblage des noms de domaine portant atteinte à des droits de propriété intellectuelle, des mesures volontaires et le renforcement de la coopération transfrontière entre les autorités chargées de l'application de la loi, les titulaires de droits et les intermédiaires en ligne.

3. Ces contributions, qui émanent des services de police (nationaux et régionaux), d'un office de propriété intellectuelle, du Ministère public, du pouvoir judiciaire et de titulaires de droits, témoignent des enjeux liés à l'application des droits de propriété intellectuelle en ligne et à la multiplicité des acteurs intervenant dans l'application des droits de propriété intellectuelle en ligne, et du besoin correspondant de renforcer la collaboration pour lutter contre ces atteintes qui, souvent, ont un caractère transnational. Ces contributions soulignent l'importance d'adopter une démarche commune et globale et de promouvoir le respect de la propriété intellectuelle.

4. Les contributions sont présentées dans l'ordre suivant :

Expérience de l'Italie en matière de lutte contre les atteintes aux droits de propriété intellectuelle sur l'Internet	3
Mécanismes institutionnels mis en place en République de Corée pour mettre un terme à la prolifération des produits contrefaisants en ligne	12
Difficultés rencontrées dans l'instruction des atteintes portées en ligne à la propriété intellectuelle : point de vue du bureau du Procureur général en Thaïlande	19
Ordonnances de blocage de sites Web : l'expérience du Royaume-Uni	25
Mécanismes institutionnels mis en place pour lutter contre les atteintes à la propriété intellectuelle commises en ligne – données d'expérience d'Europol	31
Mesures volontaires intersectorielles pour lutter contre le piratage en ligne	37

[Les contributions suivent]

EXPÉRIENCE DE L'ITALIE EN MATIÈRE DE LUTTE CONTRE LES ATTEINTES AUX DROITS DE PROPRIÉTÉ INTELLECTUELLE SUR L'INTERNET

*Contributions établies par M. Vincenzo Tuzi, colonel chargé de l'unité spéciale de protection de la propriété intellectuelle, Guardia di Finanza, et M. Stefano Vaccari, directeur de l'Inspection générale chargée de la protection de la qualité et de la répression des fraudes au Département des produits agroalimentaires, Ministère des politiques agricoles, alimentaires et forestières, Rome (Italie)**

RÉSUMÉ

Chargée de l'application de la loi en Italie, la Guardia di Finanza est un corps de police doté d'une structure militaire et de compétences spécifiques dans les domaines économique et financier en vertu de pouvoirs spéciaux conférés par la loi. Elle prône une coopération étroite en vue de réduire notablement les quantités de produits de contrefaçon qui circulent en Italie et dans l'Union européenne. En 2014, la Guardia di Finanza a créé le système d'information anticontrefaçon (SIAC), qui comprend une plateforme technologique intégrée composée d'une base de données contenant des informations historiques et statistiques ainsi que des illustrations, des documents, des renseignements et des références utiles sur les marques et les produits, rassemblés à des fins opérationnelles concrètes. Pratiquement terminée, l'application dédiée *Contraffazione Online Brand Library (COLIBRI)* favorisera une action répressive plus ciblée contre les atteintes aux droits de propriété intellectuelle sur l'Internet, qui constitue désormais la "nouvelle frontière" de la contrefaçon.

La contrefaçon sur le Web et via les réseaux sociaux est l'une des plus importantes menaces qui pèsent sur la pérennité des droits de propriété intellectuelle. Coopérer avec les titulaires de droits de propriété intellectuelle est le moyen le plus efficace pour relever ce défi. Une plus grande collaboration est également nécessaire avec ceux qui œuvrent dans le domaine des paiements électroniques afin d'explorer le potentiel de l'approche consistant à "suivre l'argent". Il serait en outre souhaitable de multiplier le nombre d'opérations sous couverture, telles les simulations d'achat.

L'Inspection générale chargée de la protection de la qualité et de la répression des fraudes au Département des produits agroalimentaires (ICQRF) est l'autorité compétente du Ministère des politiques agricoles, alimentaires et forestières pour la prévention et la répression des fraudes relatives aux produits agroalimentaires. En 2016, elle a effectué plus de 48 000 inspections et analyses, examinant 53 427 produits et contrôlant 25 190 producteurs.

Des réponses utiles aux questions relatives à la multiplication des atteintes à la propriété intellectuelle commises en ligne ont été fournies par l'ICQRF qui travaille en vue d'améliorer l'efficacité des instruments de réglementation de l'Union européenne et crée de nouveaux modes d'action grâce à la coopération entre les parties et à la mise en œuvre de mémorandums d'accord relatifs à la protection des appellations d'origine protégées (AOP) et des indications géographiques protégées (IGP), conclus avec des plateformes de commerce électronique de premier plan comme eBay, Alibaba et Amazon.

* Les points de vue exprimés dans le présent document sont ceux de l'auteur et ne reflètent pas nécessairement ceux du Secrétariat ou des États membres de l'OMPI.

I. L'EXPÉRIENCE DE LA GUARDIA DI FINANZA

A. FAITS ET CHIFFRES

1. Selon les données officielles des instituts de sondage, le chiffre d'affaires de "l'industrie de la contrefaçon" en Italie se monte à près de sept milliards d'euros. Une enquête de la Fondation CENSIS, réalisée pour le compte de la Direction générale de la lutte contre la contrefaçon de l'Office italien des brevets et des marques, sous l'égide du Ministère du développement économique, a estimé que la contrefaçon représentait quelque 6,9 milliards d'euros de manque à gagner, soit presque 2% des recettes totales de l'État¹.
2. Les résultats obtenus des actions en matière d'application des droits menées par la Guardia di Finanza² et les autres forces de police ont fait ressortir deux particularités qui caractérisent les tendances évolutives de l'industrie de la contrefaçon.
3. La première est que le marché de la contrefaçon a connu, ces dernières années, une croissance exponentielle, les saisies de produits contrefaisants ou dangereux effectuées par la Guardia di Finanza passant de 90 millions en 2006 à plus de 393 millions en 2015.
4. La seconde particularité est la diversification notable des produits de contrefaçon, lesquels ne se limitent plus aujourd'hui aux produits de luxe ou aux articles haut de gamme, généralement dans le secteur de l'habillement, mais touchent désormais aussi les biens de grande consommation les plus variés. L'aspect le plus alarmant du phénomène est l'augmentation du nombre de saisies de produits dangereux pour la santé des acheteurs ou susceptibles de compromettre la sécurité publique : cela concerne tout particulièrement les jouets, les produits destinés aux enfants et les médicaments.
5. Dans ce contexte global, on ne peut que constater le vif intérêt et l'ingérence croissante du crime organisé, tant sur le marché national qu'à l'étranger, étant donné le fort potentiel de rentabilité de l'industrie de la contrefaçon.
6. Rien qu'en 2015, 9416 particuliers ont été dénoncés à l'autorité judiciaire. La moitié des sujets suspectés de contrefaçon sont Italiens (52,34% pour être précis). En outre, plus de 11 000 opérations d'application des droits ont permis de saisir plus de 393 millions de produits.
7. De nombreuses études confirment également que l'Internet doit être considéré à juste titre comme la "nouvelle frontière" de la contrefaçon et du piratage, en raison principalement de son incroyable facilité d'accès, de la vitesse des transactions en ligne et de la garantie d'un réel anonymat pour les fournisseurs et les clients. Ces trois dernières années, la Guardia di Finanza a placé sous séquestre plus de 5000 sites Internet.
8. Compte tenu de l'ampleur du problème de la contrefaçon et de l'évolution alarmante du phénomène, il importe d'ancrer l'action dans la coopération internationale et la collaboration interinstitutionnelle. Dans cette optique, une importante plateforme multiagence a été créée

¹ "Dimensioni, caratteristiche e approfondimenti sulla contraffazione" (Ampleur, caractéristiques et analyse approfondie du phénomène de la contrefaçon) – rapport final 2012 de la Fondation CENSIS – <http://www.uibm.gov.it/attachments/Dimensioni%2c%20caratteristiche%20e%20approfondimenti%20sulla%20contraffazione%20-%20Rapporto%20finale%20%282012%29.pdf>.

² Il convient de relever les particularités du mode de fonctionnement de la Guardia di Finanza, qui se distingue par l'utilisation de modules "pluridisciplinaires" au sein desquels des pouvoirs multiples sont exercés conjointement : 1) police criminelle, lorsque l'activité est engagée par délégation du pouvoir judiciaire ou d'une autre façon, même si elle a été lancée à son initiative, pour conduire ensuite à l'identification d'une affaire relevant du droit pénal; 2) police fiscale, chargée d'enquêter sur les violations de la législation fiscale; 3) police administrative, chargée de vérifier les atteintes administratives.

en 2004 à la Direction centrale de la police criminelle qui dépend du Ministère des affaires intérieures. Elle a conduit à un échange systématique entre les experts de la Guardia di Finanza, l'Arma dei Carabinieri et les services de la police d'État, réunis dans un groupe de travail auquel participent également l'Association nationale des communes d'Italie (ANCI) et la Société italienne des auteurs et éditeurs (SIAE). On a par ailleurs renforcé les réseaux de coopération existants avec la Direction générale de la lutte contre la contrefaçon de l'Office italien des brevets et des marques (UIBM), sous l'égide du Ministère du développement économique, et avec le Conseil national anticontrefaçon (CNAC).

9. D'autre part, le Ministère du développement économique a publié un rapport détaillé de propriété intellectuelle portant sur les enquêtes menées dans le domaine de la contrefaçon (projet IPERICO)³, une base de données intégrée qui rend compte des activités anticontrefaçon.

10. Le dispositif de lutte contre la contrefaçon mis en place par la Guardia di Finanza comporte trois axes distincts.

11. La première ligne de défense est la surveillance des espaces douaniers par des officiers de la Guardia di Finanza en vue d'intercepter les trafics illicites de produits contrefaisants et dangereux en provenance de pays non membres de l'Union européenne avant que ces marchandises ne fassent leur apparition sur les marchés nationaux. Cette mesure à elle seule ne suffit pas à faire échec à l'industrie de la contrefaçon car, vu le volume considérable des échanges, seulement 10% des marchandises importées font l'objet d'un contrôle douanier.

12. Le deuxième axe de défense est le contrôle économique systématique du territoire, exercé dans la rue par nos patrouilles qui se coordonnent et collaborent avec les autres forces de police et les polices locales, afin d'opposer une réponse rapide et diffuse au petit trafic et aux ventes de détail illicites.

13. La troisième ligne de défense prend appui sur les activités d'enquête proprement dites menées par les brigades de la police fiscale, qui visent non à saisir les produits sur le lieu de vente au public mais plutôt à remonter, grâce à des activités de renseignement efficaces et unifiées, toute la filière de distribution des contrefaçons afin d'identifier les canaux d'importation, les sites de production illégale, les zones de stockage et les principaux réseaux de distribution des produits contrefaisants. C'est le volet le plus distinctif de l'action de la Guardia di Finanza en matière d'application des droits, qui permet de lever le voile derrière lequel les organisations criminelles s'abritent pour dissimuler les coupables, les recettes de leurs activités illicites et les réinvestissements qui en découlent. L'activité d'enquête permet aussi de localiser les sites d'assemblage des produits contrefaisants.

14. Les fonctions de police économique et financière rendent possible une approche interdisciplinaire indispensable pour s'attaquer à ces formes d'activités illégales. La dimension transversale est toujours présente dans le domaine de la contrefaçon et seule une vision globale, garantie par une combinaison synergique alliant analyse des risques, contrôle du territoire et enquêtes, permet d'obtenir des résultats à plus large échelle, efficaces et durables.

B. LA CONTREFAÇON SUR L'INTERNET

15. La contrefaçon sur l'Internet et via les réseaux sociaux est devenue insidieuse et dangereuse à de nombreux égards. Les personnes impliquées dans des activités de contrefaçon via les réseaux sociaux sont aussi bien des ménagères que des étudiants

³ IPERICO (Intellectual Property – Elaborated Report of the Investigation on Counterfeiting), <http://www.uibm.gov.it/iperico/home/>.

universitaires ou des chômeurs. Toutes les classes sociales et professions sont touchées, même si les jeunes sont plus concernés. On observe un comportement souvent ambivalent à l'égard de l'acquisition de biens illicites, les acheteurs pouvant se muer facilement en vendeurs et vice-versa.

16. Concernant les chaînes d'approvisionnement de biens illicites donnés, deux systèmes de stockage principaux ont été recensés. Le premier est propre aux vendeurs de rue ou à la sauvette, qui proposent des articles de mauvaise qualité et disposent d'un stock de marchandises contrefaisantes limité. Dans ce cas de figure, les revenus sont très faibles. Le second est caractéristique des vendeurs sur l'Internet, qui proposent des produits de meilleure qualité et ont un potentiel de revenu supérieur grâce à une plus grande capacité de stockage.

17. S'agissant de la contrefaçon via les réseaux sociaux, la Guardia di Finanza a coutume de gérer les achats en s'appuyant sur ses services de renseignement ou grâce aux informations fournies directement par le titulaire du droit de propriété intellectuelle. Nous sommes fermement convaincus de l'utilité de coopérer avec les titulaires de droits de propriété intellectuelle pour toutes les questions relatives à l'application des droits. Cela a abouti à la création, en 2014, d'un réseau spécial en ligne – le système d'information anticontrefaçon (SIAC) – au sein duquel toutes les sociétés enregistrées peuvent échanger des informations sur leurs droits de propriété intellectuelle.

18. Ces informations en ligne peuvent être utilisées par toutes les brigades territoriales de la Guardia di Finanza pour améliorer les résultats des activités de lutte contre la contrefaçon et le piratage. Deux procédures différentes peuvent être suivies, alternativement ou conjointement. L'une est ouverte auprès de l'autorité italienne en matière de concurrence (antitrust), l'autre engagée par l'autorité judiciaire. Dans les deux cas, les enquêtes permettent de fermer des sites Web, d'identifier toutes les personnes impliquées, de surveiller les mouvements financiers ("suivre l'argent"), de "remonter la piste de l'hébergeur" et de prendre des mesures financières à des fins pénales ou fiscales.

19. En "suivant l'argent", nous pouvons retracer et couper le soutien financier au piratage et à la contrefaçon en ligne en reconstituant les mouvements de fonds. Nous avons par ailleurs mis en place une nouvelle stratégie d'enquête consistant à "suivre l'hébergeur". Dès qu'un site opérant de manière illégale est repéré, cette méthode permet aux agents d'exiger des fournisseurs qu'ils vérifient l'existence d'une ou plusieurs infrastructures d'hébergement de sites Web dédiés, services VPS, cloud et de serveur. Il est ainsi possible de lever l'anonymat des services pour identifier l'acteur responsable d'un domaine qui se livre à des transactions illégales.

20. Nous gérons toutes les informations (numéros de téléphone, sites Web, adresses électroniques, personnes et sociétés identifiées, informations financières) relatives à la contrefaçon via les réseaux sociaux. Au terme d'une enquête approfondie, des mandats de perquisition peuvent être délivrés par l'autorité judiciaire aux fins d'autoriser des investigations plus poussées dans des cas précis. Il peut s'agir d'opérer une perquisition domiciliaire, de réaliser des enquêtes économiques et financières, de procéder à l'analyse des preuves informatiques ou d'effectuer des recherches sur des comptes bancaires et postaux. Cela permet d'établir un rapport complet en vue de résoudre une affaire. L'approche consistant à "suivre l'argent" est particulièrement utile pour recueillir ces informations. Préalablement ou parallèlement à ce processus, il est possible de mener des opérations sous couverture – en particulier des simulations d'achat – en coopération avec les titulaires de droits de propriété intellectuelle. L'avantage de cette approche est qu'elle permet notamment de recueillir des informations utiles comme l'origine des biens illicites, l'identité de l'expéditeur et le fonctionnement du système de paiement. Les études de cas semblent suggérer que les

contrefacteurs pratiquent la “méthode du stock zéro”, ce qui limite les chances de découvrir d’importants stocks de produits contrefaisants suite à une perquisition.

21. Les études de cas montrent que les contrevenants prennent des précautions. Ils changent, par exemple, tous les deux ou trois mois de numéros de téléphone et utilisent les réseaux sociaux uniquement pour établir le premier contact avec les clients. Ils passent ensuite à des modes de communication codés, plus difficiles d’accès pour les forces de l’ordre. Les produits illicites sont souvent acheminés par la poste, les paiements étant généralement effectués en monnaie virtuelle. Tout semble indiquer le déploiement de stratégies plus subtiles, telle l’utilisation de systèmes de paiement en espèces à la livraison, qui rendent le traçage des paiements plus difficile.

22. Une étude de cas qui illustre bien le problème de la contrefaçon via les réseaux sociaux est celle qui relate le cas, survenu récemment en Sicile, d’un jeune couple approchant de la trentaine qui vendait des produits horlogers haut de gamme contrefaisants via un profil sur un réseau social. En l’espace de trois ans, la vente de montres de contrefaçon a rapporté à ses auteurs plus de 750 000 euros, somme qui leur a permis d’acheter une voiture de luxe et de monter une société-écran afin de procéder à l’autoblanchiment de l’argent provenant du trafic illicite.

C. L’APPROCHE GLOBALE DANS LE CADRE DU SIAC

23. Cofinancé par la Commission européenne, le projet SIAC a été confié par le Ministère des affaires intérieures à la Guardia di Finanza, confirmant le rôle central de cette dernière dans ce secteur opérationnel particulier.

24. La Guardia di Finanza est consciente de la nécessité de mettre en place un système global et coordonné entre toutes les composantes institutionnelles et tous les acteurs engagés dans la lutte contre l’industrie de la contrefaçon et du piratage. L’initiative est née de la reconnaissance du fait que, pour faire face à un phénomène illicite multidimensionnel et transversal comme la contrefaçon, il est indispensable que toutes les parties concernées unissent leurs forces.

25. Sur cette base, le projet a été conçu sous la forme d’une plateforme télématique multifonctionnelle comportant plusieurs applications investies des fonctions suivantes :

- fournir des informations aux consommateurs concernant la lutte contre la contrefaçon et le piratage;
- favoriser la coopération entre les acteurs institutionnels, en particulier entre les forces de police, y compris la police municipale; et
- favoriser la coopération entre les acteurs institutionnels et les entreprises privées.

26. Le SIAC s’appuie avant tout sur un site Web qui présente un état actualisé des actions menées par les divers organismes institutionnels chargés de surveiller le marché de la contrefaçon et du piratage, livrant aux utilisateurs des suggestions et des conseils pratiques pour éviter d’acheter des produits de contrefaçon ou dangereux. Le système permet aussi aux titulaires de droits de propriété intellectuelle de participer activement aux actions préventives et répressives en communiquant des informations sur leurs propres produits touchés par la contrefaçon – illustrations, fiches d’information, expertises, conseils techniques ou autres – que les brigades territoriales opérant sur le terrain pourront consulter facilement.

27. Il est prévu également d’intégrer au projet une plateforme informatisée réservée à la Guardia di Finanza et aux autres forces de police (y compris la police municipale). Cette plateforme offrira des modalités innovantes de collecte de données et rassemblera tous les

résultats opérationnels afin de garantir une analyse plus efficace et rapide des informations qui présentent un intérêt pour l'enquête.

28. Évoquons pour terminer l'application spéciale du nom de COLIBRI (Contraffazione Online Brand Library, soit une bibliothèque en ligne consacrée à la contrefaçon de marques), qui est en cours de réalisation et permettra une action plus ciblée de lutte contre la contrefaçon et le piratage sur l'Internet, qui constitue aujourd'hui, à tous points de vue, la "nouvelle frontière" de la contrefaçon.

II. EXPÉRIENCE DE L'INSPECTION GÉNÉRALE CHARGÉE DE LA PROTECTION DE LA QUALITÉ ET DE LA RÉPRESSION DES FRAUDES AU DÉPARTEMENT DES PRODUITS AGROALIMENTAIRES (ICQRF)

29. Les plateformes de commerce électronique (comme eBay, Alibaba et Amazon), les réseaux sociaux (Facebook, Instagram, WeChat, etc.) et les sites Web classiques ont considérablement accru les possibilités de commercialisation pour des millions de producteurs et des milliards de consommateurs. Dans le secteur agroalimentaire, la croissance à l'échelle mondiale du commerce électronique a révolutionné le marché en permettant à des petits producteurs italiens d'atteindre des marchés éloignés. La forte attraction exercée partout dans le monde par la mention "fabriqué en Italie" a manifestement incité des producteurs d'autres pays à proposer des produits évoquant l'Italie ou usurpant cette origine, sous des dénominations qui sont protégées ou qui évoquent clairement une fausse origine italienne.

30. Des études récentes montrent que près de 3 milliards de personnes dans le monde utilisent l'Internet, dont environ 1,2 milliard achètent des articles en ligne. En 2015, les ventes en ligne de produits et services se sont élevées à 1671 milliards de dollars É.-U., représentant environ 7,4% du volume global des ventes au détail – soit une augmentation de 350 milliards de dollars É.-U. par rapport à l'année précédente. D'après les estimations, ces chiffres devraient plus que doubler d'ici 2019 et atteindre 3578 milliards de dollars É.-U., soit 12,8% du volume des ventes au détail à l'échelle mondiale.

31. L'Inspection générale chargée de la protection de la qualité et de la répression des fraudes au Département des produits agroalimentaires (ICQRF) compte environ 800 services, 29 bureaux en Italie et six laboratoires d'analyse qui sont tous agréés par l'Union européenne. Elle a également un pouvoir de sanction pour les infractions administratives dans le domaine agroalimentaire, elle joue un rôle fondamental dans la lutte contre les infractions dans ce secteur et réalise de nombreuses enquêtes pénales sur délégation des autorités judiciaires italiennes.

32. Dans le cadre de ses activités de contrôle, l'ICQRF dispose d'un programme d'action spécifique relatif au "contrôle du commerce électronique des produits alimentaires réglementés" ayant pour objet de protéger les consommateurs et les commerçants contre la concurrence déloyale grâce à la vérification des sites Web et des informations qu'ils contiennent sur la commercialisation des denrées alimentaires. Les contrôles portent sur les ventes sur l'Internet et toutes les formes de communication visant à promouvoir directement ou indirectement des produits agroalimentaires sur le Web.

33. Une attention particulière est accordée à la protection des produits de qualité au moyen d'appellations d'origine protégées ou d'indications géographiques protégées sur le Web. L'article 13 du règlement de l'Union européenne n° 1151/2012⁴ contient plusieurs dispositions

⁴ Règlement (UE) n° 1151/2012 du Parlement européen et du Conseil du 21 novembre 2012 relatif aux systèmes de qualité applicables aux produits agricoles et aux denrées alimentaires.

relatives à la protection des produits bénéficiant d'une appellation d'origine protégée ou d'une indication géographique protégée; ces dispositions précisent que les dénominations enregistrées sont protégées contre toute utilisation commerciale directe ou indirecte sur des produits génériques et toute utilisation illicite, imitation, évocation ou autre pratique susceptible d'induire le consommateur en erreur quant à la véritable origine du produit.

34. Globalement, en quelque trois ans d'activité, l'ICQRF a mené plus de 1800 opérations sur le Web dans le monde pour protéger des produits italiens et a obtenu des résultats intéressants qui sont exposés ci-dessous.

35. Entre 2014 et 2017, l'ICQRF, se fondant sur la protection internationale d'office accordée aux produits bénéficiant d'une appellation d'origine protégée ou d'une indication géographique protégée, a réglé 248 cas d'usurpation, d'évocation, d'utilisation commerciale illicite directe ou indirecte, de publicité trompeuse quant à la qualité, l'origine, etc. Les atteintes ont été commises principalement sur le Web. Dans le cadre du processus de règlement des cas, l'ICQRF a pris contact avec les administrations de 15 États membres de l'Union européenne (Allemagne, Autriche, Belgique, Chypre, Danemark, Espagne, Finlande, France, Grèce, Lettonie, Pays-Bas, Pologne, Portugal, Royaume-Uni et Suède) et de la Suisse.

36. Comme pour la protection d'office, un mécanisme de coopération entre les États membres de l'Union européenne a été créé, pour la protection des produits de la vigne (et des vignobles génériques) bénéficiant d'une appellation d'origine protégée ou d'une indication géographique protégée au moyen du règlement (CE) n° 555/2008⁵. L'article 82.2) de ce règlement dispose que chaque État membre désigne une seule instance de contact pour assurer la liaison avec les instances de contact d'autres États membres et avec la Commission. Les instances de contact transmettent et reçoivent les demandes de coopération pour les contrôles concernant les vins et elles représentent leur État dans les relations avec les autres États membres. L'ICQRF a engagé 768 procédures pour atteinte avec des résultats notables.

COOPÉRATION AVEC DES PLATEFORMES SUR LE WEB – EBAY, ALIBABA, AMAZON

37. L'une des activités les plus innovantes menées par l'ICQRF quant à la protection du secteur agroalimentaire italien est la coopération avec les marchés de commerce électronique. Si d'un côté le commerce électronique offre de multiples avantages aux consommateurs et aux entreprises en élargissant considérablement les options et les nouveaux investissements possibles, d'un autre côté il représente un nouvel espace de fraude contre lequel il n'est pas facile de lutter en raison du développement des transactions télématiques et de l'expansion des comportements illégaux au-delà des frontières nationales.

38. Face à cela, l'ICQRF a utilisé tous les moyens disponibles en matière d'application de la loi, de la détection des infractions à la mobilisation avec d'autres États membres en passant par la pression morale.

39. En vertu de l'article 14 de la directive 2000/31/CE⁶, les hébergeurs Internet n'ont aucune obligation générale de surveiller les activités de vente sur le réseau car ils n'ont pas d'obligation générale de vérifier l'absence d'activités illégales susceptibles de porter atteinte aux droits de

⁵ Règlement (CE) n° 555/2008 de la Commission du 27 juin 2008 fixant les modalités d'application du règlement (CE) n° 479/2008 du Conseil portant organisation commune du marché vitivinicole, en ce qui concerne les programmes d'aide, les échanges avec les pays tiers, le potentiel de production et les contrôles dans le secteur vitivinicole.

⁶ Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur ("Directive sur le commerce électronique").

tiers. Toutefois, si un hébergeur a connaissance d'activités illégales sur sa plateforme, il est tenu de retirer le contenu illégal et de rendre impossible l'accès des utilisateurs à celui-ci.

40. En outre, les politiques internes des grands marchés contiennent des dispositions prévoyant la suspension d'un compte si un annonceur est à l'origine de nombreuses activités illégales. Par conséquent, afin d'éviter tout engagement de leur responsabilité, les hébergeurs Internet ont créé des systèmes pour la protection des droits de propriété intellectuelle qui permettent aux titulaires de droits de signaler toute atteinte : il s'agit de la procédure de plainte appelée "procédure de notification et de retrait".

41. EBay a créé le programme Verified Rights Owners (VeRo) (titulaires de droits approuvés) qui permet aux titulaires de droits de propriété intellectuelle (droit d'auteur, marques, brevets ou indications géographiques protégées) de signaler toute atteinte à leurs droits légitimes. L'ICQRF participe à ce programme en tant que représentante du Ministère des politiques agricoles, alimentaires et forestières, titulaire de droits de propriété intellectuelle pour les appellations d'origine protégées et les indications géographiques protégées italiennes, et a la capacité d'identifier des publicités potentiellement non conformes et de demander leur retrait. En outre, l'ICQRF a créé sa propre page Web sur la plateforme eBay pour communiquer directement avec les utilisateurs et les informer des législations européenne et nationale relatives à l'obligation d'information pour les produits agroalimentaires et les questions de protection des produits en rapport avec les appellations d'origine protégées et les indications géographiques protégées. En pratique, la coopération entre l'inspection générale et eBay a débouché sur une procédure simplifiée après la conclusion d'un mémorandum d'accord : eBay fournit à l'ICQRF un formulaire lui permettant de signaler une violation en indiquant notamment ses références et, surtout, le "Numéro de l'objet" identifiant l'article illégal repéré sur la plateforme. La deuxième étape consiste à adresser une notification complète de violation à l'adresse électronique du programme VeRO qui, si la demande se révèle légitime, supprime l'entrée illégale. Ce système simple et efficace permet à l'administrateur de retirer les entrées irrégulières de la plateforme eBay dans un laps de temps très court.

42. Entre 2014 et 2017, l'ICQRF a signalé à eBay près de 523 annonces irrégulières.

43. Par ailleurs, la coopération entre l'ICQRF et le groupe Alibaba montre qu'avec des outils appropriés et des accords spécifiques entre les parties, il est possible de mener des contrôles efficaces sur le Web. Au mois d'août dernier, un mémorandum d'accord important a été signé, reconnaissant l'inspection générale en tant que "titulaire de droits" relatifs à des indications géographiques italiennes et lui permettant de participer au programme de protection de la propriété intellectuelle qui offre aux titulaires de droits la possibilité de soumettre des plaintes en ligne concernant des atteintes à la plateforme. Les résultats ne se sont pas fait attendre. Entre 2015 et 2017, 103 entrées irrégulières ont été supprimées dans un grand nombre de cas distincts.

44. Dernier point et non le moindre, sans avoir signé de mémorandum d'accord, l'ICQRF a mis en place une coopération satisfaisante avec Amazon au premier trimestre 2016. Cette collaboration consiste en la communication de rapports au Département juridique d'Amazon Europe concernant des violations constatées sur ses plateformes dans les secteurs européens. Là encore, les résultats ont été incroyables. À ce jour, 168 entrées irrégulières évoquant ou utilisant de manière illicite des vins italiens bénéficiant d'une AOP ou d'une IGP ont été signalées.

45. Globalement, l'ICQRF est intervenue sur les plus grands marchés de commerce électronique à la suite de 794 procédures de plainte avec un taux de réussite de 98%.

46. Cette forme de coopération innovante montre qu'il est possible de protéger les consommateurs et le patrimoine culturel européen sur l'Internet. Au cours des dernières

années, l'ICQRF a engagé plus de 1800 actions pour la protection de denrées alimentaires et fourragères italiennes; ces procédures constituent un cas d'étude intéressant dans le domaine de la protection des indications géographiques. Le taux de réussite élevé des actions engagées témoigne de la forte convergence entre les intérêts des marchés qui souhaitent proposer des produits commerciaux authentiques sur leurs plateformes et la méthode de lutte contre la fraude adoptée par l'ICQRF qui s'est révélée très efficace pour "éliminer" des marchés en ligne les produits irréguliers.

47. La coopération avec d'autres autorités de contrôle est tout aussi importante : outre l'établissement de liens étroits avec les autorités européennes, l'ICQRF a établi, au cours des dernières années, des accords opérationnels avec l'Administration fédérale de contrôle des produits alimentaires et pharmaceutiques et l'Alcohol and Tobacco Tax and Trade Bureau des États-Unis d'Amérique, ainsi qu'avec l'Administration générale pour la surveillance de la qualité, l'inspection et la quarantaine de la Chine (AQSIQ), en vue de faire mieux connaître les questions relatives à la protection des produits protégés par des appellations d'origine protégées et des indications géographiques protégées et les solutions les plus efficaces en matière de lutte contre la fraude.

MÉCANISMES INSTITUTIONNELS MIS EN PLACE EN RÉPUBLIQUE DE CORÉE POUR METTRE UN TERME À LA PROLIFÉRATION DES PRODUITS CONTREFAISANTS EN LIGNE

*Contribution établie par M. Lim Junyoung, directeur adjoint, Division des affaires multilatérales, Office coréen de la propriété intellectuelle (KIPO), Daejeon (République de Corée)**

RÉSUMÉ

L'Office coréen de la propriété intellectuelle (KIPO) a la responsabilité de réagir au préjudice causé par la diffusion à grande échelle de produits contrefaisants. Afin d'aborder cette question de manière efficace, plusieurs mécanismes institutionnels ont été mis en place et sont utilisés.

Le KIPO a créé une brigade d'enquête spéciale pour les marques afin d'améliorer l'application des lois sur la contrefaçon, et une force spéciale chargée de l'application de la loi en ligne a été mise en place afin de réglementer les transactions électroniques de produits suspectés de contrefaçon. Le KIPO a aussi mis au point le système de contrôle électronique de la propriété intellectuelle (IPOMS), le Centre de rapport sur les produits contrefaisants et le Conseil anti-contrefaçon.

Cependant, il existe des limitations pour ce qui est de traduire en justice les auteurs de contrefaçons. Il est nécessaire de faire des efforts pour améliorer la coopération internationale afin d'arrêter les auteurs et de bloquer les sources de distribution de produits contrefaisants.

Le KIPO travaille sans relâche à créer un système favorisant l'innovation authentique et à lutter contre la commercialisation, la distribution et la vente de produits contrefaisants, et il prévoit de poursuivre ces efforts dans ce sens.

I. RAPPEL

1. Les droits de propriété intellectuelle sont un élément essentiel de la compétitivité des produits et services et ils sont considérés comme une ressource importante pouvant apporter de la valeur ajoutée. Cependant, à mesure que les technologies de l'information et de la communication ont progressé, l'utilisation des droits de propriété intellectuelle s'est répandue rapidement dans le monde entier, attirant l'attention sur la facilité avec laquelle il pouvait être porté atteinte à ces droits. La valeur du marché des produits contrefaisants en République de Corée est estimée à environ 4,3 milliards de dollars É.-U. (environ 2 milliards de dollars É.-U. en marchandises étrangères et autour de 2,3 milliards de dollars É.-U. en marchandises produites dans le pays).

2. En particulier, la vente de produits en ligne par le biais des réseaux sociaux et des téléphones portables connaît une progression vertigineuse et la distribution ainsi que la vente d'articles de contrefaçon ont connu le même essor. Il est évident qu'étant donné que la nature des communications entre individus s'est diversifiée grâce aux réseaux sociaux, il est urgent de mettre au point des mesures préventives pour enrayer la distribution de plus en plus privée et sophistiquée de produits contrefaisants qui résulte de cette évolution.

* Les points de vue exprimés dans le présent document sont ceux de l'auteur et ne reflètent pas nécessairement ceux du Secrétariat ou des États membres de l'OMPI.

II. PRINCIPALES ACTIVITÉS

A. BRIGADE D'ENQUÊTE SPÉCIALE POUR LES MARQUES ET FORCE SPÉCIALE CHARGÉE DE L'APPLICATION DE LA LOI EN LIGNE

3. L'Office coréen de la propriété intellectuelle (KIPO) a milité activement en faveur de l'introduction d'une autorité spéciale de police judiciaire chargée d'éliminer la distribution de produits de contrefaçon et de renforcer les fondements de la protection des droits de propriété intellectuelle. En 2010, il a créé une brigade d'enquête spéciale pour les marques dans le but d'améliorer l'application des droits dans le domaine de la contrefaçon et ouvert des bureaux dans les villes de Séoul, Busan et Daejeon.

4. En novembre 2011, le KIPO a créé une force spéciale chargée de l'application de la loi en ligne et dotée d'un équipement technico-légal numérique, afin de réglementer strictement les transactions en ligne de produits de contrefaçon, d'arrêter les vendeurs de ces produits et de bloquer ou fermer les sites Web incriminés.

5. Par ailleurs, la brigade d'enquête spéciale a renforcé sa stratégie pour les enquêtes relatives à la fabrication et à la distribution en ligne de produits contrefaisants en prenant les mesures suivantes :

- mener des enquêtes sur les sites Web bloqués ou fermés à plusieurs reprises pour soupçon de vente de produits contrefaisants;
- créer une base de données et analyser les informations des sites de revente récurrents dont les serveurs sont à l'étranger ou qui ont subi de nombreuses sanctions;
- coopérer avec le Service coréen des douanes afin d'établir des mesures adéquates à la frontière;
- encourager les exploitants de sites de vente en ligne à supprimer volontairement les sites de distribution de produits de contrefaçon et à surveiller volontairement la distribution de ce type de produits; et
- partager les informations et adopter des mesures répressives conjointes avec d'autres organisations pertinentes, afin d'améliorer l'efficacité de l'action.

B. SYSTÈME DE CONTRÔLE ÉLECTRONIQUE DE LA PROPRIÉTÉ INTELLECTUELLE (IPOMS)

6. En 2010, le KIPO a mis en place le système de contrôle électronique de la propriété intellectuelle (IPOMS), qui permet, en collaboration avec l'Agence coréenne de protection de la propriété intellectuelle, un organisme public affilié au KIPO, de repérer, supprimer ou bloquer l'accès aux annonces proposant des produits de contrefaçon placés sur des marchés coréens en ligne, des sites de vente aux enchères et des sites d'achat en ligne appartenant à des particuliers.

7. L'IPOMS exploite un système de surveillance automatique qui collecte les informations tirées des annonces de vente publiées sur les sites hébergeant des marchés électroniques ouverts, et repère les produits de contrefaçon par comparaison avec des mots-clés de détection, des listes noires et des informations sur les prix. Si le système détecte la présence de produits de contrefaçon, les exploitants des sites concernés sont avisés et peuvent procéder volontairement à l'arrêt de la vente. Une fois que le produit est identifié comme contrefaisant et

que sa vente cesse, le système empêche toute autre infraction aux droits en mettant l'identifiant du vendeur sur liste noire. Les sites hébergeant des marchés électroniques ouverts peuvent aussi empêcher l'inscription de vendeurs inscrits sur la liste noire en surveillant les renseignements personnels fournis par les vendeurs.

8. Si l'IPOMS repère un site d'achat en ligne appartenant à un particulier qui vend des produits de contrefaçon, des vérificateurs professionnels rassemblent des éléments attestant de nouvelles ventes et demandent un examen par la Commission coréenne des normes de communication. L'accès au site est ensuite bloqué, ou le site est totalement fermé. En fonction des circonstances de l'affaire, c'est la police des enquêtes spéciales qui se charge d'enquêter sur les vendeurs non occasionnels et les gros vendeurs.

9. En outre, le KIPO travaille sans relâche à améliorer les fonctionnalités de l'IPOMS. En 2014, une fonction a été ajoutée afin de fournir un accès automatique aux forums des sites de vente en ligne et de faire des captures d'écran d'informations pouvant être utilisées comme preuves de la vente de produits contrefaisants et, en 2015, une fonction permettant d'obtenir l'URL des sites de vente en ligne qui proposent des produits de contrefaçon a été introduite. Les informations sont tirées d'un site communautaire ou d'un blog puis transférées sur un site portail, ce qui permet d'identifier et d'extraire l'URL du détaillant en ligne qui vend des articles de contrefaçon. En 2016, le KIPO a élargi le champ des informations recueillies par l'IPOMS pour inclure des fonctions mobiles.

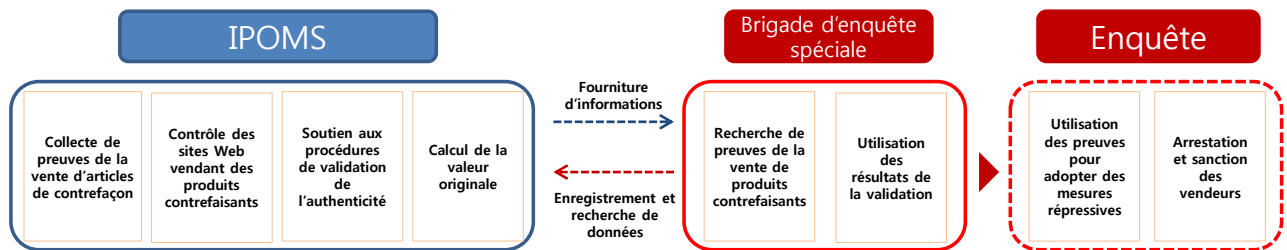
10. En 2016, le KIPO a empêché 5888 ventes de produits contrefaisants sur des marchés ouverts, et fermé 368 sites de vente en ligne. Il a également réussi à faire confisquer 31 948 produits de contrefaçon; la plupart de ceux-ci étaient des répliques de vêtements, de sacs, de portefeuilles et d'accessoires de mode de célèbres marques coréennes et étrangères.

< Activités du KIPO relatives à l'application des droits dans le domaine de la lutte contre la contrefaçon en ligne >

	2012	2013	2014	2015	2016	Total
Marchés ouverts (ventes arrêtées)	4 256	4 422	5 348	5 673	5 888	25 587
Sites de vente (fermés)	505	828	454	418	368	2 573
Poursuites pénales	109	117	41	170	159	596
Confiscation de produits	25 949	9 099	3 182	38 007	31 948	108 185

11. Afin de mettre en place un système de réponse rapide pour empêcher la distribution de produits contrefaisants, le KIPO a renforcé ses capacités à enquêter sur des sites Web de vente de produits contrefaisants grâce à des liens hors ligne avec l'IPOMS. Ce dernier fournit les adresses et les informations sur les vendeurs en lien avec les sites frauduleux proposant des produits contrefaisants, rassemble des preuves de la vente d'articles de contrefaçon, contrôle les sites Web sur lesquels est vendu ce type de produits, soutient les procédures de validation de l'authenticité et calcule la valeur originale. Ensuite, il communique les informations qu'il a recueillies à la brigade d'enquête spéciale et facilite les enquêtes.

< Procédure de soutien à l'application des droits pour la brigade d'enquête avec l'IPOMS >



C. CENTRE DE SIGNALEMENT DE PRODUITS CONTREFAISANTS ET SYSTÈME DE RÉCOMPENSES POUR LE SIGNALEMENT DE PRODUITS CONTREFAISANTS

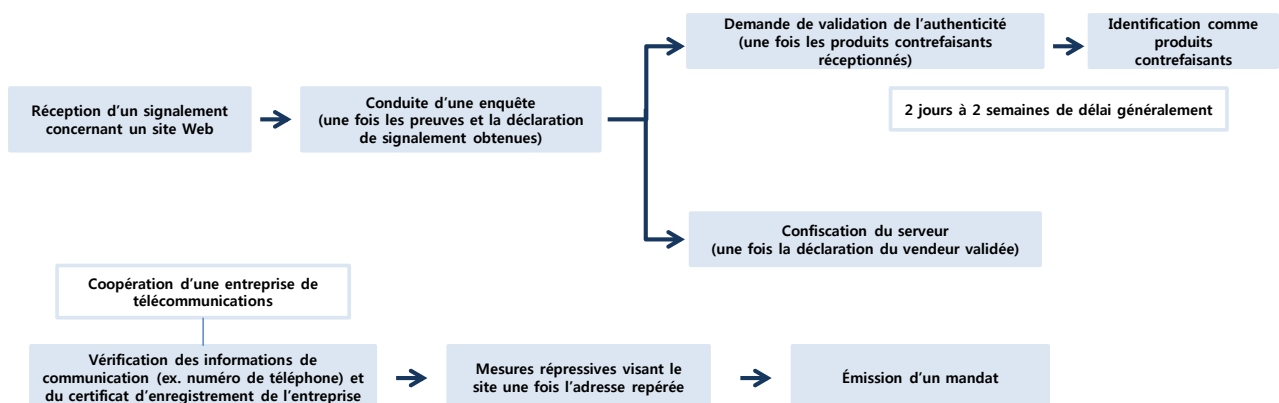
12. Le KIPO gère le Centre de signalement de produits contrefaisants dans le but de supprimer la distribution de produits de contrefaçon et de recueillir des informations concernant la fabrication, la distribution et la vente de ce type de produits. Il détermine si le contenu des signalements envoyés au centre constitue une infraction à la loi sur les marques ou à la loi sur la prévention de la concurrence déloyale et la protection des secrets d'affaires de la République de Corée.

13. Si l'infraction est légère, le signalement fait l'objet d'un encadrement administratif, notamment d'une recommandation de correction. Si elle est considérée comme grave et passible de poursuites pénales, la brigade d'enquête spéciale pour les marques enquêtera sur le suspect et enverra le dossier complet au procureur.

14. Dans le cas des infractions en ligne, par exemple sur un site Web ou un blog, le KIPO demandera à la Commission coréenne des normes de communication de fermer le site Web ou aux exploitants du portail Internet de supprimer l'annonce après avoir confirmé qu'il s'agissait réellement d'une infraction en ligne.

15. Pour faciliter le signalement des produits contrefaisants et sensibiliser le public à l'illégalité des produits de contrefaçon, le KIPO a mis en place un système de récompenses pour le signalement de produits contrefaisants en 2006. Un signalement peut porter sur la fabrication, la distribution ou la vente de produits contrefaisants, et il peut être soumis par toute personne.

< Procédure d'application des droits suite à une plainte visant un site de vente en ligne >



16. En 2016, 23 cas de ventes en ligne ont été signalés et 19,2 millions de dollars É.-U. ont été offerts en récompense. Par rapport à 2015, les données pour 2016 témoignent d'une augmentation de 228,6% des cas signalés et de 237% du montant des récompenses. Cette analyse montre une envolée récente de la circulation d'articles de contrefaçon en ligne.

< Récompenses pour le signalement de produits contrefaisants dans les ventes en ligne >

(unité : cas, milliers de dollars É.-U.)

2010		2011		2012		2013		2014		2015		2016	
Cas	Montant	Cas	Montant	Cas	Montant	Cas	Montant	Cas	Montant	Cas	Montant	Cas	Montant
12	6,9	5	2,2	4	1,7	2	0,9	5	3,3	7	5,7	23	19,2

17. En 2016, le montant total des récompenses offertes par le KIPO au cours de ses 11 années de gestion du système de récompenses pour le signalement de produits contrefaisants a atteint 1,7 million de dollars É.-U. La valeur totale des produits authentiques correspondant aux articles contrefaisants saisis grâce au système était de 2,8 milliards de dollars É.-U.

D. CONSEIL ANTI-CONTREFAÇON

18. Pour contribuer à des échanges commerciaux équitables, le KIPO a lancé le Conseil anti-contrefaçon, un système de coopération public-privé composé de 62 organisations et entreprises, y compris des organismes de contrôle des produits contrefaisants, des entreprises détentrices de marques, des sites de vente en ligne et des organisations connexes.

19. Le Conseil anti-contrefaçon a organisé des séminaires auxquels ont participé tous les membres, en vue de :

- partager des informations sur les fournisseurs de produits contrefaisants en ligne;
- mettre en place des restrictions concernant la distribution de produits contrefaisants sur les sites Web de vente de produits de contrefaçon et sur les réseaux sociaux; et
- faciliter la coopération entre les titulaires de droits sur les marques et les sites de vente en ligne afin de limiter le nombre de vendeurs de produits contrefaisants et l'émergence de circuits de distribution en ligne de ces produits.

20. De plus, les principales entreprises membres ont participé à une action conjointe en faveur de l'application des droits, distinguant rapidement les produits authentiques des produits contrefaisants sur place, ce qui a contribué au succès de cette initiative conjointe.

E. COOPÉRATION AVEC LES SITES DE VENTE EN LIGNE ÉTRANGERS

21. En raison de la croissance rapide des sites de vente en ligne, les préjudices causés par la distribution de produits contrefaisants continuent d'être signalés non seulement au niveau national mais aussi sur les sites de vente en ligne étrangers. Ainsi, le KIPO a commencé à prêter attention à la distribution nationale et internationale de produits contrefaisants provenant de sites de vente en ligne étrangers.

22. Par exemple, en avril 2014, l'Agence coréenne de protection de la propriété intellectuelle a signé un mémorandum d'accord avec une entreprise mondiale de commerce électronique afin d'aider à résoudre le problème des articles de contrefaçon qui circulent sur les sites de vente étrangers. Le principal objectif du mémorandum d'accord est de promouvoir les échanges commerciaux entre les deux entités tout en assurant la protection des droits de propriété intellectuelle, l'établissement d'un processus de coopération en vue de promouvoir la protection des droits de propriété intellectuelle et le soutien aux campagnes publiques conjointes destinées à protéger les droits de propriété intellectuelle. En particulier, le mémorandum d'accord prévoyait une procédure permettant à l'entreprise de prendre des mesures afin de faire cesser la vente de produits de contrefaçon si l'Agence coréenne de protection de la propriété intellectuelle donnait des informations sur les atteintes aux droits de propriété intellectuelle.

23. Par conséquent, en 2016, l'Agence coréenne de protection de la propriété intellectuelle a aidé l'entreprise à retirer de la vente 19 621 produits contrefaisants. La valeur des produits interceptés était d'environ 30,7 millions de dollars É.-U. et, en tenant compte des effets collatéraux tels que la réduction des ventes et l'affaiblissement de la fiabilité des entreprises mondiales en raison de la vente d'articles de contrefaçon, la chute liée aux effets de ce retrait de la vente devrait être bien plus conséquente.

III. DÉFIS ET PROJETS FUTURS

24. Le KIPO étendra le rôle de la brigade d'enquête spéciale et renforcera sa force spéciale chargée de l'application de la loi en ligne afin d'assurer un suivi et une analyse plus efficace des moyens de distribution des produits de contrefaçon.

25. Dans le cas des articles de contrefaçon vendus en ligne, les serveurs de la plupart des sites Web de distribution habituels sont situés à l'étranger. Une application des droits effective comporte de nombreuses difficultés car, bien souvent, seule la personne au nom de laquelle est enregistrée l'entreprise réside localement, tandis que le véritable directeur reste à l'étranger. Les enquêtes sont fréquemment arrêtées et considérées comme inefficaces. En outre, la plupart des suspects continuent de vendre des articles de contrefaçon même après le blocage du site Web, en changeant le nom de domaine par une adresse similaire.

26. La distribution des produits contrefaisants est en mutation : elle est de moins en moins le fait d'individus ou de petites entreprises et procède de plus en plus de grandes sociétés ayant de larges réseaux à leur disposition. Il faut concentrer les contrôles sur ce profil émergent de distributeurs. En outre, les négociants ayant un profil de société, dont certains sont associés à des groupes criminels, produisent et distribuent des produits contrefaisants afin de financer des organisations criminelles. Par conséquent, il est nécessaire de contrôler plus attentivement les articles de contrefaçon pour les éradiquer, et d'améliorer la coopération internationale pour bloquer, en dernière instance, la source de distribution des produits contrefaisants.

27. Le KIPO prévoit de se concentrer sur les arrestations visant les sociétés de distribution en ligne récidivistes, en coopération avec le procureur. En particulier, il s'efforcera de faire respecter de manière stricte les droits face aux récidivistes et prévoit de renforcer la coopération avec les organisations nationales et internationales en vue d'établir un ordre commercial équitable. De plus, le KIPO renforcera la collecte d'informations et l'application des lois contre les circuits de distribution d'articles de contrefaçon qui utilisent les sites de vente en ligne et le marché émergent des réseaux sociaux.

28. Comme la sensibilisation à ces problèmes est essentielle pour éradiquer les articles de contrefaçon, le KIPO envisage de renforcer la coopération public/privé. Dans le cadre du Conseil anti-contrefaçon, il est prévu de mettre au point des mesures afin d'éliminer la distribution de produits contrefaisants en ligne. Le KIPO continuera d'être attentif aux difficultés mentionnées par les négociants en ligne et les titulaires de droits sur les marques auxquels les produits contrefaisants portent préjudice, et il élargira la coopération en organisant des séminaires à ce sujet. Par ailleurs, il envisage de promouvoir activement la sensibilisation aux activités essentielles du Conseil anti-contrefaçon afin d'encourager d'autres entreprises et fournisseurs en ligne à y participer.

DIFFICULTÉS RENCONTRÉES DANS L'INSTRUCTION DES ATTEINTES PORTÉES EN LIGNE À LA PROPRIÉTÉ INTELLECTUELLE : POINT DE VUE DU BUREAU DU PROCUREUR GÉNÉRAL EN THAÏLANDE

*Contribution établie par Mme Duangporn Teachakumtorn, procureur, Département de la propriété intellectuelle et des litiges en matière de commerce international, Bureau du procureur général, Bangkok (Thaïlande)**

RÉSUMÉ

Cela fait plusieurs années que la Thaïlande est aux prises avec les atteintes aux droits de propriété intellectuelle. L'application effective des droits de propriété intellectuelle dans ce pays est donc considérée comme une tâche prioritaire, à laquelle il faut s'atteler rapidement. Cela étant, il est très difficile de poursuivre les auteurs des atteintes portées en ligne, compte tenu du caractère transnational de ces actes et du fait qu'il est difficile d'obtenir des preuves. En Thaïlande, l'application des lois doit passer par une meilleure coopération, tant au niveau national qu'au niveau international. Il est également clair que la Thaïlande doit laisser une plus grande marge de manœuvre à ses procureurs, afin que ceux-ci puissent prendre des décisions judicieuses et se concentrer sur les affaires les plus importantes. Enfin, il est également essentiel de promouvoir le respect des droits de propriété intellectuelle pour régler le problème. La population doit comprendre que l'atteinte aux droits de propriété intellectuelle est un problème sérieux et en être convaincue, ce qui contribuera beaucoup à l'élimination durable des activités constituant des atteintes.

I. VUE D'ENSEMBLE

1. Les atteintes portées en ligne aux droits de propriété intellectuelle sont l'un des grands problèmes auxquels les procureurs thaïlandais sont confrontés ces derniers temps. Le Bureau du procureur général a créé en 1999 le Département de la propriété intellectuelle et des litiges en matière de commerce international spécialement pour lutter contre ce phénomène. Auparavant, les atteintes aux droits de propriété intellectuelle étaient de nature physique, et l'on pouvait arrêter et poursuivre les vendeurs ambulants ou les fabricants de marchandises de contrefaçon. Mais on constate ces dernières années un véritable essor de la contrefaçon et du piratage au moyen de plateformes numériques en Thaïlande; ce commerce a donc quitté les rues pour conquérir Internet. Il faut certes encourager et embrasser le progrès technologique, mais le détournement de ces nouveaux outils pose des problèmes extrêmement difficiles et complexes aux procureurs thaïlandais. Les enquêtes sur les atteintes aux droits de propriété intellectuelle commises en Thaïlande sont de plus en plus difficiles du fait de l'existence d'éléments étrangers étroitement liés à ces affaires et établis en dehors du pays. Il arrive ainsi que les noms de domaine des sites Web constituant une atteinte soient enregistrés à l'étranger, ou que certains contrevenants aient recours à des fournisseurs de services Internet établis en dehors de la Thaïlande. Il ne faut par ailleurs pas sous-estimer les difficultés que l'on rencontre lorsqu'on cherche à réunir les éléments de preuve et à prouver les activités constitutives d'atteintes devant un tribunal.

* Les points de vue exprimés dans le présent document sont ceux de l'auteur et ne reflètent pas nécessairement ceux du Secrétariat ou des États membres de l'OMPI.

II. LÉGISLATION

2. La Thaïlande a rejoint l'OMPI en 1989. Voici les principaux textes de loi en matière de propriété intellectuelle en vigueur en Thaïlande :

- loi de 2534 (ère bouddhique) (1991) sur les marques, modifiée en 2016;
- loi de 2545 (ère bouddhique) (2002) sur les secrets commerciaux, modifiée en 2015;
- loi de 2537 (ère bouddhique) (1994) sur le droit d'auteur, modifiée en 2015;
- loi de 2546 (ère bouddhique) (2003) sur la protection des indications géographiques;
- loi de 2543 (ère bouddhique) (2000) sur la protection des schémas de configuration de circuits intégrés;
- loi de 2542 (ère bouddhique) (1999) sur la protection des variétés végétales; et
- loi de 2522 (ère bouddhique) (1979) sur les brevets, modifiée en 1999.

3. La législation thaïlandaise en matière de propriété intellectuelle est parfaitement conforme aux normes internationales. Voici les modifications qui ont été apportées récemment à cette législation.

- Loi sur les marques : dans une modification récente de la loi thaïlandaise sur les marques, on a inclus le son dans la définition de la marque. Le son est donc aujourd'hui susceptible d'enregistrement comme marque en Thaïlande. Cette loi contient aussi une disposition nouvelle concernant spécialement le reconditionnement illégal (l'infraction qui consiste à placer la copie d'un produit dans son emballage d'origine) et qui fixe des peines plus lourdes en comparaison avec l'infraction visée précédemment dans le Code pénal.
- Loi sur le droit d'auteur : la loi thaïlandaise sur le droit d'auteur a été fortement remaniée. Elle contient de nouvelles dispositions : des dispositions de lutte contre la reproduction par caméscope, des mesures techniques de protection, des informations sur le régime des droits, une disposition sur les exonérations pour les fournisseurs de services Internet, une exception d'usage loyal, une exception pour les personnes handicapées et une exception relative à la première vente.

III. POURSUITES EN MATIÈRE DE PROPRIÉTÉ INTELLECTUELLE

4. Le Département de la propriété intellectuelle et des litiges en matière de commerce international est une unité spécialisée du Bureau du procureur général. Sa compétence territoriale couvre Bangkok et cinq villes voisines : Samut Prakan, Samut Sakorn, Nakorn Pratom, Nonthaburi et Pathum Thani. Les affaires qui se produisent ailleurs sont traitées par les procureurs du bureau compétent pour la région où la violation est commise. À l'intérieur du pays, les procureurs s'occupent généralement de tous les types d'affaires et pas seulement de celles qui ont trait à la propriété intellectuelle.

5. Le Département reçoit environ 2000 dossiers de propriété intellectuelle par an, dont la grande majorité consiste en des atteintes aux marques et au droit d'auteur. Il traite aussi des atteintes aux brevets et aux secrets commerciaux, mais celles-ci sont encore peu nombreuses par rapport aux deux autres types d'affaires.

A. ÉTAPES DE L'INSTRUCTION

6. En cas d'atteinte, les titulaires des droits peuvent intenter eux-mêmes une action en justice contre l'auteur de l'atteinte; cette action peut être pénale, civile, ou les deux à la fois. Les titulaires peuvent aussi faire intervenir les autorités en déposant une plainte auprès d'un enquêteur de la police royale thaïlandaise ou du département des enquêtes spéciales du Ministère de la justice. L'enquêteur mène une enquête approfondie et réunit tous les éléments de preuve pertinents. Une fois l'enquête terminée, le dossier est transmis au procureur, qui examine les faits et tous les éléments de preuve disponibles. À ce moment, le procureur peut demander à l'enquêteur d'approfondir les recherches sur tel ou tel aspect qui doit selon lui être clarifié. Cette phase terminée, le procureur décide s'il y a suffisamment d'éléments de preuve pour prouver le méfait devant un tribunal. Dans l'affirmative, des poursuites sont ordonnées et une plainte est déposée devant le Tribunal central de la propriété intellectuelle et du commerce international¹ contre l'inculpé (qui devient défendeur). Si les éléments de preuve sont insuffisants, le procureur décide de ne pas engager de poursuites et transmet le dossier, accompagné de son avis et des raisons pour lesquelles il a décidé de ne pas engager de poursuites, au commissaire général de la police royale thaïlandaise ou au directeur général du département des enquêtes spéciales, selon le cas, afin que celui-ci puisse se prononcer sur le bien-fondé de la décision. Si le commissaire général ou le directeur général est du même avis que le procureur, l'ordre de non-poursuite devient définitif. Par contre, si le commissaire général ou le directeur général estime qu'il y a assez d'éléments de preuve pour prouver le méfait, le dossier est transmis au procureur général, qui prend la décision en dernier ressort.

B. ATTEINTES PÉNALES AUX DROITS DE PROPRIÉTÉ INTELLECTUELLE

7. On distingue deux types d'infractions pénales en Thaïlande : les infractions qui peuvent se régler par un accord entre les parties et celles pour lesquelles c'est impossible. Dans le contexte de la propriété intellectuelle, l'atteinte au droit d'auteur peut se régler par un accord, mais pas les autres atteintes aux droits de propriété intellectuelle. Cela signifie que les dossiers d'atteinte au droit d'auteur peuvent être ouverts uniquement si les titulaires des droits portent plainte. Par ailleurs, aux termes de l'article 66 de la loi de 2534 (ère bouddhique) sur le droit d'auteur, les titulaires des droits peuvent retirer leur plainte à tout moment, mais ils le font habituellement après avoir été indemnisés de façon satisfaisante. Après le retrait de la plainte, les procureurs n'ont plus le droit de poursuivre. L'affaire est classée sans suite en vertu de l'article 39 du Code de procédure pénale.

8. En Thaïlande, dans les dossiers d'atteintes portées en ligne, on constate souvent des atteintes au droit d'auteur et aux marques. Il arrive que les activités portant atteinte aux droits soient menées par l'intermédiaire de boutiques en ligne. Ces dernières sont souvent le prolongement de magasins physiques dans lesquels les auteurs des atteintes vendent des films ou des chansons pirates sur DVD, ou des produits de contrefaçon dans leur boutique en ligne ou sur des réseaux sociaux tels que Facebook et Instagram. Il arrive que les titulaires ou les enquêteurs achètent une petite quantité de marchandises de contrefaçon pour prouver la vente de marchandises constituant une atteinte. Le paiement se fait généralement par virement vers le compte mentionné par le vendeur. Après le paiement, la marchandise est livrée par courrier, et conservée en guise de preuve. Il existe aussi des boutiques numériques dans lesquelles on peut télécharger des films, des jeux ou des chansons pirates, au format numérique. Il n'y a alors aucun élément de preuve physique.

¹ Pour obtenir des informations plus détaillées sur l'expérience du Tribunal central de la propriété intellectuelle et du commerce international de la Thaïlande, voir le document WIPO/ACE/11/7, disponible à l'adresse http://www.wipo.int/meetings/en/doc_details.jsp?doc_id=342836.

9. Dans les deux types d'infraction, le principal mode de paiement est le plus souvent le virement bancaire, et non la carte de crédit. On constate l'utilisation d'adresses électroniques appartenant à des fournisseurs de services Internet établis en dehors de la Thaïlande, tels que Gmail, Hotmail ou Yahoo. Dans certaines boutiques en ligne, on trouve le numéro de téléphone du vendeur, mais ce dernier omet souvent de mentionner cette information, pour éviter de se faire repérer et poursuivre. Et lorsqu'ils sont mentionnés, les numéros de téléphone sont souvent reliés à des cartes prépayées, que l'utilisateur peut acheter sans avoir à prouver son identité. Il est donc très difficile d'obtenir des éléments de preuve solides en vue d'une condamnation. Le seul élément de preuve concret sont les opérations bancaires, qui permettent de suivre le mouvement des fonds, depuis le compte de l'acheteur jusqu'à celui du vendeur. Dès lors, le titulaire du compte est souvent arrêté et peut être accusé d'atteinte aux droits de propriété intellectuelle, puisque la réception de fonds sur le compte à son nom l'expose comme l'auteur de l'atteinte. Malheureusement, il arrive que les malfaiteurs demandent à des tiers d'ouvrir un compte pour recevoir les virements, contre une petite commission. Ce mode opératoire complique les enquêtes et a comme conséquence que les procureurs disposent d'éléments de preuve très fragiles et non concluants.

IV. DIFFICULTÉS

A. CRIMINALITÉ TRANSNATIONALE

10. Il est indéniable que les progrès techniques bénéficient à toute la société, mais ils aident aussi beaucoup les malfaiteurs en facilitant les activités constituant des atteintes sur Internet. Les atteintes aux droits de propriété intellectuelle ont changé de forme. Par exemple, les vendeurs n'opèrent plus dans des magasins physiques, mais dans des boutiques en ligne, et ils sont donc plus difficiles à identifier du fait de l'anonymat dont ils jouissent. Dans la majorité des affaires de contrefaçon et de piratage en ligne, plusieurs pays entrent en jeu. Même si l'infraction est repérée et commise en Thaïlande, il est probable que son auteur opère depuis une autre région du monde. Dans ces cas de figure, le serveur ou le nom de domaine se trouvera en dehors du territoire thaïlandais, et les autorités thaïlandaises auront alors énormément de mal à poursuivre l'auteur.

B. ÉLÉMENTS DE PREUVE NUMÉRIQUES ET POUVOIR D'ENQUÊTE INEXISTANT

11. Dans les enquêtes sur le piratage en ligne, il est important de préserver et de recueillir les éléments de preuve numériques avant qu'ils ne soient supprimés ou déplacés. Il arrive que les enquêteurs omettent de recueillir des informations importantes, et que le procureur donne donc de nouveaux devoirs d'enquête plus tard, parfois jusqu'à un an après l'atteinte, s'agissant des éléments de preuve numériques, ce qui laisse aux malfaiteurs tout le temps de supprimer ces éléments. Si les enquêteurs et les procureurs communiquaient mieux entre eux dès le début de l'enquête, les procureurs pourraient expliquer aux enquêteurs quels éléments de preuve ils jugent nécessaires pour le procès. Les enquêteurs pourraient alors concentrer leurs efforts sur ces éléments, et les recueillir rapidement avant qu'ils ne soient déplacés ou supprimés.

C. CHARGE DE LA PREUVE

12. Comme leurs homologues étrangers, les procureurs thaïlandais doivent prouver au-delà de tout doute raisonnable que l'inculpé a bien commis l'infraction qui lui est reprochée. Pour les infractions traditionnelles, le procureur fait comparaître des témoins oculaires pour tenter de prouver le méfait. Mais cela n'est pas aussi simple dans le cas des infractions en ligne, puisqu'il n'y a aucun témoin oculaire pour identifier l'auteur de l'atteinte. Par exemple, même si

le procureur parvient à prouver que l'atteinte a été portée depuis un ordinateur donné, il peut être extrêmement difficile d'identifier la personne qui utilisait l'ordinateur au moment où l'infraction a été commise.

D. RESSOURCES INSUFFISANTES

13. Internet étant un espace sans frontières, les autorités chargées de l'application de la loi ont du mal à réprimer les activités constituant des atteintes. Il est relativement facile pour les auteurs d'atteintes de ne pas se faire repérer, puisqu'ils peuvent facilement enregistrer des noms de domaine, supprimer des éléments de preuve ou déplacer le contenu constituant une atteinte vers d'autres sites Web, en quelques minutes. La rapidité de ces techniques de fuite montre à quel point les ressources consacrées à la lutte contre ces activités illégales sont insuffisantes.

V. PROPOSITIONS DE SOLUTIONS POUR AMÉLIORER LES POURSUITES QUANT AUX ATTEINTES PORTÉES EN LIGNE AUX DROITS DE PROPRIÉTÉ INTELLECTUELLE

A. MEILLEURE COOPÉRATION

14. En raison des progrès technologiques, les atteintes aux droits de propriété intellectuelle sont devenues un phénomène mondial. Il est évident que ce problème, compte tenu de son ampleur et de sa complexité, ne peut être réglé par un seul pays. Pour s'attaquer efficacement à ces atteintes, tout pays aura besoin de l'engagement et de l'aide d'autres pays, tant au niveau national qu'au niveau international.

B. POUVOIR DISCRÉTIONNAIRE DES PROCUREURS

15. Contrairement à ce qui se passe dans d'autres pays, les procureurs thaïlandais n'ont pas le choix de refuser un dossier qui leur est transmis par les enquêteurs, dans la mesure où les critères légaux sont respectés. Ils se retrouvent donc avec de nombreux petits dossiers à traiter, et des ressources rares et précieuses sont allouées à des affaires concernant, par exemple, un seul DVD pirate. S'ils avaient un plus grand pouvoir discrétionnaire, les procureurs thaïlandais pourraient consacrer les ressources dont ils disposent à de plus gros dossiers. Les enquêteurs, quant à eux, devraient présenter des dossiers plus importants pour qu'ils soient acceptés par les procureurs. Les autorités pourraient ainsi s'attaquer aux plus gros dossiers, en choisissant avec soin comment ils affectent leurs précieuses ressources.

C. SENSIBILISATION DU PUBLIC : FAIRE RESPECTER LA PROPRIÉTÉ INTELLECTUELLE

16. La dernière décennie a vu un changement dans la perception de la propriété intellectuelle par le peuple thaïlandais alors qu'un nombre plus important de créateurs et d'inventeurs thaïlandais commencent à souffrir d'atteintes à leurs droits. Cela a rendu plus pressante la nécessité de protéger les titulaires de droits, indépendamment de leur nationalité, et cette nécessité est aujourd'hui reconnue plus largement. Il faudra accompagner cette sensibilisation d'un plan pérenne à long terme pour réprimer les atteintes aux droits de propriété intellectuelle. Si le consommateur est intimement convaincu que la contrefaçon et le piratage sont une infraction équivalente au vol, qu'il faut condamner, il ne portera pas atteinte sciemment aux droits de propriété intellectuelle d'autrui.

VI. CONCLUSION

17. En raison des problèmes techniques complexes mentionnés plus haut, il n'existe aucune solution unique et simple pour dissuader les auteurs d'atteintes portées en ligne aux droits de propriété intellectuelle. La Thaïlande devrait donc mettre en place les solutions proposées et les accompagner d'un programme solide de sensibilisation au respect des droits de propriété intellectuelle. L'adhésion totale au principe du respect de ces droits serait la solution ultime et permanente aux atteintes, car elle en éliminerait la cause profonde.

ORDONNANCES DE BLOCAGE DE SITES WEB : L'EXPÉRIENCE DU ROYAUME-UNI

*Contribution établie par Mme Elizabeth Jones, Direction de l'application des droits de propriété intellectuelle et du droit d'auteur, Office de la propriété intellectuelle, Newport (Royaume-Uni)**

RÉSUMÉ

Ces dernières années, les tribunaux du Royaume-Uni ont rendu un certain nombre d'ordonnances enjoignant à certains fournisseurs d'accès à l'Internet (FAI) de bloquer l'accès de leurs abonnés à des sites Web portant atteinte à des droits de propriété intellectuelle. L'affaire *Twentieth Century Fox Film Corp & Ors c. British Telecommunications Plc [2011] EWHC 1981 (Ch)* a été un test pour les grands studios cinématographiques qui demandaient et ont obtenu une décision enjoignant à BT de bloquer l'accès de ses abonnés à un site Web connu sous le nom de Newzbin2. Depuis cette première décision, les FAI ne se sont pas opposés aux ordonnances demandées. C'est pourquoi, lorsque les circonstances sont identiques à celles d'affaires ayant fait l'objet de jugements publics motivés, la plupart des procédures sont instruites par voie de procédure écrite. En novembre 2014, dans l'affaire *Cartier International AG & Ors c. British Sky Broadcasting Ltd & Ors [2014] EWHC 3354 (Ch)* les FAI ont été contraints de bloquer l'accès aux sites Web qui vendaient des produits portant atteinte aux marques Cartier. Cette décision présentait un intérêt tout particulier pour le Royaume-Uni, où il n'existe aucune législation prévoyant expressément le blocage de sites qui portent atteinte à des marques. De telles ordonnances sont considérées comme des outils précieux dans la panoplie de mesures permettant aux titulaires de protéger et faire appliquer leurs droits de propriété intellectuelle au Royaume-Uni mais, étant donné qu'elles impliquent des efforts et des coûts considérables, elles ne sont utilisées que pour les sites qui commettent les atteintes les plus graves.

I. INTRODUCTION

1. Ces dernières années, les tribunaux du Royaume-Uni ont rendu un certain nombre d'ordonnances enjoignant à certains fournisseurs d'accès à l'Internet (FAI) de bloquer l'accès de leurs abonnés à des sites Web portant atteinte à des droits de propriété intellectuelle. Ces ordonnances s'inscrivent dans un éventail de mesures destinées lutter contre les atteintes à la propriété intellectuelle (PI), parmi lesquelles figurent la création d'une unité de police spécialisée dans la lutte contre les atteintes à la propriété intellectuelle, des mesures volontaires, notamment un Code de pratiques recommandées¹ destiné à empêcher que les consommateurs britanniques ne soient dirigés vers des sites Web qui portent atteinte au droit d'auteur, ainsi que des campagnes de sensibilisation, notamment sur le site www.getitrightfromagenuinesite.org.

* Les points de vue exprimés dans le présent document sont ceux de l'auteur et ne reflètent pas nécessairement ceux du Secrétariat ou des États membres de l'OMPI.

¹ <https://www.gov.uk/government/news/search-engines-and-creative-industries-sign-anti-piracy-agreement>.

II. LE CONTEXTE LÉGISLATIF

2. La législation de l'Union européenne (UE) permet aux titulaires de droits de demander qu'une injonction soit prononcée à l'encontre d'un intermédiaire dont les services sont utilisés par un tiers pour porter atteinte aux droits de propriété intellectuelle du titulaire. Les dispositions de l'article 8 de la directive 2001/29/CE² s'appliquent en cas d'atteinte au droit d'auteur ou à un droit connexe et celles de l'article 11 de la directive 2004/48/CE³ prévoient la possibilité d'obtenir une injonction en cas d'atteinte à un droit de propriété intellectuelle.

3. L'article 8 de la directive 2001/29/CE a été transposé dans le droit du Royaume-Uni par l'article 97A⁴ de la loi de 1988 sur le droit d'auteur, les dessins et modèles et les brevets (CDPA). Étant donné que, lors de la transposition de la directive 2004/48/CE, il a été établi que le droit du Royaume-Uni prévoyait déjà une telle injonction, aucune disposition expresse n'a été introduite à cet effet.

III. LA PREMIÈRE ORDONNANCE – NEWZBIN2

4. L'article 97A a été appliqué pour la première fois dans l'affaire *Twentieth Century Fox Film Corp & Ors c. British Telecommunications Plc [2011] EWHC 1981 (Ch)*⁵, plus connue sous le nom de *Newzbin2*. Cette affaire était un test pour les grands studios cinématographiques qui demandaient une ordonnance enjoignant à BT (un FAI du Royaume-Uni) de bloquer l'accès de ses abonnés à un site Web connu sous le nom de *Newzbin2*. Cette demande était soutenue par de nombreux secteurs des industries de la création qui subissaient de plus en plus d'atteintes à leurs droits d'auteur en ligne.

5. *Newzbin2* faisait suite à une procédure antérieure pour atteinte au droit d'auteur introduite en 2010 à l'encontre de *Newzbin Ltd* par les studios, lesquels avaient obtenu gain de cause. *Newzbin* était un site d'indexation Usenet⁶ qui permettait à ses membres de chercher et consulter de manière simplifiée un large éventail de contenus numériques publiés sur le réseau Usenet. Les studios cinématographiques ont obtenu une décision enjoignant à *Newzbin Ltd* de prévenir de futures atteintes au droit d'auteur⁷, *Newzbin* ayant été reconnu coupable d'atteintes au droit d'auteur pour avoir autorisé la copie des films des demandeurs, avoir mis les films des demandeurs à la disposition de ses abonnés premium et s'être engagé à leurs côtés dans le dessein partagé de copier les films des demandeurs, et avoir communiqué les films des demandeurs au public.

6. *Newzbin* a cessé de fonctionner, mais *Newzbin2* est apparu au même emplacement, en proposant le même service, portant ainsi atteinte de façon continue et à grande échelle au droit d'auteur. Il n'était plus hébergé au Royaume-Uni, échappant de fait à la compétence des tribunaux britanniques, mais continuait de cibler le public britannique. Les studios ont tout d'abord écrit à BT pour lui demander de bloquer l'accès à *Newzbin2* ou d'accepter de ne pas s'opposer à une ordonnance qui serait rendue dans ce but. Des preuves de l'activité de *Newzbin2* ont été fournies ainsi qu'un résumé de l'affaire *Newzbin*. BT a fait valoir qu'il n'approuvait ni ne tolérait les atteintes au droit d'auteur mais qu'il lui fallait une décision de

² 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 : <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32001L0029&from=FR>.

³ Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle : <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32004L0048&from=FR>.

⁴ <http://www.legislation.gov.uk/ukpga/1988/48/section/97A>.

⁵ <http://www.bailii.org/ew/cases/EWHC/Ch/2011/1981.html>.

⁶ Un système de forums en ligne antérieur au World Wide Web, quoique moins populaire.

⁷ *Twentieth Century Fox Film Corp c. Newzbin Ltd [2010] EWHC 608 (Ch)*.

justice pour bloquer ces services afin d'éviter d'engager éventuellement sa responsabilité juridique.

7. En conséquence, les studios ont demandé qu'une injonction soit prononcée à l'encontre de BT en tant qu'intermédiaire, en application de l'article 97A de la CDPA, car il s'agissait de la seule façon de prévenir les atteintes au droit d'auteur, ou du moins d'en réduire l'ampleur. Pour ce faire, Cleenfeed, l'outil utilisé par BT pour bloquer l'accès aux sites Internet diffusant des images de pédophilie, a été utilisé.

8. Le tribunal a formulé un certain nombre de questions pour déterminer s'il y avait lieu de délivrer l'injonction :

- Les défendeurs sont-ils des fournisseurs d'accès?
- Les opérateurs ou les utilisateurs des sites Internet portent-ils atteinte au droit d'auteur des demandeurs?
- Les utilisateurs ou les opérateurs se servent-ils des services des défendeurs pour porter atteinte au droit d'auteur?
- Les défendeurs en ont-ils une connaissance effective?

9. Le tribunal a également cherché à savoir si l'injonction constituait une mesure corrective proportionnée, efficace et dissuasive pour faire cesser l'atteinte.

10. Comme BT a reconnu qu'il était un fournisseur d'accès, il restait deux points à examiner par le tribunal : déterminer si les services fournis par BT étaient utilisés pour porter atteinte au droit d'auteur et si BT avait une connaissance effective de cette atteinte. Le tribunal a conclu que les clients de BT utilisaient les services de ce dernier pour porter atteinte au droit d'auteur et qu'il suffisait que BT sache que ses services étaient utilisés pour porter atteinte au droit d'auteur (il n'était pas nécessaire de démontrer que BT avait connaissance d'une atteinte déterminée par une personne particulière à une œuvre précise protégée par le droit d'auteur).

11. Le tribunal a également considéré que le fait de bloquer ou d'empêcher l'accès à Newzbin2 constituait un contrôle ciblé et non généralisé. L'injonction était considérée comme proportionnée car, lorsque le tribunal a mis en balance le droit à la protection de la propriété et la liberté d'expression garantie par la Convention européenne des droits de l'homme⁸, le droit des studios (et autres titulaires) de protéger leurs droits de propriété intellectuelle l'emportait sur le droit à la liberté d'expression de Newzbin2 et BT. Les coûts de mise en œuvre incombant à BT seraient proportionnés (compte tenu de l'existence de l'outil Cleenfeed). Le tribunal a également accepté l'argument des studios selon lequel l'ordonnance serait justifiée même si elle n'empêchait qu'une minorité d'utilisateurs d'accéder à Newzbin2. Compte tenu des efforts et des dépenses considérables investis dans la procédure, il était peu probable qu'elle suscite une vague de demandes d'ordonnances similaires. L'injonction a donc été rendue et les modalités en ont été fixées lors d'une audience ultérieure⁹.

12. Suite à leur victoire dans cette affaire, les studios ont demandé (et obtenu) des ordonnances similaires contre les autres grands FAI britanniques¹⁰.

13. Une deuxième demande a été déposée pour obliger les FAI à bloquer l'accès à The Pirate Bay (*Dramatico Entertainment Ltd & Ors c. British Sky Broadcasting Ltd & Ors [2012] EWHC 268 (Ch)*). Introduite par les représentants de l'industrie de la musique, cette demande n'a rencontré aucune opposition de la part des FAI. Les plaintes pour atteinte au droit d'auteur

⁸ Droit à la protection de la propriété (article premier du Protocole n° 1) et droit à la liberté d'expression (article 10) : http://www.echr.coe.int/Documents/Convention_FRA.pdf.

⁹ <http://www.bailii.org/ew/cases/EWHC/Ch/2011/2714.html>.

¹⁰ Sky, BT, EE, TalkTalk, O2 (Telefonica) et Virgin.

ne visaient pas les opérateurs de The Pirate Bay, mais une audience préliminaire a déterminé, sur la base des preuves présentées, que les utilisateurs et les opérateurs du site avaient porté atteinte au droit d'auteur. Le tribunal a estimé que cette façon de procéder était raisonnable sans pour autant constituer une étape essentielle pour les procédures à venir. La demande a abouti et The Pirate Bay a été déclaré solidairement responsable des infractions commises par les utilisateurs, étant donné qu'il avait autorisé les atteintes aux droits de copie et de communication au public commises par ses utilisateurs, allant bien au-delà du simple fait de rendre possible l'atteinte ou de prêter assistance à la commission de cette atteinte. Le tribunal a considéré que les demandeurs n'avaient aucunement l'obligation d'assigner les opérateurs du site The Pirate Bay. En effet, du point de vue juridictionnel, ni l'article 8.3) de la directive 2001/29/CE ni l'article 97A de la CDPA n'emportent obligation de citer en justice ou d'appeler en intervention les opérateurs ou les utilisateurs du site pirate.

IV. L'ÉVOLUTION DES ORDONNANCES

14. Depuis la première décision (*Newzbin2*), les FAI ne se sont pas opposés aux ordonnances sollicitées. C'est pourquoi, lorsque les circonstances sont identiques à celles d'affaires ayant fait l'objet de jugements publics motivés, la plupart des procédures sont instruites par voie de procédure écrite¹¹. On trouvera ci-après un résumé des principales décisions qui ont permis de faire évoluer ces ordonnances.

15. L'affaire *The Football Association Premier League Ltd c. British Sky Broadcasting & Ors [2013] EWHC 2058 (Ch)*¹² portait sur un site Internet (FirstRow) permettant d'accéder à des retransmissions de manifestations sportives en flux continu sans passer par les services de pair à pair, contrairement à *Newzbin2* et *The Pirate Bay*. En l'occurrence, le tribunal a conclu que, bien que les opérateurs de FirstRow ne soient pas à l'origine de la communication (la retransmission émanant d'autres sites d'hébergement), ils étaient solidairement responsables de l'acte de communication avec les opérateurs des sites d'hébergement.

16. L'affaire *Twentieth Century Fox Film Corporation & Ors c. Sky UK Ltd & Ors [2015] EWHC 1082 (Ch)*¹³ soulevait des questions différentes car, outre la demande faite aux FAI de bloquer l'accès aux sites de diffusion en continu et aux sites BitTorrent (sites d'hébergement), elle visait également les sites Web proposant l'application Popcorn Time (une application open source permettant aux utilisateurs d'accéder via un lecteur multimédia intégré à des films et des émissions télévisées grâce au protocole BitTorrent). Le tribunal n'a pas pu établir que les opérateurs du site Web de l'application Popcorn Time effectuaient un acte de communication au public, ni que ces sites autorisaient des atteintes au droit d'auteur. Il a toutefois constaté que les fournisseurs de Popcorn Time savaient pertinemment que cette application était un moyen essentiel pour permettre et encourager l'accès des utilisateurs aux sites d'hébergement et que tel était le but qu'ils poursuivaient, permettant ainsi des communications portant atteinte au droit d'auteur pour lesquelles ils étaient solidairement responsables. L'ordonnance demandée a été obtenue.

17. L'affaire *The Football Association Premier League Ltd c. British Telecommunications Plc & Ors [2017] EWHC 480 (Ch)* portait sur la réception illégale de matchs de football diffusés en continu à l'aide de décodeurs, de lecteurs multimédias et d'applications pour appareils mobiles. Les ordonnances de blocage traditionnelles ne permettent pas d'empêcher la plupart des atteintes car ces appareils ne passent pas par un site Web déterminé mais se connectent directement aux serveurs de diffusion en continu via leur adresse IP. L'ordonnance est

¹¹ Les règles de procédures civiles permettent au tribunal de connaître d'une demande sans audience si les parties sont d'accord sur ce point ou si le tribunal ne considère pas qu'une audience serait appropriée.

¹² <http://www.bailii.org/ew/cases/EWHC/Ch/2013/2058.html>.

¹³ <http://www.bailii.org/ew/cases/EWHC/Ch/2015/1082.html>.

applicable uniquement lors de la retransmission d'un match de première division. La liste des serveurs cibles à bloquer peut être réinitialisée chaque semaine, ce qui permet d'ajouter de nouveaux serveurs et de veiller à ce que les anciens serveurs dont les contenus diffusés ne portent plus atteinte au droit d'auteur ne soient pas bloqués. L'ordonnance était limitée dans le temps et ne couvrait que la saison de première division. Lorsqu'une adresse IP doit être bloquée, l'hébergeur doit être avisé. Les hébergeurs, opérateurs de sites Web ou de services de diffusion en continu ainsi que les abonnés des FAI qui s'estimaient lésés par l'ordonnance avaient la possibilité de demander l'autorisation de ne pas en tenir compte ou de la faire modifier. On s'attend à ce que de nouvelles ordonnances soient demandées en prévision de la nouvelle saison de football.

V. SITES INTERNET PORTANT ATTEINTE AUX MARQUES – CARTIER

18. À l'origine, toutes les injonctions demandées portaient sur des atteintes au droit d'auteur. En novembre 2014, dans l'affaire *Cartier International AG & Ors c. British Sky Broadcasting Ltd & Ors [2014] EWHC 3354 (Ch)*¹⁴, il s'agissait d'enjoindre aux FAI de bloquer l'accès aux sites Web qui vendaient des produits contrefaisant les marques Cartier. Cette affaire présentait un intérêt tout particulier pour le Royaume-Uni, où il n'existe aucune législation prévoyant expressément le blocage de sites qui portent atteinte à des marques. Ayant déterminé qu'il était compétent pour rendre une telle ordonnance, le tribunal a défini les conditions minimales devant être réunies pour qu'il exerce sa juridiction :

- Les FAI sont-ils des intermédiaires?
- Les opérateurs des sites Web visés portent-ils atteinte aux marques?
- Les opérateurs des sites Web visés utilisent-ils les services des FAI pour porter atteinte aux marques?
- Les FAI en ont-ils une connaissance effective?

19. Le tribunal a examiné plusieurs principes à appliquer avant de se prononcer : la mesure de réparation doit être nécessaire, efficace et dissuasive; elle ne doit pas être inutilement compliquée ou coûteuse; elle ne doit pas créer d'obstacles au commerce légitime; elle doit être juste et équitable et concilier les droits fondamentaux applicables; et elle doit être proportionnée.

20. Le tribunal s'est penché sur les autres mesures à la disposition des titulaires de droits. Celles-ci comprenaient notamment : procédures à l'encontre des opérateurs des sites; procédures de notification et de retrait par les hébergeurs; gel des paiements pour les comptes marchands des opérateurs; saisie des noms de domaine; désindexation par les moteurs de recherche; et saisie en douane. S'il a estimé que certaines de ces mesures méritaient d'être mises en œuvre, le tribunal n'a pas considéré qu'elles fussent aussi efficaces et moins contraignantes que l'ordonnance demandée.

21. Outre le blocage des sites Web visés, l'ordonnance s'étendait également à leurs domaines et sous-domaines ainsi qu'à toute autre adresse IP ou URL notifiée aux FAI. Elle autorisait également les abonnés lésés à demander au tribunal de révoquer ou modifier les ordonnances et comprenait une date limite, à moins que les FAI ne consentent à leur prolongation ou que le tribunal n'en décide ainsi.

22. L'ordonnance a été rendue mais les FAI ont ensuite interjeté appel au motif que le tribunal n'était pas compétent, que l'ordonnance était disproportionnée et que les FAI ne devraient pas avoir à supporter les coûts de mise en œuvre de l'ordonnance. La Cour d'appel a confirmé la

¹⁴ <http://www.bailii.org/ew/cases/EWHC/Ch/2014/3354.html>.

décision de la Haute Cour, l'un de ses juges ayant cependant émis une opinion dissidente sur la question de savoir qui devrait supporter les coûts de mise en œuvre. En février 2017, deux FAI ont été autorisés à déposer un recours devant la Cour suprême sur la question des coûts.

VI. EFFICACITÉ

23. Ces ordonnances sont considérées comme des outils précieux dans la panoplie de mesures permettant aux titulaires de protéger et faire appliquer leurs droits de propriété intellectuelle au Royaume-Uni mais, étant donné qu'elles impliquent des efforts et des coûts considérables, elles ne sont utilisées que pour les sites qui commettent les atteintes les plus graves.

24. Quelques incidents se sont produits dans un premier temps du fait d'interdictions excessives, des sites qui n'étaient pas visés par une ordonnance (et qui ne portaient pas atteinte au droit d'auteur) étant bloqués par inadvertance. Le problème a été résolu et ne semble plus s'être posé depuis.

25. Dans les affaires *Newzbin2* et *Cartier*, l'efficacité de ces ordonnances a été considérée comme un critère important pour évaluer leur proportionnalité. Dès lors que l'accès à un site avait été bloqué par ordonnance, on observait une diminution considérable du trafic en provenance du Royaume-Uni vers ce site. Aucune migration majeure des utilisateurs britanniques vers les serveurs proxy des sites bloqués n'a été constatée et, malgré une augmentation stable des recherches sur les réseaux privés virtuels (RPV) et Tor (réseau d'anonymisation), aucune corrélation n'a pu être établie avec les dates de mise en œuvre de l'une ou l'autre des ordonnances de blocage rendues au Royaume-Uni.

MÉCANISMES INSTITUTIONNELS MIS EN PLACE POUR LUTTER CONTRE LES ATTEINTES À LA PROPRIÉTÉ INTELLECTUELLE COMMISES EN LIGNE – DONNÉES D'EXPÉRIENCE D'EUROPOL

*Contribution établie par M. Chris Vansteenkiste, responsable d'équipe, Coalition coordonnée contre les atteintes à la propriété intellectuelle (IPC³), Europol, La Haye (Pays-Bas)**

RÉSUMÉ

Bien qu'elle ne figure pas parmi les priorités du cycle politique de l'Union européenne pour lutter contre la grande criminalité internationale organisée pour la période 2018-2021, la lutte contre les atteintes à la propriété intellectuelle reste un élément important pour Europol et ses partenaires chargés de l'application de la loi.

En 2016, la Coalition coordonnée contre les atteintes à la propriété intellectuelle (IPC³) a été créée à Europol dans le but d'exploiter pleinement les capacités opérationnelles et stratégiques d'Europol dans le domaine des atteintes aux droits de propriété intellectuelle. L'IPC³ place Europol au centre de la coordination des connaissances spécialisées et de l'expertise dans les enquêtes sur les atteintes à la propriété intellectuelle, tout en renforçant ses capacités de coordination et sa position en ce qui concerne la consignation des données des différentes parties prenantes, telles que le secteur privé et les associations de titulaires de droits de propriété intellectuelle.

La réussite des opérations menées récemment avec le concours de l'IPC³ dans le domaine de la lutte contre les atteintes à la propriété intellectuelle commises en ligne témoigne du rôle essentiel que jouent l'application du droit international et l'entraide judiciaire, ainsi que de la nécessité de renforcer la collaboration entre les autorités chargées de l'application de la loi et les nombreuses parties prenantes publiques ou privées œuvrant dans ce domaine.

I. ATTEINTES À LA PROPRIÉTÉ INTELLECTUELLE : UN PHÉNOMÈNE RÉPANDU

1. L'impact économique des atteintes à la propriété intellectuelle est particulièrement élevé dans l'Union européenne, où les produits contrefaisants et pirates représentent jusqu'à 5% des importations, pour un montant qui s'élève à 85 milliards d'euros¹.
2. Les atteintes aux droits de propriété intellectuelle ont une incidence négative sur les recettes des entreprises concernées et des répercussions sur le plan social et économique entraînant la disparition de milliers d'emplois. De plus, ces atteintes peuvent avoir de graves conséquences sur la santé et la sécurité des consommateurs, voire même entraîner la mort, car les produits contrefaisants sont fabriqués sans tenir compte des normes et des directives européennes en matière de santé et de sécurité.

* Les points de vue exprimés dans le présent document sont ceux de l'auteur et ne reflètent pas nécessairement ceux du Secrétariat ou des États membres de l'OMPI.

¹ OCDE/EUIPO, Le commerce de produits contrefaisants et piratés : analyse de l'impact économique, Éditions OCDE (2016), Paris.

3. Aujourd'hui, la plupart des produits contrefaisants sont achetés sur l'Internet et expédiés dans le monde entier. Cela rend les enquêtes en ligne d'autant plus importantes : il faut impérativement que les autorités chargées de l'application de la loi disposent d'outils, de formations et d'une législation qui leur permettent de mener des enquêtes efficaces.

II. COMMERCE EN LIGNE DE BIENS ET SERVICES ILLICITES : RAPPORT SOCTA UE 2017

4. En mars 2017, Europol a publié son rapport d'évaluation sur la menace que représente la grande criminalité organisée, dit "rapport SOCTA UE" (Serious and Organised Crime Threat Assessment (SOCTA)), dont le sous-titre était : "Criminalité organisée à l'ère des nouvelles technologies".

5. Cette étude approfondie des principales menaces qui pèsent sur l'Union européenne sert de fondement au cycle politique de l'Union européenne pour lutter contre la grande criminalité internationale organisée. Dans son rapport SOCTA UE 2017, Europol recommande de mettre l'accent sur cinq menaces criminelles prioritaires (la cybercriminalité, la production, le trafic et la distribution de drogues, le trafic de migrants, la criminalité organisée contre les biens et la traite des êtres humains) et trois menaces transversales (la criminalité financière dont le blanchiment de capitaux, la fraude documentaire et le commerce en ligne de biens et services illicites).

6. Le commerce en ligne de biens et services illicites, y compris de produits contrefaisants, est considéré comme une menace transversale, c'est-à-dire comme un élément permettant ou favorisant tous les autres types de grande criminalité organisée.

7. Le commerce de biens illicites en ligne a connu une progression constante ces dernières années et devrait connaître une progression rapide ces prochaines années. La multiplication des plateformes commerciales, y compris les plateformes hébergées sur des médias sociaux, a rendu le commerce en ligne plus facile, plus accessible et meilleur marché. Cette évolution s'est accompagnée d'un développement du commerce de produits illicites en ligne du fait que, à l'instar des honnêtes commerçants, les criminels cherchent à exploiter l'Internet pour développer leurs activités. Ces criminels sont en mesure de produire des produits de contrefaçon en grande quantité, à un coût minimum, et d'exploiter les plateformes en ligne pour écouler facilement et efficacement leurs produits dans le monde entier.

8. Dans son rapport SOCTA UE 2017, Europol suggérait de mettre l'accent sur la vente des produits contrefaisants dans le cadre de la menace transversale que représente le commerce en ligne de biens et services illicites. Toutefois, à l'issue des délibérations du groupe d'appui du Comité permanent de coopération opérationnelle en matière de sécurité intérieure (COSI) qui s'est réuni le 12 mai 2017, le Conseil de l'Union européenne a décidé de ne pas mettre l'accent sur cette question dans le cadre de la lutte contre la grande criminalité internationale organisée pour la période 2018-2021.

III. COALITION COORDONNÉE CONTRE LES ATTEINTES À LA PROPRIÉTÉ INTELLECTUELLE

9. Pour répondre à ces nouvelles tendances et conformément à sa stratégie pour la période 2016-2020, Europol a créé une nouvelle structure : la Coalition coordonnée contre les atteintes à la propriété intellectuelle (IPC³).

10. Cette nouvelle équipe, créée en juillet 2016, est rattachée au Département des opérations d'Europol, au sein du Centre européen de lutte contre la grande criminalité, et s'appuie sur les travaux réalisés dans le cadre du projet analytique COPY, qui reste la plateforme opérationnelle

en matière d'analyse criminelle. L'IPC³ bénéficie d'un soutien financier sous forme de subvention annuelle de la part de l'Office de l'Union européenne pour la propriété intellectuelle (EUIPO).

11. Europol dispose ainsi de moyens d'action accrus, notamment grâce à une augmentation de ses effectifs, qui lui permettent de lutter plus efficacement contre la contrefaçon et le piratage en ligne et hors ligne.

12. Dans ce domaine précis de la criminalité, les autorités chargées de l'application de la loi dépendent dans une large mesure de la contribution des nombreuses parties prenantes publiques ou privées (par exemple les titulaires de droits de propriété intellectuelle, les services d'enregistrement et observatoires, ainsi que les autorités chargées de la santé et de la sécurité). L'IPC³ joue ainsi un rôle central dans la coordination des échanges d'informations, notamment en centralisant les connaissances spécialisées et en apportant une expertise dans le cadre des enquêtes.

13. L'IPC³ a pour mission

- de fournir un appui opérationnel et technique aux autorités compétentes;
- de faciliter et de coordonner les enquêtes transfrontalières;
- de surveiller les tendances en matière de criminalité en ligne et l'apparition de nouveaux modes opératoires et d'établir des rapports à cet égard;
- d'œuvrer à l'harmonisation et à la normalisation des instruments juridiques et des procédures opérationnelles pour lutter contre les atteintes à la propriété intellectuelle à l'échelle mondiale; et
- de mener des actions de sensibilisation auprès du public et des autorités chargées de l'application de la loi en organisant des campagnes de sensibilisation et en proposant des formations dans ce domaine de compétences spécifique.

IV. ACTIVITÉS MENÉES PAR L'IPC³ POUR LUTTER CONTRE LES ATTEINTES AUX DROITS DE PROPRIÉTÉ INTELLECTUELLE EN LIGNE

14. Les marchés en ligne sont l'un des principaux circuits de distribution pour les produits contrefaisants. Le volume des ventes de produits contrefaisants en ligne a fortement augmenté ces dernières années. Les contrefacteurs exploitent souvent les plateformes des médias sociaux pour faire la promotion de leurs produits. Des milliers de boutiques en ligne sont utilisées pour écouler des produits contrefaisants. Le recours croissant aux services postaux et de livraison de colis rend plus difficile la détection des produits contrefaisants dans le flux postal.

15. L'IPC³ prévoit, dans le cadre de sa stratégie, un certain nombre d'activités et de tâches en ce qui concerne les atteintes aux droits de propriété intellectuelle en ligne et les systèmes de paiement en ligne. Ses moyens d'action quant à la surveillance de l'Internet ont par conséquent été renforcés et devraient être renforcés davantage.

16. Parmi les moyens mis en œuvre, on peut citer un large éventail d'activités, allant de la surveillance de l'Internet à la collecte de renseignements. L'IPC³ procède régulièrement à des contrôles sur les plateformes en libre accès afin de collecter autant de données que possible concernant les adresses IP, les sites Web, les comptes de courrier électronique, les abonnés, les adresses postales, les numéros de téléphone, les serveurs et autres données pertinentes.

Ces vérifications sont utiles dans le cadre des enquêtes car elles permettent d'étoffer les dossiers reçus des membres du réseau de l'IPC³ et d'accroître à la fois la qualité et la quantité des renseignements disponibles.

17. Les activités de collecte de renseignements comprennent la surveillance des réseaux de médias sociaux les plus populaires, des annonces publicitaires et des plateformes d'échange de devises virtuelles. Ces activités visent non seulement à permettre aux États membres et aux tiers de mettre la main plus facilement sur les sites Web sur lesquels sont commises des infractions, mais également à aider les autorités compétentes à suivre la trace de l'argent en leur donnant accès à des renseignements importants et à des données sur les nouvelles tendances en ce qui concerne les systèmes de paiement en ligne.

18. L'IPC³ s'efforce également de mener des actions de sensibilisation auprès du public et des autorités chargées de l'application de la loi en diffusant des messages d'alerte précoce, en proposant des formations et en établissant des rapports stratégiques sur les atteintes à la propriété intellectuelle commises en ligne.

V. CIBLER LES SITES SUR LESQUELS IL EST PORTÉ ATTEINTE AUX DROITS DE PROPRIÉTÉ INTELLECTUELLE; OPÉRATION "IN OUR SITES (IOS)"

19. Depuis 2012, l'opération "In Our Sites (IOS)" a permis à plusieurs reprises de stopper la vente de produits contrefaisants et pirates sur des plateformes de commerce en ligne et des réseaux de médias sociaux. Cette opération est coordonnée par l'IPC³, qui travaille en étroite collaboration avec les services d'immigration et des douanes des États-Unis d'Amérique (US ICE) et Interpol.

20. En 2016, 27 États membres de l'Union européenne et pays tiers et 24 partenaires privés volontaires ont participé à cette opération. En collectant des listes auprès des titulaires de droits de propriété intellectuelle, les autorités chargées de l'application de la loi sont parvenues, avec le concours d'Europol s'agissant de la collecte et du recoupement des renseignements, à fermer 5158 sites Web qui vendaient des marchandises contrefaisantes, à procéder à l'arrestation de 10 personnes et à saisir des produits pour un montant de plus de 1,75 million d'euros.

21. Les utilisateurs du Web qui tentent de se rendre sur des sites Web qui ont été fermés sont maintenant redirigés vers un site sur lequel s'affiche un message les informant que le site Web auquel ils tentent d'accéder a été fermé par les autorités.

22. La coopération avec les représentants des titulaires de droits de propriété intellectuelle est essentielle pour pouvoir surveiller les sites Web sur lesquels sont commises des infractions et les signaler aux autorités internationales via Europol, et joue un rôle central dans l'opération "In Our Sites". Les partenariats établis avec le secteur privé concernent non seulement les titulaires de droits de propriété intellectuelle, mais également des intermédiaires et des organismes œuvrant dans le domaine de la protection des droits de propriété intellectuelle.

23. Depuis 2012, l'opération "In Our Sites" a connu plusieurs améliorations qui ont été possibles grâce à une analyse des précédentes éditions de l'opération. Cependant, l'évolution constante des modes opératoires de la criminalité suppose un développement permanent des activités opérationnelles.

24. Pour l'heure, il est prévu de consolider les partenariats public-privé établis par l'IPC³ et de renforcer les mesures à l'égard des plateformes de médias sociaux qui font la promotion de produits contrefaisants et qui vendent ces produits.

VI. SUCCÈS DES OPÉRATIONS MENÉES RÉCEMMENT DANS LE DOMAINE DE LA LUTTE CONTRE LE PIRATAGE AUDIOVISUEL

25. Les efforts déployés par l'IPC³ pour lutter contre les atteintes aux droits de propriété intellectuelle commises en ligne ne se limitent pas à la fermeture des sites Web sur lesquels sont vendus des produits contrefaisants, mais englobent également la lutte contre le piratage audiovisuel, domaine dans lequel plusieurs opérations ont été menées avec succès au cours de ces dernières années.

A. OPÉRATION CASPER (2017)

26. L'opération Casper est un exemple parfait de coopération transfrontalière dans le domaine de la lutte contre la diffusion illicite de chaînes de télévision à péage.

27. Une enquête commune dirigée par la police nationale espagnole, avec le concours des autorités bulgares, l'IPC³ et Eurojust, a permis de démanteler un réseau criminel responsable de la diffusion illégale de plus de 1000 chaînes de télévision à péage à l'échelle européenne, au moyen de la technologie de la télévision sur protocole Internet (IPTV). Dans le cadre d'une opération coordonnée, huit suspects ont été arrêtés et 12 perquisitions effectuées simultanément en Espagne et en Bulgarie. Les enquêteurs ont saisi les serveurs utilisés pour fournir un accès illégal à ces chaînes de télévision, ainsi que de nombreux documents.

28. L'IPC³ a contribué à la réalisation des enquêtes en fournissant des services de coordination et de soutien, en offrant une expertise scientifique et en facilitant l'échange de renseignements entre les autorités chargées de l'application de la loi et les partenaires du secteur privé. Le jour de l'opération, des experts d'Europol équipés de bureaux mobiles se sont rendus en Espagne et en Bulgarie pour soutenir les opérations sur le terrain.

B. OPÉRATION FAKE (2016)

29. Une autre opération couronnée de succès dans le domaine de la lutte contre le piratage audiovisuel a été l'opération FAKE.

30. Une enquête commune dirigée par la police nationale et l'administration fiscale espagnoles, avec le concours de la police locale allemande de Hanau, l'IPC³ et Eurojust, a permis de démanteler un réseau criminel spécialisé dans la diffusion illégale de chaînes de télévision à péage en Espagne. Ces chaînes étaient accessibles au moyen de décodeurs pirates (partage de cartes) et par l'Internet.

31. Dans le cadre d'une opération conjointe menée en mai 2016, 38 perquisitions ont été effectuées simultanément dans sept villes d'Espagne. Europol a contribué à la réalisation des enquêtes en envoyant sur place deux experts équipés de bureaux mobiles. Ceux-ci ont pu analyser les renseignements et les comparer en temps réel aux données contenues dans les bases de données d'Europol, et également extraire des données des téléphones et autres dispositifs de stockage de données.

32. Au total, 30 suspects ont été arrêtés en Espagne et 48 800 décodeurs saisis, de même que 183 200 euros en liquide, 10 voitures de luxe, une voiture de luxe contrefaisante, un avion privé, plusieurs documents financiers et du matériel informatique. Il a été révélé que les criminels utilisaient des centres de minage de bitcoin pour blanchir les profits tirés de leurs activités illégales et les transformer en monnaie virtuelle. Dans le cadre des enquêtes, les autorités espagnoles ont démantelé six centres de minage de bitcoin (le plus grand nombre en Europe jusqu'ici) et saisi 78,3 bitcoins.

33. Les personnes arrêtées importaient des décodeurs de Chine, concevaient les microprogrammes utilisés pour décoder les signaux télévisuels et distribuaient ces décodeurs aux utilisateurs finals via des pages Web et des forums Internet spécifiques qu'ils contrôlaient. Ce groupe criminel utilisait également la technologie de la télévision sur protocole Internet (IPTV) pour proposer illicitement plus de 1600 chaînes de télévision de différents pays. Il utilisait des serveurs situés dans différents pays d'Europe, notamment en Allemagne, où un serveur a été fermé à la demande des autorités espagnoles.

VII. FORMATION DISPENSÉE PAR L'IPC³ À L'INTENTION DES RESPONSABLES DE L'APPLICATION DE LA LOI

34. L'IPC³ organise régulièrement des formations sur les atteintes à la propriété intellectuelle commises en ligne, à l'intention des autorités chargées de l'application de la loi.

35. Par exemple, les 11 et 12 mai 2017, au siège d'Europol à La Haye, une formation approfondie sur le piratage audiovisuel a été dispensée à des responsables de l'application de la loi, y compris à des procureurs de toute l'Europe, avec le concours de l'Audiovisual Anti-Piracy Alliance (AAPA) et de l'EUIPO.

36. Cette formation d'une journée et demie comprenait des séances sur les technologies mises en œuvre pour protéger les contenus et notamment sur la façon dont les services de télévision à péage collaborent avec des intermédiaires tels que les fournisseurs de services d'hébergement, les fournisseurs de services de paiement et les annonceurs pour perturber l'approvisionnement en contenus pirates, sur la façon d'enquêter sur les actes de piratage et d'analyser ces actes et sur la façon de collecter et de conserver des preuves, y compris à l'aide d'outils d'analyse en temps réel (live forensics). Des affaires en cours concernant la retransmission illicite de contenus et le partage de cartes ont également été analysées de manière approfondie dans le cadre de réunions en petits groupes.

MESURES VOLONTAIRES INTERSECTORIELLES POUR LUTTER CONTRE LE PIRATAGE EN LIGNE

*Contribution établie par M. Dean S. Marks, directeur général adjoint, conseiller juridique adjoint, chef, protection globale des contenus, Motion Picture Association of America, Inc. (MPAA), Los Angeles (États-Unis d'Amérique)**

RÉSUMÉ

Le piratage d'œuvres protégées par le droit d'auteur a atteint des niveaux alarmants du fait de l'augmentation de la bande passante et de l'accessibilité de l'Internet, ce qui pose de véritables défis en matière d'application des droits. Outre les méthodes conventionnelles d'application des droits, il est essentiel de développer les offres légales en ligne et de les accompagner de mesures volontaires efficaces pour faire reculer le nombre d'atteintes commises en ligne. Contrairement aux lois et aux règlements, les mesures volontaires peuvent être rapidement adaptées aux nouvelles formes de piratage en ligne. Ces mesures présentent un intérêt non seulement pour les titulaires de droits, mais également pour les intermédiaires sur l'Internet, les fournisseurs de services, les gouvernements et les utilisateurs de l'Internet. Les gouvernements devraient par conséquent encourager le recours aux mesures volontaires comme moyen efficace pour lutter contre les atteintes en ligne au droit d'auteur.

I. DÉFIS EN MATIÈRE D'APPLICATION DES DROITS POSÉS PAR LE PIRATAGE EN LIGNE

1. Avant l'ère numérique, les auteurs et les titulaires de licence autorisés exerçaient un certain contrôle sur l'utilisation qui était faite de leurs œuvres dans les différents pays. Certes, des atteintes étaient commises, mais celles-ci ne dépassaient généralement pas les frontières. Lorsque des copies illégales étaient produites dans un pays dans le but d'être distribuées dans un autre pays, les titulaires des droits pouvaient en principe compter sur les autorités douanières pour mettre un terme aux importations ou pour appliquer la loi à l'encontre de ceux qui distribuaient localement des copies illégales.

2. Mais la difficulté d'appliquer les droits d'auteur ne vient pas seulement du caractère transnational et instantané de l'Internet. Aujourd'hui plus que jamais, les composants et les opérations sur lesquelles reposent les sites Web pirates sont répartis dans plusieurs pays. Il n'est pas rare, par exemple, que l'exploitant d'un site pirate de diffusion en continu réside dans un premier pays, alors que le site est hébergé par un fournisseur de services situé dans un deuxième pays. Souvent, les fichiers des contenus portant atteinte aux droits d'auteur auxquels un site pirate accède sont hébergés par un fournisseur de services de stockage en nuage situé dans un troisième pays. Par ailleurs, les sites pirates utilisent souvent des réseaux de diffusion de contenu et des systèmes de serveur mandataire inverse situés dans un quatrième pays. De plus, le nom de domaine du site peut être géré par un organisme d'enregistrement de noms de domaine situé dans un cinquième pays. Un constat s'impose donc : les nouvelles formes de piratage remettent en cause le principe même de territorialité du droit d'auteur et rendent plus difficile l'application efficace des droits d'auteur.

* Les points de vue exprimés dans le présent document sont ceux de l'auteur et ne reflètent pas nécessairement ceux du Secrétariat ou des États membres de l'OMPI ni la position de la Motion Picture Association of America (MPAA) ou de ses sociétés membres.

II. MESURES VOLONTAIRES POUR LUTTER CONTRE LE PIRATAGE EN LIGNE

3. Compte tenu de ce qui précède, encourager les intermédiaires sur l'Internet, les fournisseurs de services et les entreprises à cesser toute relation commerciale avec les sites Web qui portent massivement atteinte au droit d'auteur apparaît comme la stratégie la plus appropriée pour lutter contre le piratage en ligne. Pour certains, cette démarche revient à "suivre la piste de l'argent". Mais cette stratégie ne se résume pas simplement à faire coopérer les plateformes de paiement et les agences de publicité en ligne. Les fournisseurs de services d'hébergement, les registres et bureaux d'enregistrement de noms de domaine, les réseaux de diffusion de contenu, les services de stockage en nuage et même les fournisseurs d'accès à l'Internet et les moteurs de recherche peuvent tous participer à cet effort en prenant des mesures pour éviter que leurs plateformes et leurs services soient utilisés d'une façon qui porte atteinte au droit d'auteur.

A. PLATEFORMES DE PAIEMENT

4. Des progrès importants ont été accomplis dans le domaine des mesures volontaires, notamment en ce qui concerne les plateformes de paiement. Mastercard et Visa, deux des solutions de paiement les plus utilisées au monde, ont collaboré activement avec la Motion Picture Association of America (MPAA) afin de mettre en œuvre des politiques efficaces pour éviter que leurs services et leurs systèmes soient utilisés par des sites Web qui portent atteinte au droit d'auteur. En outre, Visa et Mastercard acceptent tous deux que la MPAA leur signale les sites d'hébergement de fichiers (cyberlockers en anglais)¹ qui portent atteinte au droit d'auteur et qui acceptent les paiements Visa ou Mastercard. Paypal accepte également ce type d'information et a été la première plateforme de paiement à mettre un terme à ses relations avec des sites d'hébergement portant atteinte au droit d'auteur. Les exploitants de sites Web pirates ont souvent recours à toutes sortes de tactiques pour contourner ces obstacles. Néanmoins, Mastercard, Visa et Paypal procèdent à des vérifications en amont et coopèrent étroitement avec les titulaires de droits qui leurs signalent des sites d'hébergement de fichiers qui portent atteinte au droit d'auteur. Ainsi, l'application de ces mesures volontaires a permis de faire reculer sensiblement le trafic des utilisateurs sur de nombreux sites d'hébergement de fichiers.

B. AGENCES DE PUBLICITÉ EN LIGNE

5. Des progrès importants ont également été accomplis dans le domaine de la publicité en ligne. En 2012, les principales agences de publicité et associations de publicité des États-Unis d'Amérique se sont engagées à prendre les mesures nécessaires pour empêcher les exploitants de sites Web portant atteinte au droit d'auteur de bénéficier des revenus

¹ L'une des définitions les plus succinctes de "cyberlocker" est la suivante : "Contrairement aux services de stockage en nuage légaux, dont les clients sont des personnes physiques ou morales qui souhaitent stocker, consulter ou partager des données, le modèle commercial des sites d'hébergement de fichiers, dits 'cyberlockers' en anglais, consiste à attirer les clients qui souhaitent, sous le couvert de l'anonymat, télécharger ou diffuser en continu les fichiers les plus populaires qui sont mis en ligne par d'autres utilisateurs et qui portent atteinte au droit d'auteur. Ce modèle commercial repose sur le vol de contenu. En fait, ces sites d'hébergement de fichiers rémunèrent ou incitent de différentes manières les personnes qui diffusent le contenu illicite le plus demandé tout en dissuadant les utilisateurs de recourir à leurs services pour le stockage de données licites". Voir la page 1 du rapport intitulé "Behind the Cyberlocker Door : A Report on How Shadowy Cyberlocker Businesses Use Credit Card Companies to Make Millions" A NetNames Report for Digital Citizens Alliance, à l'adresse suivante : <https://www.netnames.com/assets/shared/whitepaper/pdf/dca-netnames-cyber-profilability-1.compressed.pdf>, septembre 2014.

publicitaires tirés des publicités concernant des produits et des services légaux². Mais compte tenu de la complexité de l'écosystème de la publicité en ligne, beaucoup restait encore à faire pour stopper ce flux important de revenus publicitaires vers les sites pirates. C'est ainsi que plusieurs acteurs majeurs de cet écosystème, notamment l'Association of National Advertisers (ANA), l'American Association of Advertising Agencies (AAAA) et l'Internet Advertising Bureau (IAB), ainsi que des membres de la MPAA, des titulaires de droits et des plateformes technologiques ont décidé d'unir leurs forces pour lancer le Trustworthy Accountability Group (TAG)³. Le programme intitulé "Brand Integrity Program Against Piracy", élaboré par le Trustworthy Accountability Group (TAG), vise à aider les agences de publicité et leurs partenaires technologiques à éviter les sites Web qui présentent un risque trop élevé d'atteinte au droit d'auteur et contribue ainsi à appliquer la stratégie qui consiste à "suivre la piste de l'argent" afin de priver les exploitants de sites pirates de leurs revenus publicitaires. Le Trustworthy Accountability Group (TAG) offre une solution volontaire émanant de l'industrie pour stopper les flux de revenus publicitaires qui font que la diffusion en ligne de contenus portant atteinte au droit d'auteur reste aujourd'hui encore une activité financièrement viable.

6. D'autres pays ont adopté des solutions différentes pour inciter les agences de publicité en ligne à cesser toute relation commerciale avec des sites Web pirates. Au Royaume-Uni, l'Operation Creative et l'Infringing Website List (IWL) ont déjà porté leurs fruits. L'Operation Creative est le fruit d'un partenariat entre une unité de police spécialisée dans la lutte contre les atteintes à la propriété intellectuelle (PIPCU) de la police de la ville de Londres, des titulaires de droits et le secteur britannique de la publicité. Il permet aux titulaires de droits de recenser les sites Web portant atteinte au droit d'auteur et de les signaler, preuves détaillées à l'appui, à la PIPCU. Cette dernière se charge alors d'examiner en toute indépendance les sites Web concernés et tente d'entrer en relation avec leurs exploitants pour les inciter à corriger leur comportement. Si les atteintes persistent, la PIPCU inscrit le site Web sur la liste des sites qui portent atteinte au droit d'auteur (IWL). Les agences de publicité ont accès à cette liste via un portail en ligne et peuvent l'utiliser comme ressource pour déterminer quels sont les sites Web sur lesquels elles ne souhaitent pas afficher de la publicité compte tenu de la nature illicite des activités de ces sites. L'Operation Creative et l'Infringing Website List (IWL) ont permis de faire reculer de 73% le nombre de publicités affichées par les principales agences de publicité au Royaume-Uni sur des sites Web portant atteinte au droit d'auteur⁴. Le succès de ces deux initiatives vient à la fois du soutien apporté par le gouvernement et de la crédibilité dont elles jouissent grâce à la participation de la PIPCU. Dernièrement, la MPAA a travaillé avec des gouvernements et des agences de publicité à Hong Kong (Chine) et au Viet Nam pour créer des listes de sites portant atteinte au droit d'auteur à l'échelle locale et régionale.

C. NOMS DE DOMAINE

7. L'un des meilleurs moyens de désorganiser un site Web pirate est de suspendre son nom de domaine. La MPAA a collaboré avec des services d'enregistrement des noms de domaine à l'élaboration de mesures volontaires visant à suspendre les sites Web se livrant à des activités portant atteinte clairement et de façon généralisée au droit d'auteur. En 2016, la MPAA a conclu un accord dit de "Trusted Notifier" avec Donuts, le service auprès duquel a été enregistré le plus grand nombre de nouveaux domaines de premier niveau (TLD). En vertu de cet accord volontaire, la MPAA est habilitée à signaler les sites Web se livrant à des activités portant clairement atteinte au droit d'auteur, qui opèrent dans des TLD administrés par Donuts, après

² Voir le site <https://www.ana.net/content/show/id/23408>, avril 2012.

³ Voir la section intitulée "Fight Internet Piracy", sur le site du Trustworthy Accountability Group (TAG) à l'adresse <https://www.tagtoday.net/piracy/>.

⁴ Voir l'article intitulé "Operation Creative sees 73 Percent Drop in Top UK Advertising on Illegal Sites", à l'adresse <https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/pipcu-news/Pages/Operation-Creative-sees-73-per-cent-drop-in-top-UK-advertising-on-illegal-sites.aspx>, août 2015.

que la MPAA ait tenté de prendre contact avec le fournisseur d'accès et l'unité d'enregistrement du site Web pirate afin de régler le problème. Par ailleurs, en vertu dudit accord, la MPAA soumet à Donuts des éléments de preuve et une déclaration selon laquelle le site Web signalé a fait l'objet d'une vérification humaine par la MPAA⁵. L'accord de "Trusted Notifier" s'est révélé fructueux, permettant de suspendre des TLD de sites Web pirate. Un accord similaire a été conclu avec Radix le plus grand service d'enregistrement de nouveaux domaines génériques de premier niveau, ayant son siège à Dubaï, qui administre les domaines .online, .tech, .space, .web et plusieurs autres TLD⁶. La MPAA a également conclu des accords informels de notification volontaire avec d'autres services d'enregistrement. En conséquence, plus de 25 TLD de sites Web pirates ont été suspendus jusqu'ici en vertu de ces mesures volontaires. Si les sites pirates peuvent changer de TLD, ce qu'ils font généralement, le passage à un domaine différent provoque des frictions.

D. FOURNISSEURS DE SERVICES D'HÉBERGEMENT

8. Les fournisseurs de services d'hébergement constituent une autre catégorie d'intermédiaires sur l'Internet dont dépendent les sites Web pirates. Pour les sites d'hébergement de fichiers, la perte du fournisseur de services d'hébergement peut être dévastatrice parce que ces sites ont besoin de volumes élevés en matière de capacité de serveur. Pour les sites de lecture en continu et les sites offrant des liens, le retrait d'un fournisseur de services d'hébergement est moins dommageable, ces sites, qui réapparaissent souvent rapidement chez des fournisseurs d'accès moins coopératifs ou non coopératifs, étant "légers" dans la mesure où ils ne stockent pas eux-mêmes les contenus pirates. Néanmoins, la perte d'un fournisseur de services d'hébergement peut avoir un effet perturbateur parce qu'il s'agit d'un intermédiaire décisif dont dépendent tous les sites Web pirates.

9. Selon l'expérience de la MPAA, la coopération volontaire des fournisseurs de services d'hébergement s'agissant d'arrêter la fourniture de services aux sites Web se livrant à des activités de piratage fait généralement suite à une décision judiciaire selon laquelle un fournisseur de services d'hébergement donné doit arrêter de fournir des services à un ou plusieurs sites Web pirates déterminés. C'est surtout le cas en Europe où le régime juridique autorise les titulaires de droits à solliciter devant un tribunal une injonction contre les intermédiaires et les fournisseurs de services à l'égard des activités de piratage en ligne, sans être tenus de démontrer la responsabilité de ces intermédiaires, qu'elle soit directe ou secondaire. Ce régime juridique s'est révélé précieux pour jeter les bases d'une collaboration entre les titulaires de droits et les fournisseurs de services en Europe. Par conséquent, des programmes de signalement autorisés ont été mis en place entre la MPAA et un certain nombre de fournisseurs de services d'hébergement dans toute l'Europe.

III. INCITATIONS À L'ADOPTION DE MESURES VOLONTAIRES

10. Réduire la portée des activités de piratage en ligne et les dégâts qui en résultent devrait clairement inciter les titulaires du droit d'auteur à adopter des mesures volontaires. Mais quels avantages les fournisseurs de services, les intermédiaires sur l'Internet, les organismes de paiement, les annonceurs en ligne et autres peuvent-ils tirer de telles mesures?

⁵ Voir *Donuts and the MPAA—Striking the Right Balance*, <http://www.donuts.domains/donuts-media/blog/donuts-and-the-mpaa-striking-the-right-balance>, février 2016.

⁶ Voir *Radix and the MPAA Establish New Partnership to Reduce Online Piracy*, <http://www.prnewswire.com/news-releases/radix-and-the-mpaa-establish-new-partnership-to-reduce-online-piracy-579359971.html>, mai 2016.

11. Plusieurs facteurs ont incité ces parties à adopter des mesures volontaires afin de collaborer avec les titulaires de droit d'auteur. Tout d'abord, un grand nombre d'entreprises ne souhaitent pas être associées aux auteurs d'actes illicites, y compris des activités de piratage du droit d'auteur. En outre, fermer les yeux sur des transactions avec des sites Web pirates peut avoir des conséquences négatives. Aux États-Unis d'Amérique, par exemple, des intermédiaires ont été qualifiés de complices non accusés dans des procédures pénales pour atteinte au droit d'auteur. Par ailleurs, les fournisseurs de services et les intermédiaires sur l'Internet considèrent souvent la collaboration volontaire avec les titulaires de droits comme une meilleure option qu'une possible réglementation gouvernementale ou une procédure coûteuse par laquelle leur éventuelle responsabilité (directe ou secondaire) dans une atteinte au droit d'auteur est mise en cause, ou encore la perte de la protection assurée au titre de la "sphère de sécurité" ("safe harbor"). De fait, la collaboration volontaire entre les titulaires de droits et les fournisseurs de services et les intermédiaires sur l'Internet présentent des avantages mutuels dans la mesure où elle permet de créer un écosystème sur l'Internet plus propice aux transactions légales et offrant davantage de sécurité aux consommateurs⁷.

IV. COMMENT LES GOUVERNEMENTS PEUVENT ENCOURAGER LES MESURES VOLONTAIRES ET QUELS AVANTAGES EN DÉCOULENT

12. Les gouvernements peuvent encourager l'adoption de mesures volontaires par les titulaires de droit d'auteur et les intermédiaires sur l'Internet et autres fournisseurs de services en vue de réduire le piratage en ligne de diverses manières. Ils peuvent procéder à des auditions pour découvrir comment les sites Web pirates bénéficient de l'appui d'intermédiaires sur l'Internet et de fournisseurs de services locaux (tels que des services de paiement et des annonceurs) et encourager la collaboration avec les titulaires de droit d'auteur afin de mettre un terme à cet appui aux sites Web pirates. Les gouvernements peuvent également édicter des lois ou des règlements de haut niveau prévoyant le principe de "responsabilité sans faute" analogue à celui adopté par l'Europe à l'article 8.3 de la directive européenne sur le droit d'auteur⁸. Par ailleurs, les gouvernements peuvent confier comme mission aux organismes chargés de veiller au respect de la loi de collaborer avec les intermédiaires sur l'Internet et les fournisseurs de services en vue de les encourager à adopter des mesures volontaires pour cesser de faire des affaires avec les sites pirates. La démarche adoptée à cet égard par le Gouvernement du Royaume-Uni par l'intermédiaire du PIPCU, décrite plus haut, en constitue un exemple.

13. Les mesures volontaires efficaces prises en vue de réduire le piratage en ligne sont dans l'intérêt aussi bien des gouvernements que des citoyens dans leur ensemble. En ce qui concerne les gouvernements, l'adoption de mesures volontaires efficaces donne lieu à une diminution des demandes d'application de la loi à l'égard d'actes de piratage et, potentiellement, à une moins grande nécessité de législation ou de réglementation. En outre, compte tenu du fait que des mesures volontaires efficaces permettent souvent de réduire la nécessité d'intenter des actions en justice, elles aboutissent à une réduction des contraintes pesant sur le système judiciaire. Enfin, à mesure que le piratage en ligne diminue, les transactions légales en ligne portant sur des œuvres protégées au titre du droit d'auteur

⁷ Les utilisateurs de sites Web pirates sont 28 fois plus susceptibles d'être exposés aux logiciels malveillants. Voir le rapport de Digital Citizen Alliance, "Digital Bait : How content theft sites and malware are exploited by cybercriminals to hack into Internet users' computers and personal data", à l'adresse <https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/0f03d298-aedf-49a5-84dc-9bf6a27d91ff.pdf>, décembre 2015.

⁸ Voir la 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 à l'adresse <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML>

augmentent⁹, ce qui rapporte aux gouvernements des impôts et autres avantages liés aux transactions commerciales. Pour les consommateurs, la réduction du piratage en ligne diminue les risques liés aux logiciels malveillants et autres atteintes à la vie privée.

V. CONCLUSION

14. Il n'existe pas de solution miracle pour mettre fin au piratage en ligne. L'adoption de mesures d'application de la loi et la mise en œuvre de procédures civiles ciblées demeurent des moyens décisifs de régler les cas les plus difficiles et de créer la jurisprudence nécessaire. Toutefois, au regard de l'ampleur du phénomène de piratage en ligne, il est essentiel de combiner l'augmentation de l'offre en ligne de produits licites avec des mesures volontaires efficaces en vue de réduire le niveau global d'atteintes en ligne. Les mesures volontaires ne se limitent pas nécessairement au territoire national et peuvent être suffisamment flexibles pour constituer un moyen viable de réduire la facilité et la rentabilité du piratage en ligne. Contrairement aux lois et règlements, les mesures volontaires peuvent s'adapter rapidement à l'évolution constante des modes de piratage en ligne¹⁰. Par ailleurs, comme indiqué dans le présent document, les mesures volontaires constituent une formule gagnante dans la mesure où elles sont avantageuses non seulement pour les titulaires de droits, mais aussi pour les intermédiaires sur l'Internet, les fournisseurs de services, les gouvernements et les utilisateurs de l'Internet. Les mesures volontaires doivent dès lors être encouragées par les gouvernements en tant que moyens essentiels de lutte contre le fléau du piratage en ligne du droit d'auteur.

[Fin du document]

⁹ Voir, par exemple, l'étude réalisée par l'Université Carnegie Mellon qui a établi que le blocage de 19 sites pirates au Royaume-Uni a donné lieu à une augmentation des transactions légales en ligne, "Website Blocking Revisited : The Effect of the UK November 2014 Blocks on Consumer Behavior" <https://techpolicyinstitute.org/wp-content/uploads/2016/04/UK-Blocking-2-0-2016-04-06-mds.pdf>, avril 2016.

¹⁰ Par exemple, Amazon, eBay et Facebook ont récemment modifié leurs politiques ou conditions de service afin d'interdire la vente et la publicité de dispositifs contenant des applications pirates facilitant la lecture en continu de contenus illicites. Voir à l'adresse <http://variety.com/2017/digital/news/facebook-bans-kodi-piracy-devices-1202445930/>, mai 2017. Ces changements résultent en partie de la collaboration entre les titulaires de droits et les trois plateformes en ligne.