Le pirate informatique, un explorateur des courants juridiques du réseau

Primavera de Filippi, Melanie Dulong de Rosnay

Le pirate informatique, un explorateur des courants juridiques du réseau

Primavera De Filippi

Centre d'études et de recherches de sciences administratives et politiques / CNRS / Université Paris 2
pdefilippi@gmail.com

Melanie Dulong de Rosnay

Institut des Sciences de la Communication du CNRS
melanie.dulong@cnrs.fr

> Le bateau c'est la liberté, pas seulement le moyen d'atteindre un but.
> Bernard Moitessier, navigateur, *Tamata et l'Alliance*, p. 170.

Résumé

L'article étudie la figure du pirate informatique, ses différentes facettes et son évolution sous l'influence du traitement de la technique par le droit. L'analyse s'opère selon l'angle des relations entre les normes juridiques, techniques, et sociales, en se concentrant sur l'influence réciproque des nouvelles technologies qui contournent le droit et des règles du droit qui, en essayant de réguler ces nouvelles technologies, finissent par s'étendre à de nouveaux territoires auparavant non régulés. Des premières radios libres ou pirates aux plateformes de partage de fichiers entre pairs, on observe une régularité dans les tensions et les décalages entre les innovations techniques, d'abord à la marge, et la législation en vigueur. L'extension du champ de la régulation juridique provoque une évolution de la technique, et une généralisation de l'usage de ces techniques pour exercer certains droits menacés par les législations anti-pirates.

The article examines the figure of the computer pirate, its facets and its evolution under the influence of technical developments and the regulation thereof. The analysis is carried out by looking at the interplay between legal, technical and social norms, focusing on the relationship between new technologies bypassing the law and the rules of law which, while trying to regulate these new technologies, eventually extend into new and previously unregulated territories. From the first pirate radios to the peer-to-peer filesharing platforms, a regularity can be found among the tensions and discrepancies that subsists between technical, and initially marginal innovations and the applicable law. Extending the scope of legal regulation causes changes in the technology, and a widespread deployment and use of these technologies to exercise certain rights which have been threatened by anti-piracy laws.

Internet, droit d'auteur, hackers, réseaux distribués, piratage.
Internet, copyright, hackers, distributed networks, piracy.

Introduction

L'Internet, un réseau mondial décentralisé, s'est constitué comme un espace de plus en plus régulé par des États qui luttent pour maintenir ou même établir leur souveraineté sur le réseau (Post, 1996)[1]. Suite à de nombreuses réformes législatives, les États se sont progressivement emparés du réseau, étendant ainsi leur juridiction à un espace qui se situait auparavant au-delà de leurs "eaux territoriales", ou non déterminé a priori comme faisant partie de leurs sphères de compétence régaliennes.
Ce sont dans ces eaux que se sont également installés les pirates informatiques. La notion de "pirate informatique" est une notion relativement poreuse, dont la définition évolue constamment. Est pirate, à l'origine, celui qui cracke un logiciel propriétaire et le fait circuler (comme dans la piraterie traditionnelle maritime entre brigands). Alors qu'il y avait auparavant une distinction assez claire entre les hackers (bidouilleurs informatiques) et les pirates (cybercriminels), les deux sont aujourd'hui de plus en plus regroupés dans la même catégorie, en partie en raison de la confusion entretenue par les médias et les ayants-droits qui ont tendance à criminaliser toute pratique de bidouillage perçue comme potentiellement dangereuse et à amalgamer ceux qui copient des produits culturels pour leur propre usage et ceux qui en font un trafic lucratif, tels des contrebandiers des mers (Garibian, 2008). Désormais, le terme de « pirate informatique », couramment employé par différents acteurs du numérique, assume de nombreuses définitions qui ne sont pas toujours compatibles les unes avec les autres (à cet égard voir notamment Auray, 2009). Le terme s'étend généralement à tout type d'infraction, de la contrefaçon à l'intrusion dans les systèmes informatiques, mais il est aussi utilisé par certains ayants-droits pour désigner des comportements à la marge qui ne sont pas (encore) régulés par le droit. Enfin, certain internautes se définissent eux-mêmes comme « pirates » dans la mesure où ils vont enfreindre la loi afin de préserver les droits et les libertés du public, voire réformer la politique dans son ensemble et inventer un monde meilleur inspiré de l'architecture du réseau.

Cet article se structure autour de la problématisation de la notion de pirate dans la société de l'information sous l'évolution conjointe du droit et de la technique et de leurs différents modes d'interaction : défiance, concurrence ou influence réciproque pour accompagner la transformation des usages. Les différentes facettes de la notion de pirate - les cybercriminels, les hacktivistes et les internautes engagés - sont analysées selon les relations entre les normes juridiques et sociales et la technique (Dulong de Rosnay, 2007). En effet, bien que la métaphore du « pirate » se retrouve à de nombreuses reprises dans le vocabulaire des réseaux, elle recouvre des réalités différentes techniquement et juridiquement, qui justifient de présenter la vision extérieure critique de ceux qui subissent ces activités jugées illégales et la vision subjective par les acteurs qui exercent ces pratiques qui naviguent aux frontières de la légalité.

---

1 □ Cette recherche s'insère dans le projet ANR ADAM "Architectures distribuées & applications multimédias" : http://adam.hypotheses.org/

Dans une première partie, on examinera les pirates *hors la loi* qui attaquent le système, comprenant les cybercriminels (partie 1.1) et les contrefacteurs ou trafiquants de contenus, qu'ils soient prédateurs ou opportunistes (partie 1.2). Dans une deuxième partie, on considèrera les pirates *pour les droits* qui se défendent contre le système : les pirates engagés ou "hacktivistes" qui militent pour protéger les droits fondamentaux des internautes (partie 2.1) et les internautes qui défendent eux-mêmes leurs libertés individuelles (partie 2.2). D'un côté, les cybercriminels, en informatique et au sens strict, pénètrent dans un système de manière non autorisée, soit à des fins malveillantes, soit par goût de l'exploit, pour abuser les failles de sécurité. De l'autre, les hackers engagés, sorte de Robin des Bois modernes, utilisent et développent des outils informatiques pour promouvoir la justice et la liberté de tous. Enfin, les internautes qui surfent la toile et utilisent les outils à leur disposition pour capter le flot des informations et partager les torrents de données peuvent parfois être considérés des pirates, aussi bien par des tiers que par eux-mêmes.

1. Les pirates hors la loi : à l'attaque du système

L'appréhension la plus évidente de la notion de pirate par le prisme de l'interaction entre le droit et la technique est celle de l'illégalité d'activités menées avec des outils informatiques. L'approche par le droit positif est simple et auto-référente : elle va qualifier de pirate toute personne qui, en utilisant la technique, viole des dispositions juridiques existantes ou lacunaires (*i.e*. qui ne tiennent pas suffisamment compte des spécificités du monde numérique).
Sur les réseaux, cette vision associe aussi bien les cybercriminels (qui violent la loi et s'infiltrent dans les réseaux dans le seul but d'en extraire des bénéfices individuels, tels que la gloire ou les profits) et les contrefacteurs opportunistes (qui violent le droit d'auteur en suivant le sillage et téléchargent des œuvres culturelles ou logicielles sans forcément détruire de la valeur). Cette partie analyse l'interaction entre le droit et la technique employée par les cybercriminels puis par les contrefacteurs du droit d'auteur qui eux aussi effectuent des opérations non autorisées.

1.1. Le pirate cybercriminel

La première définition du pirate au regard du droit appartient au champ de la cybercriminalité (Levy, 2004). Elle se réfère à l'intrusion non autorisée dans des systèmes informatiques ou systèmes de traitement automatique de données - souvent pour des finalités illégales - en exploitant les faiblesses des ordinateurs connectés au réseau. Alors que le concept de cybercriminalité regroupe un grand nombre d'infractions de nature différente (de l'attaque de sites à la fraude sur Internet, de la pédopornographie en ligne au vol d'identité), le piratage cybercriminel a une portée plus étroite qui ne comprend que les actes visant à pénétrer dans un ordinateur ou un réseau informatique - de manière non autorisée - dans le but d'obtenir des informations sensibles, d'introduire des logiciels tiers ou des virus informatiques au sein de ces systèmes ou de détruire le système.

Illustrés par la figure de Kevin Mitnick,[2] les pirates de cette première catégorie sont généralement accusés de méfaits informatiques, d'infraction ou d'utilisation non autorisée des ordinateurs d'autrui, de fraude électronique ou d'espionnage des communications sur le réseau, de possession et d'utilisation illégitime de données confidentielles (mots de passe, données relatives aux cartes de crédit), etc.

Même si la mise en place de dispositions spécifiques aux réseaux facilite la qualification des actes d'intrusion par la justice et ajoute des peines selon les activités menées après l'intrusion, les législations antérieures aux réseaux ont vocation à s'appliquer dès l'intrusion. Dès 1978, en France, les pirates cybercriminels pouvaient être visés par la loi informatique et libertés[3] qui réprime le traitement automatisé de données dans la mesure où il s'agit de données personnelles. Par la suite, les dispositions spécifiques au piratage informatique vont s'appliquer de manière indifférenciée quant à l'objet et l'étendue du délit. Par exemple, l'informaticien Aaron Swartz (voir plus bas dans la section 2.1) qui avait téléchargé des articles scientifiques en nombre sans toutefois les diffuser était menacé des mêmes peines qu'un pirate cybercriminel qui aurait téléchargé des données personnelles ou bancaires, celles prévues pour intrusion non autorisée par le *Computer Fraud and Abuse Act* dès 1986. Dans le cas des pirates qui pénètrent les systèmes autorisés, c'est l'intrusion qui est sanctionnée en premier lieu. Son objet ne vient que dans un deuxième temps.

Aujourd'hui, la plupart des pays occidentaux ont introduit dans leur législation nationale des lois pour sanctionner les activités de "hacking" (attaques de systèmes d'information, intrusions, vol de données, etc.) afin de pouvoir poursuivre les pirates informatiques en justice aussi bien pour leurs intrusions que pour les conséquences qui en découlent. En France, par exemple, la loi Godfrain de 1988[4] sanctionne non seulement le fait d'accéder frauduleusement à des systèmes informatiques, mais aussi le fait d'entraver ou de fausser le fonctionnement de ces systèmes, d'altérer les données et de mettre à disposition d'autrui un équipement permettant d'accomplir ces infractions. Les sanctions relatives à ces infractions ont été successivement majorées suite à l'introduction de la loi LCEN[5] en 2004, avec des peines allant jusqu'à 5 ans d'emprisonnement et 75.000 euros d'amende pour la suppression ou la modification illicite des données contenues dans un système informatique. Ces dispositions prévoient également des peines de 2 ans et 30.000 euros d'amende pour l'accès frauduleux dans un système de traitement automatisé de données, sans suppression ni altération des données ni du système. Ainsi, le simple fait de s'introduire dans un système

---

2 ☐ Kevin Mitnick fut le premier pirate arrêté (en 1995) par le FBI pour avoir compromis plusieurs systèmes informatiques de nombreuses entreprises telles que Pacific Bell, Fujitsu, Motorola, Nokia, Sun Microsystems, et pour avoir accédé illégalement aux bases de données du Pentagone. Il est le premier hacker à figurer dans la liste des dix criminels les plus recherchés par le FBI aux États-Unis.

3 ☐ Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés dite Loi Informatique et Libertés.

4 ☐ Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain.

5 ☐ Loi pour la confiance dans l'économie numérique, n° 2004-575 du 21 juin 2004, abrégée sous le sigle LCEN.

informatique constitue une infraction même en l'absence d'autre préjudice matériel. C'est donc déjà l'exercice de la simple capacité technique qui est réprimée par les dispositions anti-piratage informatique, indépendamment des finalités de l'acte technique. Certes, les utilisations altérant les données et le système constituent des facteurs aggravants, mais le premier élément régulé est le seul exercice de la technique nécessaire pour s'introduire dans un système, même en l'absence d'action ultérieure nuisible.

1.2. Le pirate contrefacteur

Depuis les années 1990, la technique a évolué avec l'arrivée des réseaux pair à pair et le passage à l'échelle du nombre de téléchargement de fichiers couverts par le droit d'auteur. Cette nouvelle vague technologique permet aux particuliers de reproduire des œuvres couvertes par le droit d'auteur et les droits voisins de manière instantanée et sans perte de qualité. L'industrie culturelle, pour tenter de faire réguler ces comportements par l'État, développe un discours qui ne distingue plus entre les pirates informatiques qui infiltrent le système ou qui fournissent des outils pour ce faire (les hackers cybercriminels), les pirates contrefacteurs (les prédateurs[6]) qui vont s'enrichir du trafic de contenus, et, enfin, par extension, l'internaute qui télécharge des fichiers sans autorisation (les pirates opportunistes).

Or, ce n'est pas tant l'acte technique, ni l'infraction juridique, mais bien la conséquence économique qui appelle au contrôle de la technique par le droit. Dès les années 1980, le discours à l'égard du magnétoscope et du magnétophone, qui permettent d'enregistrer les programmes et de dupliquer des supports sur des cassettes audio et vidéo, s'apparente à ces discussions dans la mesure où l'atteinte aux droits par la technique est immédiatement assimilée à une perte de revenus économiques, comme si chaque reproduction remplaçait un achat et devait donc être condamnée. Le ministre de la culture Jean-Philippe Lecat (INA, 1980) déclare au MIDEM en 1980 que le piratage, désignant à la fois les éditions pirates, et la copie privée de cassettes, serait responsable de la chute de la vente de disque. Il opère alors une distinction entre la contrefaçon à des fins commerciales par des professionnels qui revendent des copies, et la reproduction à titre personnel et individuel.

Cette différence entre la revente à but lucratif et la copie privée va s'amoindrir dans les débats depuis la fin des années 1990 avec les premiers téléchargements sur l'Internet. S'opère alors dans le discours des titulaires de droits un amalgame avec l'utilisation du terme de pirate pour désigner deux types d'activités. Le téléchargement non autorisé à des fins personnelles ou le partage de fichiers entre pairs est un acte qui implique une reproduction technique. Mais la revente de copies à la sauvette de cassettes ou de DVD et l'organisation d'un trafic en réseau à plus large échelle, également considérée comme du piratage, n'implique pas forcément d'infraction liée à l'utilisation de la technologie de reproduction. L'activité de contrefacteur prédateur retirant des bénéfices économiques impliquait la complicité d'un projectionniste, de bars ou de vidéos clubs au siècle dernier, ou la mise en place d'un réseau de distribution commercial. L'équivalent de cette catégorie de pirate sur l'Internet conserve l'aspect commercial, et nécessite la vente de publicité ou d'abonnements pour les logiciels de téléchargement, les

---

6 □ Nous reprenons cette expression de Auray, 2009.

réseaux de partage ou les services de lecture en direct ou *streaming*[7].

Le pirate contrefacteur, la deuxième définition du pirate au regard du droit - tout aussi communément utilisée - se distingue de son homologue cybercriminel à plusieurs titres. Tout d'abord, l'activité ne requiert pas de compétences informatiques ni d'intrusion. Elle s'effectue en tant que simple utilisateur de systèmes, la terminologie de pirate ne s'appliquant pas seulement aux développeurs des réseaux pair à pair avec des compétences de hackers mais aussi aux simples utilisateurs. De plus, elle a un objectif unique, le téléchargement de fichiers d'œuvres littéraires et artistiques. Enfin, elle est définie et punie par la législation du droit d'auteur, une branche de la propriété intellectuelle qui a été mise en place pour réguler les relations entre les auteurs et les distributeurs des oeuvres, initialement des entreprises plus que des consommateurs. Dans le cas du téléchargement de fichiers, souvent le fonctionnement des logiciels pair à pair demande à la personne qui effectue un téléchargement descendant de partager aussi de manière ascendante. Ainsi, l'architecture accompagne l'acte de consommation d'un acte de distribution. Cette distinction a motivé la tentative des titulaires de droits, lors du vote de la loi Droit d'Auteur et Droits Voisins dans la Société de l'Information (DADVSI) en France en 2006, de demander la création d'une infraction spécifique pour l'utilisation de logiciels d'échanges pair à pair. Une telle disposition a été censurée par le Conseil Constitutionnel[8] car elle aurait introduit "une différence de traitement injustifiée" et une rupture du principe d'égalité devant la loi entre ceux qui téléchargent des fichiers couverts par le droit d'auteur avec un certain type de système et ceux qui utilisent d'autres méthodes de communication électronique. L'arsenal Hadopi a ensuite été développé spécialement pour contrer le partage de fichier dans le cadre des réseaux pair à pair.

Les représentants des titulaires de droits d'auteur et droits voisins[9] considèrent perdre des revenus à l'occasion du téléchargement non autorisé d'œuvres couvertes par le droit d'auteur et les droits voisins. Les conséquences économiques de la contrefaçon en droit d'auteur sur les réseaux sont en réalité controversées. Certaines études indiquent une diminution du chiffre d'affaires liée au téléchargement[10], d'autres ne trouvent pas de lien de cause à effet, voire notent que ceux qui téléchargent le plus sont ceux qui dépensent le plus en biens culturels[11]. Quoiqu'il

---

7 Le pirate contrefacteur prédateur peut revêtir la figure de Kim Dotcom.

8 Décision n° 2006-540 DC du 27 juillet 2006.

9 Notamment les sociétés de gestion collective du droit d'auteur en France, les syndicats de l'industrie de la musique et du film et les juristes qui les représentent.

10 Des études sont financées par l'industrie musicale et cinématographique, notamment la CISAC (Confédération Internationale des Sociétés d'Auteurs et de Compositeurs) l'IFPI (*International Federation of the Phonographic Industry*) qui regroupe les producteurs de phonogrammes, la RIAA (*Recording Industry Association of America*) et la MPAA (*Motion Picture Association of America*) qui représentent l'industrie phonographique et cinématographique aux Etats-Unis. Elles analysent l'impact de l'activité de téléchargement non autorisé, qualifiée de piratage, sur les ventes de musique et de films en ligne, sur la perte d'emplois dans les industries culturelles et sur la création artistique.

11 L'impact de la copie privée de produits culturels sur la vente est controversé, de nombreuses études démontrent que les utilisateurs qui copiaient des cassettes vierges et qui aujourd'hui téléchargent sont ceux qui achètent le plus de biens et de services culturels. Voir la liste des études dressée

en soit, le droit positif assimile à de la contrefaçon l'acte de reproduction non autorisé, et la copie privée à partir de réseaux pair à pair implique une telle reproduction, ainsi qu'un acte de distribution. Par conséquent, le téléchargement est qualifié de contrefaçon. Les mêmes peines peuvent en théorie s'appliquer à l'internaute individuel qui télécharge un morceau à des fins personnelles qu'à la personne qui va télécharger en masse et en vue de revendre des DVD par exemple. La loi représentant l'opinion des titulaires de droits considère que les deux activités sont nuisibles économiquement et criminelles et prévoit des peines de trois ans d'emprisonnement et 300 000 euros d'amende pour les deux types d'activité (Article L. 335 du Code français de la Propriété Intellectuelle). Ces peines maximales n'ont pas été mises en oeuvres pour des internautes, mais le traitement prévu par le droit positif ne différencie pas les deux comportements : pirates opportunistes et pirates prédateurs sont visés par les mêmes dispositions sur la contrefaçon. Contrairement aux représentants des titulaires de droits qui estiment leurs revenus directement menacés par les deux types de contrefaçon, les représentants des utilisateurs, des consommateurs et de certains titulaires de droits voisins, comme les sociétés d'artistes interprètes en France se sont ralliés à une approche susceptible de leur procurer des revenus supplémentaires plutôt qu'à une approche répressive qui condamne les pirates à des amendes sans directement produire de revenus. Des revenus pourraient être obtenus sous la forme d'une limitation des droits exclusifs : licence légale en vertu des articles L. 214-1, L.331-4 et L.342-3 du Code de la Propriété Intellectuelle pour la copie privée sur support, propositions de licence globale ou contribution créative (Aigrain, 2012) pour la copie privée par téléchargement, ou encore sous la forme de dommages et intérêts. Mais ceux-ci sont octroyés pour dédommager les victimes dans le cadre de procédures de droit civil, alors que les dispositions régissant la contrefaçon sont du ressort du droit pénal, renforçant encore la confusion entre le pirate contrefacteur opportuniste (à des fins personnelles non marchandes) et le pirate criminel prédateur (à l'échelle marchande). À cet égard, l'activité de copie privée est considérée comme un vol, au même titre que l'activité de contrefaçon professionnelle, ou le trafic de contrebande, qui garde d'ailleurs des points communs avec la piraterie maritime lorsqu'elle désigne le transport illégal de marchandises, qui peut s'opérer par bateau.

Dans le cas du pirate internaute coupable de contrefaçon au sens du droit d'auteur comme dans le cas du pirate hacker qui s'introduit dans un système sans y toucher, c'est l'utilisation d'un outil technique de manière non autorisée par la loi qui opère la qualification juridique d'infraction de manière auto-référentielle. Ces acceptations de pirates, les plus récentes et communément employées par les médias et l'industrie culturelle, ne sont pas liées à la finalité de profit économique visée par la régulation de la contrefaçon en droit d'auteur et sont indépendantes de la destruction de valeur et du préjudice qui peuvent accompagner ou non l'infraction technique rattachée à la cybercriminalité. En brandissant la peur du pirate qui s'introduit dans un système technique avant même d'en avoir fait un usage criminel, et du pirate qui télécharge en pair à pair à des fins personnelles non marchandes, le droit vise des actes techniques (l'intrusion, la reproduction), avant de réguler leurs effets réels ou supposés (l'altération de données ou de systèmes, la perte de revenus). Nous allons à présent examiner comment ce contrôle de la technique par le droit peut produire des effets pervers en poussant à une sophistication de la

---

par la Quadrature du Net : http://www.laquadrature.net/wiki/Etudes_sur_le_partage_de_fichiers, notamment (Liebovitz, 2005), (Oberholzer-Gee, Strumpf, 2007) et (Huygen *et al*., 2009), et même (Hadopi, 2011).

technique pour échapper au droit.

1.3. La régate entre le droit et la technique

Cette partie analyse les stratégies du droit pour tenter de réguler les techniques utilisées par les pirates hors-la-loi et les effets que cette régulation engendre à la fois sur d'autres droits et sur les développements des techniques elles-mêmes. Trois exemples nourrissent cette réflexion, tout d'abord les tentatives de blocage des radios pirates et ensuite celles du téléchargement de la culture avec la régulation juridique et la régulation technique.

1.3.1 Les radios pirates

On observe avec les radios pirates peut-être la première superposition entre les pirates des mers et les pirates de la musique, et l'explication de l'emploi du terme pour désigner l'activité de diffusion ou de reproduction non autorisée qui se retrouve avec les pirates contrefacteurs opportunistes. Les radios pirates utilisaient déjà l'image du flibustier ; installées à l'origine sur des embarcations, elles se dénomment aussi radios libres car elles proposent une alternative culturelle, luttent contre le monopole de l'État et pour la liberté d'expression. Lors de la période où elles ont été illégales, leurs activités ont été entachées d'affaires d'espionnage et de meurtre entre associés, renforçant l'aspect mythique et criminel de l'activité.

Les radios pirates anglaises émettaient à la limite des eaux territoriales britanniques afin d'être captées à Londres (INA, 1966) sans toutefois être soumises aux législations fiscales, sur la publicité, le droit d'auteur, les télécommunications et le monopole d'Etat (AFDI, 1966). Les DJ de Radio Caroline, la radio pirate anglaise, se qualifiaient déjà en 1966 de Robins des Bois (INA, 1966) car ils considéraient rendre un service culturel au public et aux artistes qui n'auraient pas été diffusés sur les ondes d'État. Les radios pirates occupaient des fréquences qui ne leur avaient pas été attribuées et exploitaient un vide juridique (Lesueur, 2002). Elles pouvaient brouiller l'émission des ondes officielles et les conventions internationales des télécommunications et du droit de la mer ont tenté de les interdire notamment sur la base de cette simple possibilité (AFDI, 1966). De la même manière que pour la cybercriminalité, le droit tente d'abord d'appliquer les règlementations générales aux radios pirates avant d'élaborer une loi spécifique anti-radio pirate (en 1967 en Grande-Bretagne, en 1978 en France). Ces lois durcissent les peines et mettent les programmes explicitement dans l'illégalité pendant quelques années, jusqu'à ce que soient délivrées des licences puis que la bande FM soit libéralisée. Cet épisode illustre la différence entre le hors le loi et l'illégalité. Le pirate qui viole la loi effectue des actions illégales (criminalité, contrefaçon) alors que les pirates sont "hors-la-loi" dans la mesure où ils se situent au-delà des limites de la loi (à cause d'un vide juridique) ~~et qui~~ ne sont, donc, par conséquence, pas (encore) illégaux.

1.3.2 La régulation juridique du téléchargement

Le même phénomène se retrouve avec les techniques numériques de diffusion de la culture. D'abord non régulées par le droit lors de leur apparition et donc "hors-la-loi", elles deviennent une concurrence et une source d'inquiétude pour les diffuseurs traditionnels qui cherchent à se

protéger en demandant le développement de dispositions juridiques anti-piratage. Au lieu d'appliquer les dispositions qui régulent l'effet produit par la technique (la contrefaçon de droit d'auteur), elles cherchent à cibler directement la technique, qui devient alors illégale. Les techniques évoluent ensuite pour sortir de la définition de ce que la loi désigne comme contrefaçon. Ainsi, l'architecture des réseaux de partage de musique va évoluer, de Napster aux réseaux pair à pair décentralisés (Musiani, 2013), avec des techniques de plus en plus sophistiquées pour préserver l'anonymat.

Les actions en justice des titulaires de droits s'attaquent d'abord directement aux pirates contrefacteurs opportunistes : les internautes qui téléchargent (Auray, 2009), puis à l'infrastructure sur laquelle les pirates s'appuient : les développeurs de services et protocoles permettant l'échange de contenus, les fournisseurs d'accès et les hébergeurs. Ces poursuites des pirates opportunistes conduisent fréquemment à éliminer en même temps des usages légitimes, à brider des droits et des libertés fondamentales et à entraîner une surveillance généralisée des communications et des données personnelles.
Suite au traité ACTA (*Anti-Counterfeiting Trade Agreement*) qui proposait, afin de limiter la contrefaçon sur l'Internet, d'introduire des mesures de surveillance des communications par les intermédiaires du réseau, d'autres projets de loi tels que SOPA (*Stop Online Piracy Act*) et PIPA (*Protect-IP Act*) ont tenté de renforcer la responsabilisation des intermédiaires avec les procédures de *notice and takedown (*notification et retrait[12]). Ces trois traités utilisent la responsabilisation des intermédiaires comme une tactique juridique pour lutter contre le piratage sans toutefois s'attaquer aux utilisateurs finaux ni aux concepteurs des outils : les intermédiaires deviendraient ainsi les nouveaux "corsaires" dans la mesure où ils sont chargés de surveiller et de faire appliquer le droit sur le réseau, devenant ainsi une forme de police privée de l'Internet.

En France, au nom de la protection des droits d'auteur, la loi DADVSI a tout d'abord éliminé le droit à la copie privée. Ensuite, la loi HADOPI, avec la riposte graduée, avait proposé d'ordonner la coupure de l'accès à internet d'un foyer en cas de téléchargement. Enfin, la loi LOPPSI, en déployant un dispositif de filtrage destinée à la lutte contre le terrorisme et la pédophilie, est susceptible d'empiéter sur la liberté d'expression. De même, les injonctions juridiques données à certains fournisseurs d'accès de bloquer techniquement les contenus sont perçues comme contraires à la liberté de recevoir ou de communiquer des informations[13].
Ces mesures (aux retombées plus larges que les infractions qu'elles visent) portent atteinte aux libertés fondamentales des citoyens. Elles ont d'ailleurs été condamnées par un rapport de l'ONU qui place les droits fondamentaux comme la liberté d'expression comme supérieur au droit d'auteur (La Rue, 2011).

1.3.3 La régulation technique du téléchargement

---

12 □ Procédure légiférée aux États-Unis par le *Digital Millennium Copyright Act* (DMCA) section 512(c), en Europe par la Directive *Enforcement* (Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative aux mesures et procédures visant à assurer le respect des droits de propriété intellectuelle), et en France dans l'article 6 de la LCEN.

13 □ Décisions de la Cour de Justice de l'Union Européenne (CJUE), 24 novembre 2011, Scarlett Extended, et 12 février 2012, SABAM c/ Netlog.

Le développement de lois visant spécifiquement les pirates qui développent et utilisent des logiciels pouvant servir à la contrefaçon est associé à la mise en place de mesures de protection technique (MPT). Ces *Digital Rights Management systems* ou DRM proposent d'inclure la règle de droit et son application dans une application technique pour accroître l'effectivité du droit. Les mesures de protection techniques cherchent à rendre impossible les actes techniques de copie. Cependant, elles ont un champ de visée très large et agissent même pour empêcher des actes qui ne relèvent pas des droits exclusifs des titulaires de droits (Cohen, 1997, Koelman et Helberger, 2000, Samuelson, 2003). Par exemple, les activités de copie privée, d'archivage, de prêt, de consultation en bibliothèque, de création d'oeuvres transformatives (*remix)*, de fouille des données (*data mining*) à des fins de recherche, se sont retrouvées impossibles à accomplir *de facto* car les fichiers ne laissent pas la possibilité technique d'exercer ces droits.

Avec les législations visant à protéger le droit d'auteur, la législation s'étend au-delà de ses eaux territoriales pour contrôler des activités sociales légitimes qui utilisent les mêmes outils que les pirates opportunistes. Les eaux territoriales des activités libres non régulées, les exceptions au droit d'auteur (Dusollier, 2005), se réduisent sous l'action conjointe des restrictions juridiques et des mesures techniques qui traduisent et mettent en œuvre les règles de droit. À la double protection juridique et technique du droit des auteurs s'est ajoutée, dans cette régate entre le droit et la technique, une protection juridique supplémentaire, celle de la mesure technique elle-même (Traités OMPI, 1996, Directive EUCD, 2001, loi DADVSI, 2006). Il est illégal de contourner techniquement une mesure technique - comme les hackers savent le faire - même pour accomplir des activités légitimes au regard du droit. Le champ du droit s'étend alors à une activité technique auparavant légale qui devient ainsi criminelle. Ainsi, alors que le régime du droit d'auteur était censé encourager la création d'œuvres de l'esprit en empêchant les tiers de tirer injuste profit de l'investissement des auteurs et des autres titulaires de droits, il est aujourd'hui utilisé pour interdire des usages autrefois perçus comme étant légitimes (la copie privée[14], le partage non-marchand[15]), censurer les communications en lignes (suite à la procédure d'avis et retrait[16]) et criminaliser des activités qui ne sont que lointainement associées à l'exploitation des œuvres de l'esprit (la non-sécurisation de l'accès à l'Internet,[17] le contournement des mesures techniques de protection[18], la vente[19] ou la diffusion[20] d'outils ou d'informations susceptibles de faciliter de

---

14

- Voir le jugement du TGI, arrêt de la Cour d'Appel et décision de la Cour de Cassation dits « Mulholland Drive »: TGI Paris, 3ème chambre - 2ème section, 30 avril 2004, M. Stéphane P., UFC Que Choisir c/ SA Films Alain Sarde, SA Universal pictures video France et autres ; CA Paris, 4ème chambre - Section B, 22 avril 2005, M. Stéphane P., UFC Que-Choisir c/ Universal Pictures Video Fr, SEV, Films Alain Sarde, Studio Canal et Cass. 1ère civ, Arrêt n° 549, 28 février 2006, Stés Studio Canal, Universal Pictures Vidéo Fr, SEV c/ Stéphane X et UFC Que-Choisir.

15

- Voir la seule décision appliquant Hadopi, un internaute ayant été condamné à une amende pour défaut de sécurisation de sa connexion ayant donné suite au téléchargement de deux titres, T. police Belfort, 13 sept. 2012, *Revue Lamy Droit de l'immatériel* 2012/86, p. 15.

16

- cf. France c. Yahoo! Inc. et Société Yahoo! France (*LICRA v. Yahoo!*)

17

- cf. la décision Hadopi, *op cit*.

18

- cf. les décisions Mulholland Drive, *op cit*.

19

détournement de ces technologies).

***

Ainsi, alors que l'évolution des technologies numériques appelle à une réforme de certaines normes juridiques pour tirer partie du progrès technique, l'évolution du droit encourage, à son tour, le développement de nouveaux dispositifs technologiques qui tentent de dépasser, ou de contourner les nouvelles règles de droit (Lessig, 2003). C'est ainsi que la production de règles visant à réguler les nouvelles techniques et architectures en ligne peut avoir des effets incertains, ou tout au moins inattendus : plus le droit essaie de contrôler ces architectures, plus il encouragera le développement de nouveaux outils et architectures de plus en plus décentralisées visant à échapper toujours plus à ce contrôle (ces outils seront analysés en détail dans la section 2).

L'appréhension par le droit positif du hacker et du contrefacteur opportuniste, deux figures médiatisées du pirate, révèle que la loi vise les seuls actes d'intrusion et de reproduction techniques avant de réprimer les actes d'altération de données et de contrefaçon professionnelle, les sources incontestées de préjudice et de destruction de valeur. Après l'examen du pirate hors-la-loi vu sous l'angle des rapports entre le droit et le technique, les parties suivantes vont s'attacher à l'analyse des pirates engagés (2.1) en enrichissant la dialectique droit-technique d'un aspect politique visant à faire évoluer le droit, puis à celle des pirates utilisateurs (2.2) en intégrant l'angle des usages pour défendre leurs droits.

2. Les pirates *pour les droits* contre-attaquent le système

En se concentrant à présent sur les techniques qui ne sont pas prévues par le droit au moment de leur apparition, il s'agit d'analyser l'impact sur la société des activités de pirates qui ne relèvent ni de la cybercriminalité (pirates cybercriminels de la section 1.1) ni de la contrefaçon (pirates contrefacteurs de la section 1.2). Il s'agit ici d'examiner le statut des hackers ou hacktivistes qui militent pour la défense des droits fondamentaux (section 2.1) et des utilisateurs lambda qui utilisent la technique dans le seul but de se défendre contre les excès du droit (décrits dans la section 1.3). La criminalisation des usages autrefois légitimes, et les poursuites juridiques qui en découlent, ont poussé au développement d'applications de plus en plus sophistiquées qui visent à échapper aux règles (juridiques et techniques) qui se sont établies sur le réseau, non pas dans le but d'enfreindre la loi mais, plutôt, dans le but de préserver la vie privée des internautes, de permettre l'anonymat et de promouvoir la liberté d'expression sur Internet.

□ Thomas Michael Whitehead fut le premier pirate reconnu coupable sous le DMCA (Digital Millennium Copyright Act) pour la vente de dispositifs susceptibles de servir à capter illégalement des radiodiffusions par satellite.

□ Dans un arrêt du 27 octobre 2009, la Cour de Cassation a confirmé qu'il n'était pas légitime de diffuser sur un site web publiquement accessible des logiciels informatiques ou les codes source de logiciels permettant d'exploiter des failles de sécurité. La Cour a rappelé, cependant, qu'il était légitime d'informer le public des failles de sécurité exploitées par ces logiciels.

1. Les hacktivistes, des pirates engagés

Au cours des dernières années, le stéréotype du pirate informatique en tant que cybercriminel ou contrefacteur opportuniste a largement évolué. Une définition extensive assimile désormais les pirates à des experts ou des spécialistes du réseau. Si la piraterie, c'est l'art de bien connaître les eaux dans lesquelles on navigue, alors, dans le monde numérique, les pirates sont ceux qui connaissent parfaitement le fonctionnement du réseau et des technologies numériques.

Les pirates engagés appartiennent à la culture des "hackers" : des individus passionnés qui étudient (de manière souvent autodidacte) le fonctionnement des ordinateurs et des réseaux informatiques, en explorent les opportunités et en identifient les failles ; ils apprennent non seulement à se servir des nouvelles technologies, mais aussi (et surtout) à les développer, à les enrichir, et, parfois, à les détourner afin de rejoindre plus rapidement leurs objectifs (Thomas, 2003). Ces acteurs représentent une figure héroïque du pirate. Ils utilisent la technique pour développer de nouveaux outils pour exercer une action positive pour le réseau et la société dans son ensemble.
En effet, le caractère de plus en plus répressif de la loi qui cherche à contrôler les techniques employées par les pirates hors-la-loi a engendré une vague de protestations de la part d'individus engagés contre l'instauration d'un cadre juridique susceptible de limiter les libertés de l'ensemble des internautes. Suite aux nombreuses réformes législatives visant à réguler le réseau et les différentes technologies qui s'y sont progressivement établies, nous en sommes, aujourd'hui, arrivés à une situation presque paradoxale où la loi, dans le but de faire face à ces nouvelles technologies, se retrouve avec une portée telle qu'elle menace les droits et les libertés individuelles des citoyens qu'elle était censée protéger. Un nombre croissant d'internautes se transforment alors progressivement en militants qui revendiquent l'exercice de leurs droits à la vie privée et à la liberté d'expression en s'opposant aux différents projets de lois qu'ils considèrent être de nature trop restrictive ou "liberticide" (Delamotte *et al*., 2009).
C'est ainsi que, à côté de la notion traditionnelle du pirate dépeint comme un "voleur", un "criminel" ou même un "terroriste" (Garibian, 2008), s'instaure une vision plus romantique du pirate entendu comme un "voleur de vagues", un "criminel engagé" ou même parfois un "défenseur des libertés". Il s'agit des pirates engagés, des hackers activistes (ou "hacktivistes") qui infiltrent des réseaux, piratent des serveurs, et, parfois, détournent la loi au nom de leurs principes et de leurs convictions politiques (Hintikka, 2008). Ces individus ont de bonnes compétences techniques. Ils utilisent les techniques de piratage informatique (tels que les dénis de service ou *distributed denial-of-service* attack (*DDoS*), les vols d'informations, ou les défigurations de sites web, etc.) afin de promouvoir l'activisme politique. Ils développent aussi des outils pour contourner la loi par la technique, non pas pour servir leurs intérêts personnels, mais pour les mettre ensuite à disposition du public pour qu'ils puissent être utilisés par la société dans son ensemble.

C'est le cas, par exemple, du collectif Anonymous (Coleman, 2011), une communauté d'individus décentralisée agissant de manière anonyme, mais qui parviennent cependant à coordonner leurs activités afin de réaliser une série d'infractions technologiques pour infiltrer ou attaquer les serveurs de plusieurs gouvernements (États-Unis, Israël, Tunisie, Ouganda, etc.), de certaines organisations religieuses (telle que, notamment, l'église de scientologie), et d'entreprises privées (PayPal, Mastercard, Visa, etc.). Bien que considérés par les médias et de

nombreuses institutions gouvernementales comme des cybercriminels ou des cyber-terroristes, les Anonymous sont un groupe extrêmement hétérogène dont les membres révèlent des valeurs et des pratiques diverses. Certains d'entres eux sont poussés par des motivations fondamentalement altruistes : ils poursuivent des valeurs démocratiques et dénoncent les abus des libertés civiles sur les réseaux, tel que, notamment, l'érosion de l'anonymat et de la vie privée sur Internet et la défense de causes qui comme Wikileaks ont été victimes d'un boycott de la part d'entreprises privées.

En 2012, durant les négociations des traités SOPA, PIPA et ACTA, de nombreux pirates informatiques ont eu l'occasion d'employer leur expertise en informatique et réseaux pour des finalités à caractère fortement politique et social. Les Anonymous sont intervenus avec des attaques "par déni de service" (DDoS) pour bloquer les sites webs des grands acteurs de l'industrie culturelle (tels que ceux de Warner Bros, la RIAA et la MPAA), ainsi que les pages officielles du ministère de la Justice, du FBI, et même de la Maison Blanche. De même, le collectif AntiSec (associé à Anonymous) s'est infiltré dans le site web de la *Federal Trade Commission* pour revendiquer le droit à l'échange non-marchand de fichiers et dénoncer les atteintes à la liberté d'expression qui découlent des clauses de ces traités. Enfin, en Pologne, de nombreux sites gouvernementaux ont été attaqués par des hacktivistes comme forme de représailles contre l'intention du gouvernement polonais de signer le traité ACTA.

Conformément aux convictions d'Edward Abbey - un écrivain et essayiste américain renommé d'après qui *si la liberté est hors-la-loi, seuls les hors-la-loi seront libres* - ces pirates engagés se battent contre le pouvoir établi pour défendre leurs valeurs et leurs libertés fondamentales (Samuel, 2004). La plupart de ces pirates (bien que condamnés par la loi comme cybercriminels) ne sont pourtant pas considérés comme des "criminels" par le grand public (Manion et Goodrum, 2000) ; ils sont, au contraire, souvent vu comme des héros (Levy, 2001).
Aaron Swartz est peut-être un des cas les plus emblématiques de cette nouvelle génération de pirates informatiques, entre hacker cybercriminel et hacktiviste. Auteur du *Open Access Guerilla Manifesto*,[21] Aaron Swartz revendiquait que "L'Information est pouvoir. Mais comme tout pouvoir il y a ceux qui veulent le garder pour eux-mêmes". Convaincu que les conditions d'accès aux publications scientifiques sont trop restrictives, Aaron Swartz a milité pour promouvoir le libre partage des savoirs et des connaissances (Guédon, 2003; Suber, 2012). En 2011, accusé de s'être introduit illégalement pour télécharger plusieurs millions d'articles scientifiques provenant de la base JSTOR, il a subi de nombreuses poursuites judiciaires.[22] Suite à son suicide à l'âge de 26 ans, Aaron Swartz est désormais considéré comme un véritable héros par de nombreux partisans de la culture libre.

La figure du pirate en tant qu'hacktiviste engagé s'assimile ainsi à celle d'un « chevalier paladin » qui lutte pour préserver les libertés d'autrui et qui est prêt à remettre en cause le système établi au nom de ses valeurs et principes. Mais les outils utilisés par ces « paladins » se

---

21
- http://archive.org/details/GuerillaOpenAccessManifesto

22
- Aaron Swartz était accusé de onze infractions à la loi sur la fraude électronique (*Computer Fraud and Abuse Act*) et passible d'une peine maximale cumulée de 1 million de dollars et de 35 ans d'emprisonnement.

sont désormais largement diffusés sur le réseau, et sont aujourd'hui à disposition du public au sens large, et les utilisateurs s'en emparent pour préserver leurs libertés fondamentales, tels que les droits à la vie privée et à la liberté d'expression.

Cette reconnaissance positive de la notion de pirate au sein de la société est clairement illustrée par l'émergence et la montée en popularité des Partis Pirates, aussi bien en France qu'à l'étranger[23], qui détournent la figure du pirate informatique et contrefacteur. En France, le Parti Pirate crée en 2006 prône une plus grande transparence politique, l'ouverture des données publiques, et la légalisation du partage non-marchand.[24] Loin de faire l'apologie de la cybercriminalité ou de la contrefaçon, ces partis ont pour dessein de défendre les droits et les libertés des citoyens sur l'Internet et dans la vie politique en général, ainsi que de réduire les débordements du droit d'auteur et des brevets pour maximiser l'accès à la culture et aux savoirs. Ce ne sont pas des hacktivistes à proprement parler, mais des hackers du droit et de la politique.

2.2. Les citoyens, des apprentis pirates

On observe aujourd'hui l'émergence d'une troisième figure de "pirate", une catégorie d'individus beaucoup plus large et plus difficile à cerner puisqu'ils ne retombent ni dans la catégorie de pirates cybercriminels ou contrefacteurs (dans la mesure où ils n'opèrent pas dans une optique criminelle et ne violent aucune loi), ni dans la catégorie de pirates engagés (dans la mesure où ils ne donnent à leurs actions aucune valeur idéologique ou politique). Il s'agit des utilisateurs qui apprennent à se servir des outils qui leur ont été fournis par les pirates informatiques (pirates hors-la-loi ou engagés), mais pas dans le but de s'échanger des fichiers parfois protégés par le droit d'auteur (comme le font les pirates contrefacteurs par opportunité[25]). Ces outils sont en premier lieu utilisés afin de communiquer de façon anonyme, d'échapper à la censure et de protéger leur droit à la vie privée (e.g. Tor[26], I2P[27], Freenet,[28] etc.). Bien que ces outils puissent

---

23 ☐ Pour un aperçu de tous les partis pirates actuellement existants et de leur répartition dans le monde, voir http://piratetimes.net/pirate-parties-worldwide/

24 ☐ Pour plus d'informations sur le programme du Parti Pirate, voir http://legislatives.partipirate.org/2012/notre-programme/

25 ☐ Le pirate par nécessité peut aussi être un pirate contrefacteur opportuniste, mais pas au même moment. Les deux notions ne sont pas mutuellement exclusives.

26 ☐ TOR, acronyme de *The Onion Router*, littéralement : « le routeur oignon », rend possible les échanges anonymes de par sa structure décentralisée. Ce réseau distribué a été conçu pour faciliter la communication anonyme. Basé sur le mécanisme de routage en oignon (*onion routing*), Tor introduit une nouvelle couche de communication cryptographiée sur le réseau de façon à camoufler non seulement les contenus, mais aussi l'origine et la destination des communications. Plus de détails sur https://www.torproject.org/

27 ☐ I2P, acronyme de *Invisible Internet Project*, est un réseau anonyme chiffré que les applications peuvent employer pour envoyer de façon anonyme et sécurisée des informations entre elles. La communication est chiffrée de bout en bout. Plus de détails sur https://www.i2p2.de/

28

aussi être utilisés pour des finalités criminelles, ils sont de plus en plus utilisés dans une optique défensive : suite à la criminalisation d'une grande partie des usages auparavant légitimes, ces internautes utilisent ces technologies non pas pour contourner les règles de droit (e.g. infiltrer des systèmes ou télécharger des fichiers en pair à pair), mais plutôt pour échapper à des législations et pratiques de surveillance qui empiètent sur ce qu'ils considèrent comme leurs libertés fondamentales, droit à la vie privée et liberté d'expression (Boyle, 1997; Deibert, 2003). Ces internautes sont souvent des utilisateurs experts conscients de l'impact que l'extension du droit peut avoir sur leurs libertés fondamentales. Ils adoptent ainsi de nouveaux outils et comportements défensifs, qu'ils intègrent à leurs usages et pratiques numériques. Par exemple, ils vont encrypter par défaut leurs communications, et surfer de manière anonyme, afin d'éviter que leurs comportements soient croisés et fichés, plus que pour cacher des comportements répréhensibles. Pirates en apparence dans le sens où ils utilisent des outils que les cybercriminels et les terroristes (les pirates au sens de Garibian, 2008) utilisent à d'autres fins, ils représentent aujourd'hui une proportion croissante des internautes soucieux de protéger leur vie privée et leur liberté d'expression.

Les dispositions anti-piratage ne s'attaquent désormais plus seulement aux comportements criminels, mais aussi aux activités du public au sens large. Avec l'apparition de nouveaux systèmes de communication visant à contourner des règles qui ne paraissent plus légitimes à une majorité d'internautes (extension de la protection du droit d'auteur, surveillance des communications, censure, etc), la dénomination de pirate se généralise petit à petit à une large portion de la société. Ces nouveaux apprentis pirates ne sont ni des cybercriminels, ni des hackers curieux d'explorer les nouvelles opportunités offertes par les technologies numériques, ils sont de simples internautes (Gantz et Rochester., 2005) qui utilisent ces outils dans le seul but de pouvoir naviguer tout en exerçant leurs droits et libertés fondamentales : accès à la culture, création transformative, citation audiovisuelle, protection de la vie privée, liberté d'expression, etc. Ainsi, au-delà des plateformes pour le partage des fichiers (Napster, Kazaa, Gnutella, et plus récemment BitTorrent) utilisées souvent sans respecter le droit d'auteur – bien que des utilisations telles que le partage non marchand et la copie privée soient considérées légitimes par la plupart des internautes (Auray, 2009) – on voit se développer des outils orientés vers la protection des libertés fondamentales, les « *liberation technologies* » qui visent à redonner aux internautes la faculté technique de faire valoir leurs droits sur les réseaux, de protéger leur vie privée, d'exprimer librement leurs opinions, et d'accéder à tout type de contenu ou d'information en ligne (Ziccardi, 2012).

Tor est peut-être l'un des exemples les plus marquants de ces nouveaux outils de « libération citoyenne ». Ce logiciel Open Source protège les internautes contre toute forme de surveillance du réseau qui pourrait porter atteinte à leur vie privée et leurs libertés fondamentales (Bendrath et Mueller, 2011). Bien sûr, cette technologie n'est qu'un outil, un instrument qui peut être utilisé aussi bien pour de bonnes que pour de mauvaises finalités. Ainsi, bien qu'il soit utilisé pour préserver ou renforcer les libertés des internautes citoyens qui ne commettent pas d'infraction, ainsi que par les militaires américains (entre autres) soucieux de sécuriser leurs réseaux, Tor peut

---

□ Freenet (http://freenetproject.org) est un réseau informatique anonyme et distribué construit sur l'Internet. Il vise à permettre une liberté d'expression et d'information totale fondée sur la sécurité de l'anonymat, et permet donc à chacun de lire comme de publier du contenu.

aussi être utilisé pour dissimuler des activités illégales des pirates hors-la-loi. Tel est le cas de Silkroad : une plateforme d'échange entre pairs (semblable à Ebay) mais qui, afin d'assurer l'anonymat à la fois des acheteurs et des vendeurs, n'est accessible que par le réseau Tor et ne permet de réaliser des transactions que par le biais d'une monnaie électronique anonyme (Bitcoin[29]). Bien qu'il n'y ait, en théorie, pas de contrainte sur le type de marchandise que l'on puisse acheter ou vendre sur ce site, l'anonymat du service facilite l'échange de ce qui ne peut pas être vendu ou acheté légalement, notamment des stupéfiants et des armes (Barratt, 2012).

Il devient aujourd'hui, toujours plus difficile de distinguer entre les vrai pirates du réseau (ceux qui relèvent de la cybercriminalité), les hackers ou les hacktivistes (qui militent contre une régulation excessive, et souvent répressive du réseau), et, enfin, les utilisateurs lambda désormais considérés comme des pirates par le simple fait qu'ils utilisent des outils qui ont potentiellement des finalités ou des usages criminels.

2.3. La libération par les techniques

Aujourd'hui, en dépit de la fluidité des frontières sur l'Internet, le réseau ne peut plus échapper à la souveraineté des États (Drezner, 2004; Goldsmith et Wu, 2006). Le droit a évolué, bien que souvent après un certain délai, afin de venir réguler cet espace longtemps considéré comme une îlot de liberté et de prospérité (Weiser, 2009). C'est ainsi que de nombreux internautes, dont les activités se situaient auparavant en dehors de la juridiction des États, sont devenus des pirates, des hors-la-loi, mais de quelle loi parlons-nous si l'exercice des droits ne peut être garanti qu'en utilisant les techniques des pirates ?

Des lois obsolètes, fondées sur une vision essentiellement territoriale du droit ou qui n'ont pas su s'adapter à la réalité du numérique : elles répriment des usages qui sont à la fois légitimes et qui n'entrent pas en concurrence avec les intérêts économiques des titulaires de droits, tels que le droit de citation, de parodie, etc. Des lois à la portée beaucoup trop vaste, souvent trop strictes et sévères, incapables d'accommoder les nouvelles pratiques qui se sont progressivement établies sur le réseau. Il convient alors de se demander si, aujourd'hui, le droit en vigueur est effectivement apte à réguler un réseau transnational et en mutation constante tel que l'Internet. Après avoir analysé l'influence réciproque entre le droit et la technique et leurs effets sur la notion de pirate, il s'agit à présent de comprendre la mesure dans laquelle l'un pourrait l'emporter sur l'autre. Or, bien que la technique évolue toujours plus rapidement que le droit, ce dernier vient combler le vide législatif avec des lois de plus en plus lourdes et restrictives (Engel, 2006), apparemment sans se souvenir de sa mission de protection des droits et des libertés. Sur l'Internet, ces dérives du droit ont conduit à l'émergence de nouvelles technologies de « libération citoyenne » (Ziccardi, 2012) qui visent à échapper à certaines conséquences de cette extension récente du droit dans le seul but de préserver les droits et les libertés des internautes (par exemple les *liberation technologies* pour maintenir l'anonymat ou éviter une surveillance excessive des communications en ligne). Tels sont les nouveaux pirates du réseaux : des individus

---

29 □ Bitcoin est une monnaie électronique dont la possession n'est pas nominative et qui est complètement séparée du système bancaire international. Plus d'informations sur http://bitcoin.org/

qui essaient par la technique de rétablir cet îlot de liberté qu'ils avaient un temps connu sur l'Internet (Lessig, 1999). Le phénomène n'est pas nouveau, il avait été constaté à l'occasion du développement d'autres techniques comme les radios "pirates" (voir section 1.3) qui, après avoir été initialement développées de manière indépendante et dérégulée, se sont ensuite transformées en radios "libres" après qu'elles aient été régulées de façon à contrôler les communications radios.

Conclusion

Cet article a analysé différentes facettes de la notion de pirate au regard de l'évolution de la technique et du droit. Les rapports entre la technique et le droit sont ambivalents. D'un côté, le droit court après la technique pour tenter de réguler des espaces et des usages nouveaux. De l'autre côté, le droit se doit de maintenir des valeurs et d'arbitrer entre la légitimité d'activités au statut controversé, entre légalisation et répression dans le cas des systèmes de partage de fichiers.

Les premiers explorateurs du réseau, les dénommés "hackers", étaient poussés par des motivations virtuoses : la curiosité d'étudier le fonctionnement du réseau et le désir de modifier, de détourner ou de « bidouiller » un système informatique pour y apporter de nouvelles fonctionnalités. Ensuite, ce sont les cybercriminels qui s'emparent de ce nouvel espace numérique, profitant du retard législatif et de l'application parfois difficile des lois sur Internet, afin d'effectuer des activités illicites telles que la fraude informatique, la contrebande de logiciels et la contrefaçon de contenus couverts par le droit d'auteur. Enfin, ce sont les activistes (ou « hacktivistes ») qui s'approprient la figure du pirate pour des raisons politiques ou idéologiques. En parallèle, les utilisateurs lambda qui téléchargent ou « piratent » des contenus sous droit d'auteur sont assimilés à des contrefacteurs, et des utilisateurs un peu plus sophistiqués utilisent les mêmes techniques que les pirates cybercriminels, mais pour préserver leur vie privée.

Notre analyse de la notion de pirate sous trois visages s'est articulé autour des tentatives de régulation juridique des évolutions techniques et sociales qui peu à peu normalisent ces comportements, et des rapports entre les infrastructures développées par les pirates et les normes sociales qui en découlent (les usages au sens de Cohen, 2012). Leurs activités s'amorcent souvent dans un espace non régulé par le droit, un îlot de liberté caractérisé par le vide législatif. Ces activités sont, par conséquence, hors-la-loi, bien qu'elles ne soient pas (encore) illégales. C'est avec l'expansion du droit pour les contrer que ces activités acquièrent un statut illégal et que la marge de manœuvre des acteurs du réseau se réduit par conséquent. Les pirates informatiques sont alors tous poussés à innover vers de nouveaux territoires. Grâce à leur maîtrise des nouvelles technologies, ils développent et utilisent de nouveaux outils de communication et de diffusion qui se présentent comme des plateformes plus libres et diverses que les médias existants dans l'offre dite légale. S'en suit une période d'opposition avec le pouvoir établi, qui va tenter d'empêcher le développement de ces nouvelles techniques, le plus souvent par des moyens juridiques.

Les nouvelles pratiques sont toujours difficiles à qualifier lors de leur introduction car elles reflètent des luttes sur l'évolution du droit face à l'innovation, entre maintien des prérogatives et modèles des acteurs installés et soutien aux activités économiques et culturelles naissantes. Quelques années après leur introduction, les nouvelles pratiques sont classiquement régulées et entrent dans la norme, les radios pirates deviennent radios libres, les matériels et supports de

reproduction privée sont taxés, les intermédiaires sont responsabilisés. Il s'agit alors de déterminer si la dialectique entre technique et droit peut arriver à réguler les comportements déviants sans exclure les activités à la marge mais source d'innovation. Construit social autour d'une dialectique entre droit et technique, les pirates contribuent (par une force centrifuge) à transformer l'infrastructure technique et juridique et donc les normes sociales.

Références

AIGRAIN Philippe, 2012, *Sharing: Culture and the Economy in the Internet Age*, Amsterdam, Amsterdam University Press.

AURAY Nicolas, 2009, « Pirates en réseau : détournement, prédation et exigence de justice », *Esprit*, vol. 7, p. 168-179.

BARLOW John Perry, 1996, A Declaration of the Independence of Cyberspace, ressource en ligne: https://projects.eff.org/~barlow/Declaration-Final.html (visité le 07-01-2014)

AFDI, 1966, La répression des émissions de radiodiffusion effectuées par des stations hors des territoires nationaux. — Législations nationales et accord européen, *Annuaire français de droit international*, vol. 12, p. 470-502.

BARRATT Monica J., 2012, « Silk road: eBay for drugs », *Addiction*, n°107, vol. 3, p. 683-683.

BENDRATH Ralf et MUELLER Milton L., 2011, « The end of the net as we know it? Deep packet inspection and internet governance », *New Media & Society*, n° 13, vol. 7, p. 1142-1160.

BOYLE James, 1997, « Foucault in cyberspace: Surveillance, sovereignty, and hardwired censors », *University of Cincinnati Law Review*, n°66, p. 177-205.

DEIBERT Ronald J., 2003, « Black code: Censorship, surveillance, and the militarisation of cyberspace », *Millennium-Journal of International Studies*, n° 32, vol. 3, p. 501-530.

COHEN Julie E., 1997, « Some reflections on Copyright Management Systems and Laws Designed to Protect Them », *Berkeley Technology Law Journal*, n°12, p. 161-187.

- 2012, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, Yale, Yale University Press.

COLEMAN Gabriella, 2011, « Hacker Politics and Publics », *Public Culture*, n° 23, vol. 3, p. 511-516.

DELAMOTTE Eric, LAMARCHE Thomas, et ZIMMERMANN Jean-Benoît, 2009, « La propriété intellectuelle emportée par le numérique ? », *Terminal,* n° 102, Paris, L'Harmattan.

DREZNER Daniel W., 2004, « The global governance of the Internet: Bringing the state back in », *Political Science Quarterly*, n° 119, vol. 3, p. 477-498.

DULONG DE ROSNAY Mélanie, 2007, *La mise à disposition des œuvres et des informations sur les réseaux. Régulation juridique et régulation technique*, Doctorat de droit public, Université Paris 2

DUSOLLIER Séverine, 2005, *Droit d'auteur et protection des œuvres dans l'univers numérique – Droits et exceptions à la lumière des dispositifs de verrouillage des œuvres*, Bruxelles, Larcier.

ENGEL Christoph, 2006, « The Role of Law in the Governance of the Internet », *International Review of Law Computers & Technology*, n° 20, vol. 1-2, p. 201-216.

GANTZ John et ROCHESTER Jack B., 2005, *Pirates of the Digital Millennium*, Upper Saddle River, NJ, Prentice Hall/Financial Times.

GARIBIAN Sévane, 2008, « Hostes humani generis: les pirates vus par le droit », *Critique*, n° 733-734, p. 470-479.

GINSBURG Jane C., 2002, « Essay-How Copyright Got a Bad Name For Itself », *Columbia Journal of Law and the Arts*, 26(1), p. 61-62

GOLDSMITH Jack L. et WU Tim, 2006, *Who Controls the Internet? Illusions of a Borderless World*, Oxford, Oxford University Press.

GUÉDON Jean-Claude., 2003, « Open Access Archives: from scientific plutocracy to the republic of science », *IFLA Journal*, n° 29, vol. 2, p. 129-140.

HADOPI, 2011, Biens culturels et usages d'Internet : pratiques et perceptions des internautes français,

83 p., ressource en ligne : http://www.hadopi.fr/download/hadopiT0.pdf (visité le 07-01-2014)

HARRIS Frances J., 2011, *I Found it on the Internet: Coming of Age Online*, Chicago, IL, ALA Editions.

HINTIKKA Kari A., 2008, « Pirates in Politics–Internet Piracy as Individualised Politics », *Net Working/Networking: Citizen Initiated Internet Politics*, Teoksessa Häyhtiö, Tapio & Rinne, Jarmo éd., Tampere, Finland, Tampere University Press. , p. 335-354

HUYGEN Annelies *et al*., 2009, *Ups and downs. Economic and cultural effects of file sharing on music, film and games*, a study by TNO Information and Communication Technology, SEO Economic Research and the Institute for Information Law, commissioned by the Dutch Ministries of Education, Culture and Science, Economic Affairs and Justice. Resource en ligne: http://www.ivir.nl/publicaties/vaneijk/Ups_And_Downs_authorised_translation.pdf (visité le 07-01-2014)

INA, « Pop pirate », Zoom, 28 juillet 1966, 22 mn.

INA, « Lecat au Midem », 21 janvier 1980, 1 mn.

KOELMAN Kamiel et HELBERGER Natali, 2000, « Protection of technological measures », *Copyright and electronic commerce*, HUGENHOLTZ Bernt P. éd., Kluwer Law International, Information Law Series 8, p. 165-227.

LA RUE, Frank, 2011, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Office of the United Nations High commissioner for Human Rights, 22 p.

LESSIG Lawrence, 1999 *Code: And other laws of cyberspace*, New-York, Basic Books.

- 2003, « Law regulating code regulating law », *Loyola University Chicago Law Journal*, 35, 1. p. 1-14

LESUEUR Daniel, 2002, *Pirates des ondes : Histoire des radios pirates au XX^e siècle*, Paris, L'Harmattan.

LEVY Steven, 2001, *Hackers: Heroes of the computer revolution*, vol. 4, New York, Penguin Books.

LEVY Elias, 2004, « Criminals become tech savvy », *Security & Privacy, IEEE*, n° 2, vol. 2, p. 65-68.

LIEBOWITZ Stan J., 2006, Testing file-sharing's impact by examining record sales in cities. *Management Science, Vol. 54, No. 4, p. 852-859*

LITMAN Jessica, 1996, « Revising copyright law for the information age », *Oregon Law Review*, n° 75, p. 19-46.

MANION Mark et GOODRUM Abby, 2000, « Terrorism or civil disobedience: toward a hacktivist ethic », *ACM SIGCAS Computers and Society*, n° 30, vol. 2, p. 14-19.

Moitessier Bernard, *Tamata et l'Alliance*, Arthaud, 1993, 401 p.

MUSIANI Francesca, 2013, *Nains sans géants. Architecture décentralisée et services Internet*, Paris, Presses des Mines.

OBERHOLZER-GEE Félix et STRUMPF Koleman, 2007, « The effect of file sharing on record sales: An empirical analysis », *Journal of Political Economy*, n° 115, vol. 1, p. 1-42.

POST David G., 1996, « Governing cyberspace », *Wayne Law Review*, n°43, p. 155-171

SAMUEL Alexandra W., 2004, *Hacktivism and the future of political participation*, Doctoral dissertation, Harvard University Cambridge, Massachusetts.

SAMUELSON Pamela, 2003, « Digital Rights Management {and, or, vs.} the Law », *Communications of the ACM*, n° 46, vol. 4, p. 41-45.

- 2007, « Preliminary thoughts on copyright reform », *Utah Law Review*, No 3 (2007) p.551-571

SUBER Peter, 2012, *Open Access*, Cambridge, MIT Press.

THOMAS Douglas, 2003, *Hacker culture*, Minneapolis, University of Minnesota Press.

WEISER Phil, 2009, *The future of Internet regulation*, University of Davis Law Review, n°. 43, p. 529-590

ZICCARDI Giovanni, 2012, *Resistance, liberation technology and human rights in the digital age,* vol. 7. New York, Springer.