HAL open science

Surveillance et sécurisation: Ce que l'Hadopi rate

Franck Macrez, Julien Gossa

To cite this version:

Franck Macrez, Julien Gossa. Surveillance et sécurisation: Ce que l'Hadopi rate. Revue Lamy Droit de l'immatériel, 2009, 50, pp.79-91. hal-02971874

HAL Id: hal-02971874

https://hal.science/hal-02971874v1

Submitted on 2 Aug 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Surveillance et sécurisation : ce que l'Hadopi rate.

À propos de la petite loi « Création et Internet »

Franck Macrez

Maître de conférences

Centre d'Études Internationales de la Propriété Intellectuelle (Ceipi)

Université de Strasbourg

Julien Gossa

Maître de conférences

Laboratoire des Sciences de l'Images, de l'Informatique et de la Télédétection (LSIIT)

Imagerie et Calcul Parallèle Scientifique (ICPS)

Université de Strasbourg

Introduction

I.- La mission de surveillance des réseaux par l'Hadopi

A.- Un champ d'application limité au pair-à-pair

1.- Les moyens techniques de diffusion des œuvres

a.- Les diffusions « face-à-face »

b.- Les diffusions centralisées : le streaming et les newsgroups

c.- Les diffusions décentralisées : le pair-à-pair

2.- Une surveillance complexe

B.- Une constatation des faits laborieuse

1.- Les faits illicites constatés

a.- L'identification des contenus protégés

b.- Les opérations à constater

i.- Les opérations nécessaires au téléchargement

ii.- Caractère illicite de ces opérations

2.- L'identification de l'auteur des faits constatés

a.- La difficile détection des contrefacteurs

i.- IP dynamiques

ii.- L'utilisation de proxy

iii.- Translation

b.- La fausse détection

II.- L'obligation de surveillance de son accès par l'abonné

A.- Sécurisation de l'accès

1.- Notion de sécurisation

a.- Sécurisation de l'accès sans fil et évolution technique

b.- Filtrage des communications, paramétrage et inégalité des compétences.

2.- Notion d'accès

B.- Le « moyen de sécurisation »

1.- Le logiciel espion et son possible détournement

2.- Le « moyen de sécurisation » : une faille de sécurité ?

Introduction

1. Présentation de la petite loi. Le projet de loi « favorisant la diffusion et la protection de la création sur internet » est issu des « accords de l'Elysée » intervenus à la suite du rapport Olivennes[1]. L'objectif poursuivi par le texte est de lutter contre le « développement de la piraterie numérique », « menace contre la vitalité culturelle en France »[2], autrement dit les téléchargements non autorisés d'œuvres protégées par un droit de propriété littéraire et artistique[3]. L'économie du dispositif législatif consiste principalement en la mise en place de sanctions à l'obligation de surveillance de leur accès par les abonnés à un service Internet, créée par la loi « Dadvsi » du 1er août 2006 (article L. 335-12 du Code de la propriété intellectuelle). Pour ce faire est instituée une Autorité Administrative Indépendante, communément dénommée « Hadopi », qui se substitue à l'Autorité de Régulation des Mesures Techniques et qui est investie d'un certain nombre de missions.

2. Les missions de l'Hadopi. La Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet est une autorité publique indépendante (art. L. 331-12 nouveau[4]), c'est-à-dire une autorité administrative indépendante dotée de la personnalité juridique. Sa mission est définie à l'article 2 de la loi créant un nouvel article L. 331-13. L'Hadopi assure :

« 1° Une mission d'encouragement au développement de l'offre légale et d'observation de l'utilisation licite et illicite des œuvres et des objets auxquels est attaché un droit d'auteur ou un droit voisin sur les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne ;

---

1 D. Olivennes, Le développement et la protection des œuvres culturelles sur les nouveaux réseaux, Rapport au ministre de la culture et de la communication, Paris, nov. 2007. V. : J.-B. Auroux, *Rapport Olivennes : les grandes lignes de la loi DADVSI 2 ?*, RLDI 2007, 12, Analyse in°33 ; v. sur la genèse du projet : M. Coulaud, « L'adoption au Sénat du projet de loi «Création et internet»: la confirmation d'une méthode de régulation consensuelle en propriété littéraire et artistique », RLDI 2009, 46, Étude, 1532, p.85.

2 F. Riester, Rapport n°1486 sur le projet de loi favorisant la diffusion et la protection de la création sur internet, Assemblée Nationale, p. 11 et s (pour les deux citations).

3 Car en dépit de l'omniprésence, dans les débats au Parlement et dans les médias, des termes « piratage », « piraterie » ou « pirate », cela ne révèle aucun sens juridique dans le contexte qui est le nôtre : nous sommes bien loin des côtes somaliennes.

4 Les références à la loi nouvelle sont basées, dans cette étude, sur la « Petite loi » (Projet de loi favorisant la diffusion et la protection de la création sur internet, Assemblée nationale, n°275), antérieure à la décision du Conseil constitutionnel, non encore intervenue à la date de rédaction de ces lignes.

2° Une mission de protection de ces œuvres et objets à l'égard des atteintes à ces droits commises sur les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne ;
3° Une mission de régulation et de veille dans le domaine des mesures techniques de protection et d'identification des œuvres et des objets protégés par un droit d'auteur ou par un droit voisin. »

3. La mission centrale de « protection des œuvres ». La nouveauté réside dans les deux premières missions, puisque le 3° est une reprise de la mission dévolue à l'Autorité de Régulation des Mesures Techniques.
La mission centrale est celle décrite au 2° (elle figurait d'ailleurs en première position dans le projet initial du gouvernement) : mission de « protection des œuvres » sur les réseaux informatiques, ce qui désigne tout acte de contrefaçon en ligne, quelle qu'en soit la modalité ou la technique utilisée (pair-à-pair, *streaming*, etc.)[5]. Au-delà de l'apparente tautologie, cette mission implique la mise en œuvre de la fameuse « riposte graduée », décrite précisément à l'article L. 331-24 nouveau : « Lorsqu'elle est saisie de faits susceptibles de constituer un manquement à l'obligation définie à l'article L. 336-3, la commission de protection des droits peut envoyer à l'abonné […] une recommandation lui rappelant les dispositions de l'article L. 336-3, lui enjoignant de respecter l'obligation qu'elles définissent et l'avertissant des sanctions encourues en cas de renouvellement du manquement présumé […].
En cas de renouvellement […] de faits susceptibles de constituer un manquement à l'obligation définie à l'article L. 336-3, la commission peut adresser une nouvelle recommandation […]. Elle peut assortir cette recommandation d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date d'envoi de cette recommandation. »
Dans l'hypothèse où l' « abonné » ne se conforme aux obligations qui lui ont été rappelés, l'Hadopi peut prononcer des sanctions (art. L. 331-25 nouveau) : « suspension de l'accès au service » (1°) et « injonction de prendre […] des mesures de nature à prévenir le renouvellement du manquement constaté, notamment un moyen de sécurisation » (2°).

4. La mission d'observation des usages. La seconde mission caractéristique de l'Hadopi est celle « d'encouragement au développement de l'offre légale et d'observation de l'utilisation licite et illicite des œuvres et des objets auxquels est attaché un droit d'auteur ou un droit voisin sur les réseaux de communications électroniques utilisés pour la fourniture de services de

5 Rapport Riester, p.106.

communication au public en ligne » (article L. 331-13, 1°). À ce titre la Haute Autorité est chargée de publier annuellement des « indicateurs dont la liste est fixée par décret » (art. L. 331-21-1, al. 1er) : il s'agira par exemple du « nombre de titres musicaux, de séries et de films proposés dans les catalogues de téléchargement légal ; le volume de téléchargements d'œuvres ou d'objets protégés via des plates-formes légales ; le volume de téléchargements non autorisés ; le chiffre d'affaires engendré par les plates-formes de téléchargement légal ; le montant des droits non perçus du fait des téléchargements non autorisés »[6]. Outre la mission de « labellisation » des offres présentant un « caractère légal » (al. 2), elle « identifie et étudie les modalités techniques permettant l'usage illicite des œuvres […] ». Nous nous concentrerons, dans le cadre de cette étude, sur la mission de protection des œuvres.

5. L'objet de la loi et le bonneteau des qualifications. L'objet principal de la loi est de créer à la charge de l'abonné une obligation de surveillance de son accès. Le but évident est de contourner la censure de la « riposte graduée » opérée par le Conseil constitutionnel[7], ayant considéré que des sanctions différentes de pouvaient être attachées à une même qualification de contrefaçon[8]. Obligation de surveillance distincte, donc, mais consistant à veiller que l'accès ne soit pas utilisé à des fins de contrefaçon. Il est difficile d'ailleurs d'imaginer que l'Hadopi avertisse ou sanctionne des internautes pour une autre raison, dès lors que sa mission est de s'assurer de la « protection des œuvres » sur Internet[9]. « Géniale justification »[10], « tour de passe-passe »[11] ou « piètre déguisement »[12] : ce jeu de bonneteau des qualifications juridiques consiste très clairement à « sanctionner la contrefaçon... sans le dire »[13]. Quelles que soient les

6 Rapport Riester, p.129.

7 M. Vivant, *et al., Lamy Droit de l'informatique et des réseaux*, Lamy, Paris, 2009, n°2525.

8 Cons. const., déc. n° 2006-540 DC, 27 juill. 2006, JO 3 août, n° 178, p. 11541

9 C. Alleaume, « Le projet de loi "Création et Internet" du 18 juin 2008 », Propriétés Intellectuelles 2008, 29, Libre opinion, p.388 (p.389 : « (…) ce n'est pas tant le *défaut de surveillance*, mais le *téléchargement illicite causé par le défaut de surveillance* qui sera poursuivi. Car, en fait, il est évident que celui-ci sera déduit de celui-là... »

10 A. Gitton, « La géniale justification d'une prise en otage de l'abonné à un service de communication en ligne : "Si ce n'est toi, c'est donc ton fils !" Ou un effondrement des cours de la loi et du juge », RLDI 2008, 8, Etude, 41.

11 C. Alleaume, « Le projet de loi "Création et Internet" du 18 juin 2008 », préc., p.389.

12 A. Gitton, préc., n°48.

13 M. Vivant et *al*., préc. n° 2525.

éventuelles censures et / ou réserves que le Conseil constitutionnel apportera sur cette petite loi[14], il apparaît nécessaire d'analyser le dispositif, notamment quant à son effectivité.

6. Quelle mise en œuvre ? Quelle effectivité ? La mise en œuvre de ces différentes missions implique de mobiliser de nombreux moyens informatiques. Il en est de même de l'obligation de l'abonné de sécurisation de son accès à Internet. Car la loi « Création et Internet » n'est pas, substantiellement, une loi de droit d'auteur, mais bien une loi qui porte sur des questions liées à la sécurité informatique et les questionnements qu'elle induit doivent naturellement s'insérer dans ce cadre. Ainsi, il apparaît important de mesurer l'effectivité, l'efficacité, voire les dangers du dispositif, en tenant compte de cette dimension technique : de quelle manière, concrètement, la Haute Autorité va-t-elle exercer sa mission de surveillance des réseaux de téléchargement illégal ? Quelle est la teneur de l'obligation de sécurisation de son accès par l'abonné ? Les difficultés, tenant à la complexité des architectures informatiques, ne peuvent laisser le juriste indifférent puisqu'elles impliquent des incertitudes quant au principe du contradictoire, au droit des données personnelles et, finalement, à l'effectivité des règles de la propriété littéraire et artistique sur les réseaux numériques. Du point de vue de la Haute autorité, cela conduit à analyser la manière dont devrait être menée sa mission de surveillance (I), tandis que du point de vue de l'abonné il faut mesurer ce que recouvre l'obligation de sécurisation de son accès à Internet (II).

I.- La mission de surveillance des réseaux par l'Hadopi

7. Surveillance des réseaux et traçage des internautes. La mission de surveillance des réseaux par l'Hadopi doit être exercée par la commission de protection des droits sur saisine d'« agents assermentés » (nouvel article L. 331-22, al. 1er) ou du procureur de la République (al. 2). La commission « dispose d'agents publics assermentés » (art. L. 331-20, al. 1er) qui, tout comme les membres de la commission, reçoivent les saisines ; ils « procèdent à l'examen des

14 V. La saisine est consultable en ligne, p. ex. sur le site web de PC Inpact : M. Rees, « Hadopi : le recours devant le Conseil Constitutionnel en détail », PC Inpact 20 mai 2009, <www.pcinpact.com> ; v. aussi les critiques dressées par M. Gitton, art. préc. (not., n°48, par rapport au principe de légalité de délits et des peines : « Tant que l'on ne dissociera pas la responsabilité du titulaire de l'abonnement des faits de contrefaçon qui laissent supposer son défaut de surveillance, le dispositif légal constituera, sous un piètre déguisement, une violation permanente du principe de la personnalité des délits et des peines. »)

faits et constatent la matérialité des manquements à l'obligation » de sécurisation de l'accès de l'abonné (al. 2). Pour ce faire, il est expressément prévu qu'ils peuvent « obtenir tous documents, quel qu'en soit le support, y compris les données conservées et traitées par les opérateurs de communication électroniques […] » (al. 3).

8. Quelle effectivité ? Cette mission de surveillance des réseaux se heurte, pour sa mise en œuvre, à des difficultés factuelles : bien que la loi prétende englober l'ensemble des actes de contrefaçon de droit d'auteur sur les réseaux, son champ d'application semble, de fait, limité au « *peer-to-peer* » (A) ; et même dans ce cadre restreint, la mise en œuvre du dispositif apparaît pour le moins délicate (B).

A.- Un champ d'application limité au pair-à-pair

9. Égalité devant la loi ? Le choix de cantonner le champ d'application de la loi à la contrefaçon *en ligne* est en lui même critiquable, eu égard au principe d'égalité des citoyens devant la justice, selon lequel « tous les citoyens sans distinction plaideront en la même forme et devant les mêmes juges, dans les mêmes cas »[15].

10. Neutralité technique ? La généralité de la règle de droit implique que le législateur se contente de « légiférer en des termes généraux afin de ne pas obérer la pérennité du régime de protection mis en place »[16]. La mission de surveillance de l'Hadopi concerne ainsi l'ensemble des techniques possibles de diffusion des œuvres *via* Internet, la loi ne visant pas l'une de ces techniques en particulier. Le rapport Riester en a d'ailleurs dressé un inventaire exhaustif, tout en centrant son propos sur « les techniques les plus répandues »[17] : le pair-à-pair et le *streaming*. En réalité, et bien que le *streaming* soit à juste perçu par le législateur comme un phénomène majeur de ces dernières années, cette petite loi *ne concerne effectivement que le seul pair-à-pair*. Le champ d'application effectif de la loi peut en effet se déterminer à l'analyse des actes surveillés par la Haute autorité, aussi en bien en ce qui concerne les différentes techniques de téléchargements (1), que les différents actes techniques du téléchargement (2).

---

15 Loi des 17 et 24 août 1790.

16 A. Latreille et T. Maillard, "Mesures techniques de protection et d'information", J.-Cl. Propriété littéraire et artistique, fasc. 1660, n°15.

17 Rapport Riester, p. 13, se fondant sur l'étude réalisée par la société QualiQuanti pour le compte du centre national de la cinématographie : *Les nouvelles formes de consommation des images : TNT, TVIP, VOD, sites de partage, piraterie… Analyse qualitative*, nov. 2007, <www.cnc.fr>, p.38 et s., à propos de « la piraterie » (sic), de sa généralisation et de ses techniques.

1.- Les moyens techniques de diffusion des œuvres

11. La variété des moyens techniques de diffusion des œuvres peut être présentée selon la typologie suivante : les diffusions « face-à-face » (a), les diffusions centralisées (b), et les diffusions décentralisées (c).

a.- Les diffusions « face-à-face »

12. ***Friend-to-friend* : hors ligne et en ligne.** Les diffusions « humaines », aussi appelées « face-à-face », se retrouvent dans la catégorie « disques durs externes » du rapport Riester[18] et sont une pratique concernant les échanges de contenus par le déplacement de leurs supports physiques : elle se rapporte aux pratiques d'échange avant la démocratisation de l'Internet. Elle est actuellement facilitée par la démocratisation et l'augmentation considérable des capacités de stockage et de communication des supports portables (par exemple, les téléphones modernes de base sont capables de stocker une dizaine de films et une centaine d'albums de musique). Ces pratiques n'impliquant pas Internet (« les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne », pour reprendre les termes de la loi), elles sont *de facto* hors du champ de la petite loi.
La technique appelée *Friend-to-Friend* (ou F2F par analogie au P2P)[19] peut être considérée comme analogue à ces pratiques mais, cette fois, dans un environnement en ligne. Les utilisateurs font partie d'un réseau social, c'est-à-dire qu'ils doivent connaître quelqu'un appartenant au réseau et être acceptés par les autres utilisateurs avant de pouvoir partager des fichiers.

13. **Absence de surveillance du *Friend-to-friend*.** Outre le fait que l'acte de contrefaçon hors ligne n'est pas concerné par la petite loi, il est clair que le *friend-to-friend* exercé *via* Internet ne peut, en pratique, entrer dans la mission de l'Hadopi. En effet, un tel système fonctionne, comme son nom l'indique, *entre amis*, ou tout au plus par un mécanisme de cooptation. Les réseaux, s'organisent autour de communautés dans lesquelles les communications sont privées, empêchant tout contrôle des données échangées. Mener des investigations au sein de tels réseaux pour constater des atteintes aux droits de propriété littéraire et artistique nécessiterait des moyens considérables d'intrusion et d'infiltration à

18 *Ibidem.*

19 J. Li et F. Dabek, « F2F: Reliable Storage in Open Networks » *in* 5th International Workshop on Peer-to-Peer Systems (IPTPS '06), Santa Barbara, CA, USA, Février 2006, <http://pdos.csail.mit.edu/>

l'intérieur de « réseaux d'amis » qui échangent des œuvres protégées d'autant qu'une communauté ciblée par la riposte graduée sera instantanément dissoute ou désertée de ses membres. Plus incontrôlable encore, il est probable que des toiles de « *box* » en accès libre se développent, en particulier dans les lieux de concentration d'internautes, comme les villes : les capacités de communications sans-fil de ces « *box* » peuvent être utilisées afin de créer des réseaux privés étendus indépendants d'Internet : les contrefacteurs pourraient alors échanger des fichiers sans aucun contrôle.

En outre, il est vraisemblable que la menace que va constituer l'Hadopi sur les réseaux pair-à-pair va conduire à un regain de popularité de telles techniques d'échange de fichiers dont la popularité était jusqu'alors toute relative en raison des attraits du pair-à-pair. En effet, l'augmentation des vitesses de connexion, en particulier avec l'expansion du très haut débit par fibre optique, encouragée par le gouvernement[20], rendra les techniques de pair-à-pair inutiles car ces techniques ont pour objectif premier de palier à la lenteur des connexions en permettant de télécharger un même fichier depuis plusieurs sources simultanément. Avec la fibre optique, une seule source sera capable d'alimenter de nombreux clients. Les techniques de *streaming* seront alors utilisables directement entre pairs[21] : l'absence de serveur rendra impossible les contrôles éventuels du *streaming* actuel, alors que le faible nombre de protagonistes nécessaires à un téléchargement donné rendra très difficile la détection des internautes. Les réseaux privés fermés qui se développent lentement depuis plusieurs années prendront alors une ampleur sans précédent.

Pour l'heure, il faut simplement relever que l'Hadopi ne dispose pas des moyens de contrôler ce type de technique, ce qui est assurément une faiblesse du dispositif quant à son effectivité et à sa pérennité.

b.- Les diffusions centralisées : le streaming *et les* newsgroups

14. Présentation: *newsgroups* et *streaming.* Dans les échanges par diffusions centralisées, les internautes sont désignés par le terme « clients » et utilisent un « serveur » pour obtenir des contenus protégés, qui font en général l'objet d'un hébergement professionnel. L'objectif de ces

20 V. le plan de développement de l'économie numérique confié, le 2 avril 2008, au Secrétaire d'État chargé de la Prospective, de l'Évaluation des politiques publiques et du Développement de l'économie numérique par le Président de la République et le Premier Ministre : <www.francenumerique2012.fr>.

21 Y. Liu1, Y. Guo et C. Liang, « A survey on peer-to-peer video streaming systems » *in Peer-to-Peer Networking and Applications, Springer New York, 2008.*

sites est de dégager des revenus, soit par la publicité, soit par des abonnements. Comme présenté dans le rapport Riester, ils concernent essentiellement les *newsgroups* et le *streaming*.

La technique des *newsgroups* consiste à détourner l'utilisation première des serveurs de *news* (« Service permettant discussions et échanges sur un thème donné : chaque utilisateur peut lire à tout moment les interventions de tous les autres et apporter sa propre contribution sous forme d'articles »[22]) à l'origine conçus pour fonctionner comme des forums de discussion. Gratuits ou payants, mis à disposition par les fournisseurs d'accès ou par des tiers, ils sont maintenant utilisés pour échanger des contenus protégés. Leur utilisation est loin d'être aisée et demande de bonnes connaissances techniques. Les contenus sont peu nombreux et disponibles en temps très limité, en revanche leur récupération est extrêmement rapide.

La technique du *streaming* consiste, quant à elle, à se connecter à un site Internet mettant à disposition illégalement des contenus protégés et à les visualiser directement dans son navigateur Web. Elle est donc très facile à mettre en œuvre par n'importe quel utilisateur, pouvant même être amené à penser être sur une plate-forme légale. Les contenus sont immédiatement disponibles, en revanche ils sont en général en anglais non sous-titré, puisque sur des plates-formes étrangères, et limités aux dernières sorties, puisque le modèle économique de ces sites est basé sur la publicité avec pour critère principal le nombre de visites.

15. L'impossible surveillance décentralisée des diffusions centralisées. Étant basée sur une communication directe entre un serveur et un client, trois méthodes de détection de la contrefaçon par diffusion centralisée sont envisageables : au niveau du client, au niveau du serveur ou au niveau de la communication entre les deux.

- surveillance du serveur : soit en surveillant en temps réel ses connexions, soit en récupérant ses journaux de connexions. Ces serveurs étant systématiquement situés à l'étranger, cette approche semble difficile à mettre en œuvre par des moyens légaux sans une législation internationale. En tout état de cause, la mission de surveillance de l'Hadopi apparaît comme totalement inutile puisque les ayant-droits ne semblent pas avoir de difficulté particulière à intenter des actions devant les juridictions judiciaires à l'encontre du serveur[23].

22 V° « Forum » *in* Lamy Droit de l'Informatique et des Réseaux 2009 - Lexique relatif au vocabulaire informatique et à la terminologie des télécommunications et du réseau internet.

23 V. les nombreuses affaires ayant mis en cause les sociétés Dailymotion et Youtube.

- surveillance du client : cette surveillance se réalise par exemple *via* un logiciel espion reportant l'utilisation faite de la machine de l'internaute ou éventuellement par le blocage des sites incriminés. Cette approche est très difficile à mettre en œuvre, notamment en raison des incertitudes quant aux spécifications fonctionnelles à assigner au « moyen de sécurisation[2]» (*infra* Partie II).

- surveillance des lignes de communication : on peut envisager de bloquer l'accès à ces sites[24]. Cependant, cette activité pouvant dégager des revenus très importants, les administrateurs de ces sites n'hésitent pas à les fermer puis les rouvrir sous un autre nom afin de contourner les blocages, cette opération pouvant se faire pour quelques dizaines d'euros en quelques heures.

Ces trois approches impliquent une analyse fine des utilisations du réseaux où des machines des internautes, en particulier car le *streaming* illégal est techniquement indissociable du *streaming* légal. Or le *streaming* légal représente une majorité des utilisations d'Internet[25], il s'agirait donc d'analyser une très grande part des informations échangées sur l'Internet, ce qui impliquerait des temps de calcul gigantesques et en conséquence un ralentissement global de la vitesse d'Internet en France.

c.- Les diffusions décentralisées : le pair-à-pair

16. Les diffusions décentralisées n'impliquent pas de serveur ; les contenus sont échangés directement entre les machines des internautes, appelés « pairs », sans intermédiaire : c'est ce qui est communément dénommé pair-à-pair (ou *peer-to-peer*, ou encore *P2P*).

17. **Pair-à-pair.** Le pair-à-pair consiste à l'installation d'un logiciel dédié à l'échange des contenus stockés sur les machines des internautes. Le système ne présent pas, pour l'essentiel, de but lucratif, et demande souvent quelques connaissances techniques afin de paramétrer et d'utiliser correctement le logiciel. Le choix des contenus est extrêmement vaste, mêlant indifféremment contenus protégés et libres. N'ayant aucune instance de contrôle, il n'est pas rare que les contenus ne correspondent pas à leur présentation (d'où la remarque de Mme

24 C'est la méthode adoptée par le projet de loi « Loppsi » à propos du filtrage des sites pédopornographiques, devant être réalisé au niveau des fournisseurs d'accès : v. article 4 du projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure, présenté au Conseil des ministres le 27 mai 2009, <www.interieur.gouv.fr> (consulté le 1er juin 2009).

25 50% des visites uniques pour Youtube : v. « Internet dans le monde : trafic », <http://www.journaldunet.com>, 27 avril 2009 (source : Nielsen, mars 2009).

Albanel lors des débats à l'assemblée : « Les enfants qui tapent Winnie l'ourson ont 40 % de risques de tomber sur des films pornographiques »[26]). Il est à noter que cette technique est la plus lente, certains contenus pouvant mettre plusieurs semaines avant d'être finalement visualisables. Pour palier ce problème, des sites Web, appelés « *board »*, mettent à disposition non pas les contenus, mais des liens identifiants des contenus vérifiés disponibles sur les réseaux pair-à-pair. Bien que n'étant pas la plus efficace, le pair-à-pair étant probablement la technique de téléchargement la plus populaire, elle est la cible principale de l'Hadopi.

18. De la loi « Création et pair-à-pair ». Il semble à première vue logique que soit visée en premier lieu, parmi les fins poursuivies par la loi, la pratique la plus répandue pour la diffusion d'œuvres sans autorisation, même si la différence de traitement entre actes de contrefaçon en ligne et hors ligne est en elle même critiquable[27]. Mais en réalité, le pair-à-pair n'est pas le moyen *principalement* visé : il est *le seul moyen* concerné par la petite loi, malgré le texte même du projet et la présentation qui en a été faite par ses promoteurs[28]. Peut-être cela est-il le résultat d'une méconnaissance des techniques informatiques que l'on entend réguler[29]. Il s'agit plus sûrement d'une posture délibérée destinée à éviter la censure du Conseil constitutionnel en raison du non respect du principe d'égalité des citoyens devant la loi pénale. Car le but initial de cette loi « Création et pair-à-pair » est bien de remédier à la censure opérée à propos de la loi du 1er août 2006 et de sa « riposte graduée ». L'article 24 de la loi dite «DADVSI», instaurant une contravention pour le téléchargement et la mise à disposition d'œuvres sur les réseaux, avait été censuré par les sages de la rue Montpensier, qui avaient considéré que « (…) les personnes qui se livrent, à des fins personnelles, à la reproduction non autorisée ou à la communication au public d'objets protégés au titre de ces droits sont placées dans la même situation, qu'elles utilisent un logiciel d'échange de pair-à-pair ou d'autres

26 Assemblée Nationale, Compte rendu intégral, Première séance du mercredi 1 avril 2009. De forts soupçons, dont la réalité du fondement est invérifiable, dans la communauté des contrefacteurs pèsent sur la culpabilité des ayant-droits, qui entretiendraient cet état de fait afin de « polluer » le téléchargement de leurs contenus.

27 V. E. De Marco, « Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux », Juriscom.net 4 juin 2009, <www.juriscom.net>, spéc. p. 8.

28 Rapport Riester, pp.12 et s. ; D. Olivennes, Le développement et la protection des œuvres culturelles sur les nouveaux réseaux, Rapport au ministre de la culture et de la communication, Paris, nov. 2007, p. 6.

29 Les exemples tirés des débats parlementaires sont nombreux. Pour s'en tenir au rapport fait à l'Assemblée Nationale sur le projet de loi, celui-ci oppose « téléchargement » et « *streaming* » (p.13), ce qui est doublement absurde : le *streaming* nécessite un acte de téléchargement (même s'il n'est pas, comme tel, perçu par l'utilisateur), et les autres techniques présentées (*newsgroups*, FTP, etc.) relèvent également du téléchargement. Il faut comprendre (et traduire en conséquence) que dans l'esprit du rapporteur, « téléchargement » signifie « pair-à-pair ».

services de communication au public en ligne ; que les particularités des réseaux d'échange de pair-à-pair ne permettent pas de justifier la différence de traitement qu'instaure la disposition contestée ; que, dès lors, l'article 24 de la loi déférée est contraire au principe de l'égalité devant la loi pénale »[30] Dès lors qu'on veut bien ne pas s'en tenir aux apparences et analyser le texte pour ce qu'il est, c'est-à-dire un texte visant à sanctionner un seul des modes de téléchargement d'œuvres protégées sur Internet, il ne devrait pas résister à la censure du Conseil constitutionnel (malgré le fait que l'argument n'ait pas, à notre connaissance, été avancé par les auteurs de la saisine).

L'efficacité du dispositif projeté, c'est-à-dire l'adéquation aux fins visées par la norme juridique[31], peut également être questionnée. À supposer que l'Hadopi mène à bien sa mission de surveillance des réseaux pair-à-pair et endigue le phénomène (ce qui reste, selon nous, douteux), l'étroitesse du champ qu'il est possible de surveiller conduirait les internautes à reporter leurs pratiques vers des moyens techniques que la Haute autorité ne pourra appréhender. En d'autres termes, l'internaute adepte du pair-à-pair se reportera vers une solution *Friend-to-friend* (ou tout autre moyen précédemment évoqué, de manière non exhaustive) pour éviter les foudres de l'Hadopi. Les statistiques pourraient même être très encourageantes (puisqu'elles porteraient sur le pair-à-pair) tandis que la réalité resterait quasiment inchangée, puisque la loi serait de ce fait obsolète et inadaptée. Des vicissitudes de « la courte vue érigée en principe »[32] de législation...

Par ailleurs, au sein de ce champ d'application beaucoup plus étroit que celui de la contrefaçon en ligne de manière générale, la mission assignée à l'Hadopi se révèle particulièrement complexe.

2.- Une surveillance complexe

19. Nécessité d'un pair-espion. Les réseaux pair-à-pair n'impliquent pas nécessairement de serveur : les internautes échangent directement les contenus protégés entre eux, sans intermédiaire. La surveillance de ces réseaux doit donc être mise en œuvre par l'exécution d'un pair-espion : l'entité de surveillance utilise les mêmes logiciels que les internautes à surveiller

30 Conseil constitutionnel 27 juillet 2006, décision n°2006-540, considérant n°65.

31 V° « Efficacité » *in* A.-J. Arnaud (dir.), Dictionnaire encyclopédique de théorie et de sociologie du droit, LGDJ, Paris, 1993.

32 M. Vivant et J.-M. Bruguière, Droit d'auteur, Dalloz, coll. « Précis Droit Privé », Paris, 2009, n°12.

et se contente de repérer les pairs se livrant aux différents actes de téléchargement. Les difficultés principales de mise en œuvre de la surveillance de ces flux de données tiennent à la complexité des algorithmes utilisés et au fait que les « surveillants » peuvent être détectés.

20. Complexité des algorithmes. Une première difficulté est impliquée par les algorithmes utilisés par les réseaux pair-à-pair. Il est techniquement impossible d'effectuer une recherche parmi les contenus mis à disposition par les millions d'utilisateurs d'utilisateurs de ces réseaux : les recherches seraient trop longues et trop de messages seraient envoyés sur le réseau. Pour palier ces problèmes, des algorithmes très évolués ont été développés (le plus utilisé étant Kademlia[33]), qui ont pour but de garder une bonne qualité de recherche tout en réduisant le nombre de pairs à quelques centaines. Dans le but de collecter le plus d'adresses de contrefacteurs, les surveillants devront modifier ces algorithmes dans leur pair-espion. En plus de la difficulté technique, voire scientifique, de cette tâche, le nombre de ces algorithmes et leur rapidité d'évolution implique un travail très conséquent et continu[34]. De plus, l'exécution d'algorithmes modifiés altère le comportement du pair-espion, ce qui augmente de fait les risques de détection des surveillants par l'ensemble des autres pairs.

21. Détection des surveillants : le jeu du « chat et de la souris ». La surveillance des réseaux pair-à-pair implique obligatoirement un jeu du « chat et de la souris » entre contrefacteur et surveillants. Cela a été le cas dans les réseaux pair-à-pair impliquant des serveurs : après que des ayants-droit ont mis en place des serveurs espions collectant toutes les mises à disposition des utilisateurs, les logiciels de pair-à-pair ont intégré un système de filtrage des serveurs soupçonnés d'être des espions. Commence alors le jeu du « chat et de la souris » : les surveillants créent de nouveaux serveurs espions pas encore filtrés, puis les contrefacteurs les intègrent dans la liste de filtrage. Une des raisons du développement des systèmes de pair-à-pair totalement décentralisés (c'est-à-dire sans serveur intermédiaire), en plus de la possibilité d'action à l'encontre de l'hébergeur du serveur lui-même comme cela a été par exemple le cas pour Napster aux États-Unis[35], est d'éviter ce fastidieux travail. Avec des surveillants utilisant

33 Maymounkov, Petar et Mazieres, David « Kademlia: A peer-to-peer information system based on the xor metric » *in Peer-to-peer systems : First International Workshop*, IPTPS 2002, Cambridge, MA, USA.

34 V. Martins, E. Pacitti et P. Valduriez, « Survey of data replication in P2P systems », Rapport de Recherche inria-00122282, 2006.

35 United States District Court for the Northern District of California, 10 août 2000, n° C 00-0074 MHP, Sony Music Entertainment, Inc. et autres c/ Napster, Inc.

des pair-espions, ce jeu recommencera et on peut prévoir une utilisation massive de logiciels de filtrage tels que *PeerGardian*[36] qui bloquent toutes les communications avec les machines soupçonnées d'être utilisées par les surveillants. Finalement, le champ d'application de la mission de surveillance de l'Hadopi se voit restreint par les parades qui sont déjà pratiquées sur les réseaux et ont vocation à se généraliser, avant même que le dispositif ne soit mis en application.

B.- Une constatation des faits laborieuse

1.- Les faits illicites constatés

22. S'agissant de la constatation de faits de contrefaçon, la mission de l'Hadopi implique que les téléchargements observés concernent des œuvres protégées (a), ainsi qu'une interprétation de sa part concernant l'illicéité des opérations en cause (b).

a.- L'identification des contenus protégés

23. **Le *watermarking* et ses limites.** L'identification des contenus protégés est en réalité une opération très complexe, en particulier sur les réseaux pair-à-pair. En effet, les recherches sur ces réseaux sont basées sur le nom du fichier, qui peut-être facilement modifié lors de la déclaration de mise à disposition (sur laquelle, *infra* n°25). Ainsi des contenus protégés peuvent porter des noms fantasques, tout comme des contenus libres peuvent porter le nom de contenus protégés. C'est pourquoi les ayants-droits financent des recherches sur les techniques de tatouage numérique (*watermarking*[37]) : elles permettent d'identifier le contenu réel d'un fichier indépendamment de son nom, et donc de certifier qu'il s'agit d'un contenu protégé. Deux problèmes se posent. Tout d'abord ces techniques nécessitent de disposer des contenus, il faudrait donc télécharger intégralement chacun des fichiers partagés sur Internet avant de vérifier formellement et avec certitude leur contenu, ce qui est impossible compte tenu de leur nombre. Ensuite, si les contenus diffusés par les ayant-droits font l'objet de ces techniques, ce n'est pas le cas des contenus créés par les contrefacteurs (par exemple numérisation de DVD) : des contenus protégés non identifiables seront donc toujours mis à disposition.

36 <http://phoenixlabs.org/pg2/>

37 V., p. ex. : Digital WatermarkingWorld, <http://www.watermarkingworld.org/>.

On peut ainsi prévoir que les agents assermentés se contenteront de surveiller une liste restreinte de contenus formellement identifiés comme protégés, parmi les plus populaires et probablement en se basant sur liens mis à disposition dans les « *boards* » (v. *supra* n°17). Cela n'empêche pas l'œuvre en soi d'être contrefaite puisqu'une même œuvre est en général distribuée dans plusieurs dizaines de fichiers, différant par leur langue, sous-titrage, qualité et format (et souvent même sensiblement identiques, mais simplement diffusées par des internautes différents). L'internaute avisé pourra alors télécharger impunément les versions ayant peu de chance d'être surveillées, par exemple une version originale non sous-titrée, dans un format peu populaire, non répertoriée sur les « *boards* », diffusée par un contrefacteur original peu populaire et proposant peu de sources de téléchargement.

b.- Les opérations à constater

24. Il convient de rappeler quelles sont les différentes opérations réalisées lors d'un téléchargement (i) avant qu'en soit discuté le caractère illicite tel que l'Hadopi devra le déterminer (ii).

i.- Les opérations nécessaires au téléchargement

25. Les phases préalables obligatoires. La *recherche* est la phase préalable obligatoire au téléchargement : l'internaute formule une requête décrivant les contenus recherchés, contenant par exemple une partie du nom du titre, une taille minimum ou un type (p. ex. : audio, vidéo, ou même format numérique) ; il récupère ensuite une liste de contenus correspondants à ces critères, et pour chacun des contenus, la liste des sources le mettant à disposition. La *déclaration de mise à disposition* est la phase préalable obligatoire à l'*upload*. Elle consiste à déclarer une liste contenus pouvant être envoyés sur demande. La phase de recherche permet donc de récupérer parmi les déclarations de contenus, ceux qui correspondent à la requête formulée.

26. *Download* et *upload*. Le téléchargement (*download*) consiste à récupérer effectivement tout ou une partie d'un contenu au travers du réseau, qu'il provienne d'un pair ou d'un serveur. C'est l'acte majeur du piratage. Il est à noter que le *streaming* implique également un téléchargement, mais que le contenu est stocké de façon temporaire, *a contrario* des autres techniques. L'envoi de contenu (*upload*) consiste à envoyer effectivement tout ou une partie d'un contenu vers d'autres internautes. Il faut noter que les techniques de pair-à-pair permettent

le *download* et l'*upload* simultané[38], non seulement sur plusieurs contenus, mais également sur un même contenu : dès qu'une partie d'un contenu partagé est téléchargé, il est immédiatement mis à disposition en *upload*.

ii.- Caractère illicite de ces opérations

27. La nécessaire interprétation des textes. Les difficultés d'interprétation de la loi sur le droit d'auteur concernant le téléchargement sont connues des spécialistes : dans quelle mesure l'exception de copie privée peut-elle s'appliquer[39] ? L'acte de mise à disposition réalisé par l'*upload* est sans aucun doute contrefaisant, mais la qualification du *download* est discutée en doctrine. La question centrale est sans doute celle de la licéité de la source de la copie comme condition d'application de l'article L. 122-5, 2°. Et il est difficile d'ignorer la nécessaire application du triple test en la matière, en particulier sur la question de savoir s'il y a « atteinte à l'exploitation normale de l'œuvre »[40]. En tout état de cause, la cour d'appel de Paris, non censurée sur ces questions par la Cour de cassation, évite soigneusement de se prononcer sur le fond en déniant l'existence d'un « droit à » la copie privée et en en déduisant l'irrecevabilité de toute demande : « Pas de droit, pas d'action »[41].

Pourtant, la mission dévolue à la Haute autorité implique nécessairement que, pour chaque situation qui lui est soumise, soient tranchées des questions pour lesquelles il n'y a pas d'unanimité au sein des spécialistes et sur lesquelles les magistrats et le législateur ont évité de se prononcer. Les faits constatés seront-ils uniquement des téléchargements ascendants

38 Sur lequel, v. : F. Macrez, « Les pirates en galère... », RLDI 2005, 11, 305, spéc. n°4.

39 V. : A. Lucas et H.-J. Lucas, Traité de la propriété littéraire et artistique, Litec, 2006, n° 350 et s. ; M. Vivant et J.-M. Bruguière, Droit d'auteur, Dalloz, coll. « Précis Droit Privé », Paris, 2009, n° 585 et s. ; A. Latreille, « La copie privée démythifiée », RTD Com.. 2004, p.403 ; J. Larrieu, « "Peer-to-peer" et copie privée », Dalloz 2004, jurisprudence, p.3132 ; F. Macrez, *Créations informatiques : bouleversement des propriétés intellectuelles ? - Essai sur la cohérence des droits,* thèse Montpellier 2007 (à paraître aux éditions Litec, coll. du Ceipi), n°290 et s. ; A. Bensamoun, « La copie privée : victoire ou défaite du droit d'auteur ? », *RLDI* 2009, supp. au n°49, p.21.

40 Article L. 122-5 CPI, avant-dernier alinéa.

41 V. Cass. 1ère civ., 19 juin 2008, RLDI 2008/40, n°1322, obs. Costes L. ; RLDI 2009/46, n°1502, note Pignatari, O. ; RIDA 2008/3, pp. 209-223, spéc. p. 215, obs. Sirinelli P. ; RTD com. 2008, p. 551, obs. Pollaud-Dulian F. ; Comm. com. électr. 2008, comm. 102, note Caron Ch. Sur la question, v. en particulier : O. Pignatari, « "Pas de droit, pas d'action"… ou comment éviter la délicate appréciation du test des trois étapes », RLDI 2007, 27, n°15 ; S. Carre, « Le vertige de l'irrecevabilité (À propos de l'arrêt de la Cours de cassation du 19 juin 2008) », à paraître à la RIDA.

(*upload)* ou également des téléchargements descendants (*download*) ? Les phases préalables pourront-elles être jugées suffisantes, telle la déclaration de mise à disposition ?

28. L'Hadopi, interprète légitime ? Le choix d'une autorité administrative indépendante est en ce sens critiquable puisqu'elle est amenée à se prononcer sur des questions fondamentales pour l'économie générale du droit d'auteur[42], et que cette procédure se superpose aux voies judiciaires classiques, multipliant ainsi les risques d'antinomies[43] dans les nombreuses interprétations possibles[44]. En réalité, il semble que les agents assermentés et l'Hadopi se contentent, au moins dans un premier temps, de sanctionner *la mise à disposition* (l'*upload*) sur les réseaux pair-à-pair. En effet, le système prévu peut être analysé à travers le Cahier des Clauses Techniques Particulières (ci-après CCTP) « Acquisition d'un prototype de gestion de la mission de protection des œuvres et objets auxquels est attaché un droit d'auteur ou un droit voisin »[45] fourni par le ministère de la culture aux entreprises candidates à la mise en œuvre du système d'information de l'Hadopi, qui décrit précisément la procédure d'identification des contrefacteurs. La première étape, dénommée « c*ollecte de masse sécurisée* », concerne essentiellement la constitution des saisines selon les relevés des ayants-droit. Ces saisines « contiennent la constatation qu'un poste informatique ou autre équipement connecté *met à disposition sur Internet une ou plusieurs des œuvres protégées* par les droits d'auteur dont les ayants droit ont décidé de surveiller la diffusion, ainsi que l'adresse IP publique utilisée pour cette *mise à disposition*. »[46] Il reste à s'interroger sur le sens de l'expression « mise à disposition » utilisée ici : s'agit-il de constater simplement la *déclaration de mise à disposition*

---

42 « DADVSI 2, Hadopi, "Création et internet"... De bonnes questions ? De mauvaises réponses », Dalloz 2008, p.2290 : « (…) il est hors de doute que le juge judiciaire est techniquement le mieux placé et institutionnellement le plus légitime pour les mettre en œuvre. »

43 *Ibid.* : « Il est d'ailleurs permis de s'interroger sur les conséquences qui résulteraient d'un jugement statuant sur une action en contrefaçon et contredisant les décisions prises par la Commission. Mais conférer à la Commission de protection des droits des attributions concurrentes n'est-il pas le meilleur moyen de générer incohérences et chicanes ? »

44 En outre, il est possible de s'interroger du bien-fondé de ce transfert de compétences eu égard à la bonne administration de la justice : v. E. De Marco, art. préc., spéc. p.6.

45 G. Champeau, « Exclusif : l'Hadopi ciblera en priorité les récidivistes potentiels ! » *in* <http://www.numerama.com> (20/05/2009).

46 CCTP, p. 9 (nous soulignons). Le système de la SCPP, non autorisé par la Cnil en 2005, reprenait ces termes de « fichiers mis à disposition » : (CNIL, Délibération portant refus d'autorisation de la mise en œuvre par la Société Civile des Producteurs Phonographiques (SCPP) d'un traitement de données à caractère personnel ayant pour finalités, d'une part, la constatation des délits de contrefaçon commis via les réseaux d'échanges de fichiers dénommés "peer to peer", d'autre part, l'envoi de messages pédagogiques informant les internautes sur les sanctions prévues en matière de délit de contrefaçon, Délibération 2005-236 du 18 octobre 2005)

ou bien un *upload* effectivement réalisé ? Il semble que les agents assermentés se contentent de la première des opérations (qui n'implique donc aucun transfert effectif), tels ceux de la Sacem et de la SDRM qui relèvent l'adresse IP des internautes dès lors qu'ils ont eu accès à la « *liste des œuvres protégées* irrégulièrement proposées sur la toile »[47]. Cette déclaration de mise à disposition pourrait être considérée comme une tentative punissable, si ce n'est que, comme on l'a vu et de l'aveu même des promoteurs du mécanisme (*supra* n°17), les noms de fichiers peuvent n'avoir aucun rapport avec leur contenu réel. Il conviendrait dès lors que la saisine comporte le fichier en cause, ce qui est totalement irréalisable en termes de coût de stockage et de traitement[48].

Et, quoiqu'il en soit, un écueil subsiste : celui de l'identification de l'auteur des faits.

2.- L'identification de l'auteur des faits constatés

29. L'adresse IP, outil de l'identification. Le principe de personnalité des délits et des peines implique que soit identifié l'auteur de l'infraction constatée, indépendamment de la désignation de la personne responsable, réglée de manière originale par l'obligation de surveillance de l'accès par l'abonné *(infra* II). L'adresse IP est présentée comme le moyen principal permettant de repérer et d'identifier les contrefacteurs. Elle peut être comparée à un numéro de téléphone ou une adresse postale : c'est un numéro permettant d'acheminer les informations au travers du réseau physique de l'Internet. L'adresse IP utilisée lors des actes du téléchargement illégal est donc le seul moyen d'identifier les contrefacteurs. L'Hadopi peut obtenir l'identité civile de l'internaute utilisant une adresse IP auprès de son opérateur. Donnée à caractère personnel, le traitement automatisé nécessaire à la constatation des infractions sur les réseaux pair-à-pair soulève sans aucun doute des questionnements quant au respect des données personnelles des internautes, que nous n'envisagerons néanmoins pas spécifiquement dans cette étude[49].

---

47 Cass. crim., 13 janv. 2009, n° 08-84.088, RLDI 2009, 46, Actualité n°1507, obs. L. Costes (nous soulignons).

48 Une solution intermédiaire consisterait à joindre à la saisine une partie seulement du fichier (« chunk »). Mais les coûts de stockage resteraient exorbitants. V. : G. Champeau, « Exclusif : l'Hadopi ne collectera pas de preuve matérielle... pour l'instant », *Numerama* 27 mai 2009, <www.numerama.com>, citant « une information complémentaire transmise par le ministère de la Culture à un candidat au marché public ».

49 Il convient néanmoins de noter que la Cnil a rendu un rapport défavorable au projet de loi « Création et internet » (CNIL, Délibération n°2008-101 du 29 avril 2008 portant avis sur le projet de loi relatif à la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet, inédit, reproduit in La Tribune, 3 nov. 2008). En outre, une éminente spécialiste estime que « le dispositif issu de ce projet met en place des tolérances que l'on peut qualifier d'inacceptables si l'on s'en tient à la protection des données personnelles » :

Quant à l'identification de l'auteur de la mise à disposition (quelque soit la forme que l'on en retient), il faut relever que cette détection est particulièrement difficile à réaliser en raison des nombreux obstacles inhérents à certains dispositifs techniques (a), ce qui peut mener à des identifications erronées (b).

a.- La difficile détection des contrefacteurs

30. La procédure d'identification. Le Cahier des Clauses Techniques Particulières, dans sa description de la procédure d'identification des contrefacteurs, présente une procédure en trois étapes :

(1) *Collecte de masse sécurisée*, présentée *supra*.

(2) *Notarisation et échantillonnage*, dont l'objectif essentiel est de mettre en œuvre « des critères de sélection [qui] permettront à l'Hadopi de traiter une partie des saisines transmises par les ayants droit. »[50], ayant pour but de réaliser un échantillonnage permettant « d'identifier les adresses IP ayant de grandes chances de correspondre à des réitérations sur les 7 derniers jours de recueil de saisines. »[51].

(3) *Gestion sécurisée de dossiers et de procédures*, qui exploite l'échantillon pour identifier l'abonné et alimenter le « fichier des contrevenants potentiels ».

31. Les difficultés d'identification. Trois dispositifs techniques rendent l'identification des contrefacteurs difficile[52] : l'existence d'adresse IP dynamiques (i), la possible utilisation de *proxys* (ii), et la translation (iii).

N. Mallet-Poujol, « Big Brother et Anastasie au chevet du droit d'auteur : réflexions su le projet de loi « Création et Internet », Légicom 2009/4, 42, p.85.

50 CCTP, p. 10

51 CCTP, p. 15

52 A noter également que certaines solutions, régulièrement présentées comme parade par des internautes, sont en réalité totalement inefficaces, en particulier les réseaux pair-à-pair anonymisés et/ou sécurisés (les plus connus étant FreeNet, <http://freenetproject.org/> et StealthNet, <http://www.stealthnet.de>). Ces réseaux utilisent les mêmes liens que les réseaux pair-à-pair classiques. En revanche, les réseaux pair-à-pair sécurisés cryptent les communication d'un pair à l'autre, de telle façon qu'aucune détection ne puissent être effectuée sur la ligne de communication (par exemple au niveau du FAI). Dans le cadre de surveillants utilisant un client de pair-à-pair, sécuriser la communication est inutile : le pair-espion pourra décrypter les communications avec le pair contrefacteur, qui sera donc détecté. Les réseaux anonymisés utilisent des techniques de routage pour que les communications passent par plusieurs pairs choisis aléatoirement entre le pair qui met à disposition et celui qui télécharge. Il est donc impossible de savoir quel est le destinataire final des contenus partagés. Mais ce détail importe peu puisque la petite loi ne sanctionne pas la contrefaçon, mais le manquement à l'obligation de

i.- IP dynamiques

32. Présentation. La première est que certains fournisseurs d'accès fournissent par défaut une adresse IP dynamique à ses abonnés : l'adresse IP peut être changée par le simple redémarrage de leur « *box* ». Or, la phase d'échantillonnage est clairement un classement des adresses IP en fonction des « chances de correspondre à des réitérations » : en clair un classement des adresses IP en fonction du nombre de saisines les concernant sur les « 7 derniers jours » . Ce classement ne peut se faire en fonction de l'identité civile de l'internaute puisque celle-ci est récupérée après la phase d'échantillonnage (probablement en raison de son coût financier). C'est au moment de cette « identification des titulaires de plage d'adresse IP »[53] que l'Hadopi saura si l'adresse IP relevée est statique ou dynamique. Dans ce dernier cas, la pertinence du classement devra être remise en cause. Reste à savoir quelle sera l'attitude de l'Hadopi : abandonner les poursuites ou bien sanctionner l'internaute sans considération avec le classement. Ceux qui disposent d'une IP dynamique seraient alors respectivement favorisés ou défavorisés face au dispositif de détection.

33. Une rupture d'égalité devant la loi pénale. Il s'agit, une nouvelle fois, d'une atteinte au principe d'égalité devant la loi pénale : l'abonné à un opérateur fournissant une IP statique est détectable, tandis que celui à qui est attribuée dynamiquement une IP n'a aucune chance d'être détecté, puisque, précisément, son adresse change quotidiennement. Car il est vraisemblable que l'Hadopi choisisse de ne pas rechercher la sanction pour une adresse IP ne remplissant pas le critère de répétition de l'infraction qu'elle s'est fixé. Dans le cas contraire où l'Hadopi choisit de poursuivre malgré une adresse dynamique, on se trouverait dans l'hypothèse d'une rupture d'égalité face à la procédure spécifique à l'Hadopi : l'adresse IP dynamique serait systématiquement sanctionnée en dépit des autres critères. Même s'il est possible qu'à l'avenir, le choix de l'opérateur sera fait par l'internaute adepte du pair-à-pair en fonction de ce paramètre, il faut bien considérer que cet état de fait lui est totalement extérieur. Cette situation conduit à douter sérieusement de la constitutionnalité du mécanisme, la rupture d'égalité devant la loi étant ici flagrante.

---

vigilance. Les internautes usants de tels services s'exposeraient donc à une sanction, y compris sans avoir eux-mêmes téléchargé.

53 CCTP, p. 16

ii.- L'utilisation de proxy

34. Une hypothèse non appréhendée. Le proxy est un « dispositif informatique associé à un serveur et réalisant, pour des applications autorisées, des fonctions de médiation, telle que le stockage des documents les plus fréquemment demandés ou l'établissement de passerelles. »[54] Un proxy est une machine relayant les communications d'autres machines clientes. Toutes les communications sont alors perçues comme provenant du proxy, et non des clientes, qui sont ainsi masquées. La détection des faits commis sur les machines clientes renverra donc l'IP du proxy, qui peut être situé à l'étranger et donc hors de la compétence de la haute autorité. Deux catégories de proxys existent : les proxys serveurs, souvent payants et qui seront amenés à se développer en cas de contrôles accrus de l'Internet ; et les proxys collaboratifs, basés sur des logiciels installés sur les machines des internautes et qui permettent de brouiller complètement les communications, rendant toute détection difficile au prix d'une baisse des performances. De plus, l'exploitation des trous de sécurité régulièrement découverts dans les systèmes d'exploitation permettent d'installer des proxys sur des machines à l'insu de leur propriétaire.

Selon le CCTP, aucune décision n'a encore été prise dans ce cas, puisque « les adresses IP ne correspondant pas à un FAI ou une entreprise […] devront être conservées de manière à prendre des mesures si ce nombre d'adresses IP croît trop rapidement. »[55]. Il reste douteux que, dans cette hypothèse, l'Hadopi soit efficace, s'agissant de proxys dont l'adresse IP sera située à l'étranger.

iii.- Translation

35. Une difficulté contournée par la loi. La troisième technique rendant la détection difficile, appelée translation d'adresse[56], permet à plusieurs machine de partager une même

54 Comm. gén. term., JO 16 mars 1999, *in* Lamy Droit de l'Informatique et des Réseaux 2009 - Lexique relatif au vocabulaire informatique et à la terminologie des télécommunications et du réseau internet, v° « Serveur mandataire ».

55 CCTP, p. 15.

56 Le NAT, « Network Adress Translation » ou « translation », permet à plusieurs machines possédant des adresses IP différentes, mais privées et donc inappropriées à Internet, de partager une unique adresse IP publique, donc utilisable sur Internet. Ce mécanisme sert à palier au nombre trop restreint d'adresses IP publiques prévu dans le protocole Ipv4 sur lequel est basé Internet. Il est aujourd'hui utilisé dans toutes les « adsl-box » afin que l' abonné puisse connecter plusieurs machines, tout en ne lui fournissant qu'une adresse IP publique, dont l'acquisition coûte cher (puisque pratiquement toutes les adresses publiques Ipv4 sont aujourd'hui réservées).

adresse IP publique (celle utilisée sur Internet et donc visible par les surveillants). C'est le cas par exemple au domicile des internautes, lorsque plusieurs machines sont connectées à une même « *adsl-box* » (ou « *box* ») : vues de l'extérieur, toutes les communications sont perçues comme à destination de la même « box ». Il est donc impossible de connaître l'identité du contrefacteur au sein du foyer. De plus, le « piratage » (c'est-à-dire lorsque la métaphore fonctionne : au sens de la loi Godfrain d' « atteintes aux systèmes de traitement automatisé de données »[57]) de l'accès sans fil de cette « *box* » permet d'usurper l'adresse IP de son propriétaire. C'est une des raisons d'être de l'obligation de surveillance de l'accès, permettant de ne pas rechercher plus avant qui est auteur des faits : l'abonné sera tenu pour responsable[58].

36. L'identification des internautes sur les réseaux pair-à-pair n'est donc pas chose aisée, que ceux-ci usent volontairement de techniques propres à les rendre indécelables ou que cela résulte de l'architecture technique sur laquelle ils n'ont aucune emprise.

b.- La fausse détection

37. **Faux-positifs.** Une critique fréquente à l'encontre de l'Hadopi concerne les « détections en faux-positif » (Un faux positif est un résultat à un test déclaré positif à tort, là où il est en réalité négatif), c'est-à-dire la sanction, au terme de la procédure de riposte graduée, d'internautes n'ayant jamais téléchargé d'œuvres sans autorisation. Outre le problème de l'échantillonnage « en aveugle » d'adresses IP dynamiques, qui risquent de sanctionner lourdement des contrefacteurs occasionnels (contrairement au but affiché de se concentrer sur les « téléchargeurs » les plus actifs), le fournisseur d'accès peut potentiellement fournir une identification erronée du titulaire de l'abonnement, par exemple en fournissant l'identité civile du titulaire de l'adresse IP quelques minutes avant ou après son changement dynamique : les problèmes d'horodatages sont récurrents en informatique[59], par exemple à cause des horaires d'été ou de l'utilisation des heures GMT ou locales.

---

57 Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, Journal officiel du 6 janvier 1988.

58 Dans le cadre d'une entreprise, le problème devient critique puisque plusieurs dizaines, voire centaines de machines peuvent partager la même adresse IP publique. Or comme la sanction de coupure de l'accès Internet a été jugée disproportionnée pour les entreprises, elle sont dispensées de cette sanction et deviennent de fait un lieu de prédilection pour l'installation de proxys « pirates ».

59 Marinescu, C. et Tapus. « A survey of the problems of time-stamping or why it is necessary to have another time-stamping scheme », *in* Proceedings of the 25th Conference on IASTED international Multi-Conference: Software Engineering (Innsbruck, Austria, February 13 - 15, 2007). W. Hasselbring, Ed. ACTA Press, Anaheim, CA, 341-346.

Par ailleurs, une riposte est envisageable de la part des contrefacteurs : pour des raisons de performances, les recherches et déclarations de mise à disposition (v. *supra* n°25) sur les réseaux pair-à-pair sont relayées par plusieurs pairs entre l'émetteur initial de la requête et ceux proposant le contenu. Ce mécanisme de relai des recherches n'est soumis à aucun contrôle. Ainsi, des pairs peuvent aisément jeter le doute sur la pertinence des sanctions prononcées par l'Hadopi : en déclarant que des requêtes concernant des contenus protégés ont été émises par certains pairs choisis aléatoirement, ces derniers sont susceptibles de faire à tort l'objet de saisines. Plus généralement, toutes technique d'usurpation d'adresse IP[60] peut être utilisée pour faire accuser à tort le titulaire l'adresse IP usurpée, quelle que soit la méthode de contrefaçon. Les surveillants peuvent néanmoins écarter les internautes victimes de requêtes falsifiées en initiant effectivement le téléchargement avec le demandeur supposé afin de s'assurer de son authenticité. En conséquence, seuls les téléchargements effectifs font office de preuve solide de tentative de contrefaçon. Outre que les surveillants sont donc eux-même obligés de se livrer à de l'« *upload* », et donc à de la contrefaçon, cela limite énormément le champ de détection : alors que les actes de recherche et déclaration de mise à disposition sont transmises au plus grand nombre de pairs (au moins plusieurs dizaines de milliers), permettant donc au surveillant de collecter une grand nombre d'adresses IP, le téléchargement en soit fait rarement intervenir plus d'une dizaine de pairs et s'avère donc beaucoup moins efficace en terme de nombre de détections.

38. Une présomption de culpabilité... irréfragable ? La détection erronée par l'Hadopi est particulièrement grave, puisque la loi instaure une présomption de culpabilité à l'égard du titulaire d'accès. Bien plus, il est difficile d'imaginer comment il sera possible pour un abonné de prouver son innocence lorsqu'il aura été détecté à tort : adresser à l'Hadopi son disque dur, comme cela a été affirmé pendant les débats à l'Assemblée Nationale, nous paraît d'une valeur probatoire nulle puisqu'il n'est pas possible d'établir que le disque en question était bien connecté à un ordinateur lui-même connecté à l'accès en cause... Et nombreuses sont les personnes à disposer de plusieurs ordinateurs à leur domicile. En outre, il est difficile d'imaginer quels seraient les éléments, sur ce disque dur, qui permettraient de prouver avec certitude

60 L'usurpation d'adresse IP (en anglais : IP spoofing ou IP address spoofing) est une technique de hacking malveillante consistant à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribué à l'ordinateur qui les émet. Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auquel il a accès. < http://fr.wikipedia.org/wiki/Usurpation_d%27adresse_IP >

l'absence de téléchargement non autorisé d'œuvres protégées. La preuve est doublement diabolique : à la fois négative, et d'une technicité particulière. En ce sens, il faut considérer que la procédure intentée par l'Hadopi instaure une présomption irréfragable de culpabilité à destination de l'abonné.

A suivre cette analyse, il faut à nouveau s'inquiéter de la constitutionnalité de la petite loi : le Conseil constitutionnel a en effet jugé, en se fondant sur l'article 9 de la déclaration des droits de l'homme et du citoyen, « qu'en principe le législateur ne saurait instituer de présomption de culpabilité en matière répressive ; que, toutefois, à titre exceptionnel, de telles présomptions peuvent être établies, notamment en matière contraventionnelle, dès lors qu'elles ne revêtent pas de caractère irréfragable, qu'est assuré le respect des droits de la défense et que les faits induisent raisonnablement la vraisemblance de l'imputabilité »[61]. Malgré ces forts soupçons d'inconstitutionnalité quant à la détection et à la sanction de la contrefaçon sur les réseaux pair-à-pair, la sanction porte, formellement au moins, sur l'obligation de surveillance de son accès par l'abonné : à ce jeu de bonneteau des qualifications juridiques, il est probable que ce soit le bonneteur qui gagne.

II.- L'obligation de surveillance de son accès par l'abonné

39. De la surveillance à la sécurisation. L'obligation faite à la « personne titulaire de l'accès à des services de communication au public en ligne » est définie en ces termes par le nouvel article L. 336-3[62] : « obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de » contrefaçon[63]. Cela se traduit par l'obligation de mettre en place un « moyen de sécurisation », qui peut lui être enjointe à titre de sanction (art. L. 331-25, 2°), ou lors de la transaction préalable à la procédure de sanction (art. L.331-26, 2°). Bien *qu'a priori* les moyens de la surveillance de l'accès ne sont pas imposés (les parents peuvent toujours épier l'écran de leurs enfants lorsqu'ils naviguent sur Internet), c'est principalement une obligation de

61 Décision 99-411 DC du 16 juin 1999. Il faut préciser que ces exigences « ne concernent pas seulement les peines prononcées par les juridictions répressives mais s'étendent à toute sanction ayant le caractère d'une punition même si le législateur a laissé le soin de la prononcer à une autorité de nature non juridictionnelle » (Décision n°913, août 1993).

62 Cet article est une reprise de l'article L. 335-12 issu de la loi du 1er août 2006, mais l'obligation est, cette fois, assortie d'une sanction.

63 « reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise. »

sécurisation de l'accès qui résulte de la surveillance de son accès par l'abonné.

La sécurité informatique est un domaine qui présente ses contraintes propres qu'il convient de cerner pour évaluer la teneur de l'obligation de sécurisation (A) avant de rechercher ce que représente le « moyen de sécurisation » imposé par la petite loi (B).

A.- Sécurisation de l'accès

40. Des notions introuvables pour l'utilisateur. Il peut paraître étonnant, pour l'utilisateur averti, de se trouver dans l'obligation de sécuriser son accès Internet, ou tout du moins de surveiller son utilisation. En effet, la sécurité informatique est une problématique tout à la fois vaste en thématiques[64] et très pointue au point de vue technique. Il est connu que la « sécurité absolue » est illusoire, elle est plutôt affaire de mise en œuvre personnelle soumise à de nombreux compromis, ce qui la rend particulièrement inappropriée à faire l'objet de « spécifications fonctionnelles pertinentes ». Outre ces questions d'ordre général, la mise en œuvre pratique de la sécurité dans le cadre de l'Hadopi implique en premier lieu d'identifier la machine devant exécuter le « moyen de sécurisation ». Or cette question ne peut être tranchée de façon optimale, ce qui jette un discrédit supplémentaire sur la pertinence du « moyen de sécurisation » dans sa double mission de limiter la contrefaçon et de permettre à l'internaute de prouver son innocence dans le cadre de la riposte graduée. De plus, les difficultés juridiques quant à la détermination de la licéité de tel ou tel acte (*supra* n°27) sont désormais à la charge de l'internaute, ce qui est bien délicat s'agissant de questions sur lesquelles les spécialistes n'arrivent pas à s'accorder[65]. En réalité, l'imprécision de l'obligation tient également aux moyens à mettre en œuvre : dans le domaine informatique, la sécurité est affaire de spécialiste. La teneur de l'obligation de sécurisation de l'accès est ainsi extrêmement floue, tant il est délicat de déterminer ce que signifie la « sécurisation » (1) de l' « accès » (2).

64 Le terme « sécurité informatique » regroupe en réalité de nombreuses thématiques qui diffèrent par leur contexte (sécurité des systèmes d'information, sécurité des communications, sécurité des applications...) et leur objet (chiffrement, authentification, identification, contrôle d'intégrité...) et peut être aussi bien extrêmement théorique que pratique.

65 V. en particulier : A. Singh, « Loi "Création et Internet" : une obligation "floue" à la charge de l'internaute ? », Dalloz 2009, p.306 (« Il est évident que cette obligation de surveillance n'a de sens et n'est intelligible que si l'internaute sait quels actes sont en effet soumis à l'autorisation des ayants droit. Or, la réponse à cette question demeurant parfois incertaine même pour les spécialistes, il nous semble illégitime de la part du législateur de demander aux internautes de faire mieux. »).

1.- Notion de sécurisation

41. Illusion et contraintes de la sécurité. La labellisation par l'Hadopi de « moyens de sécurisation » censés prévenir un point d'accès de toute utilisation à des fins de contrefaçon, tout en permettant à l'abonné de se disculper en cas de prise dans la riposte graduée implique une assertion forte : la possibilité d'une sécurisation absolue, durable et valable pour tout un chacun. Or cette assertion se heurte à deux cruelles réalités : l'impossibilité d'une sécurisation absolue et durable, illustrée par la sécurisation de l'accès sans-fil face aux évolutions techniques (a) et l'inexistence d'une sécurité absolue valable pour tout un chacun, illustrée par le filtrage des communications qui implique un paramétrage personnel et un problème sensible de compétences (b).

a.- Sécurisation de l'accès sans fil et évolution technique

42. Protection de l'accès sans-fil. « L'obligation de surveillance pour un titulaire d'abonnement » implique en priorité pour l'abonné de se prémunir contre l'utilisation de son accès Internet par un tiers *via* une connexion sans fil. À l'heure actuelle, les opérateurs proposent en général deux algorithmes : le WEP (*Wired Equivalent Privacy*)66, le WPA-PSK (*Wi-Fi Protected Access - Pre-Shared Key*)[67]. Le WEP est surnommé par les spécialistes « *Weak Encryption Protocol »* (« Protocole de Cryptage Faible ») à cause de ses faiblesses[68] : il suffit de quelques minutes à quelques heures et de peu de connaissance techniques pour surmonter cette protection. Bien qu'elle soit encore à l'heure actuelle la plus utilisée, elle devrait être écarté par tout abonné consciencieux. Aujourd'hui l'internaute utilisant le WPA possède une sécurité satisfaisante, à condition que la clé de chiffrement – c'est-à-dire le mot de passe – utilisée soit d'une taille conséquente et générée de manière aléatoire.
Mais ces sécurités sont toutes relatives, en particulier en raison de l'évolution technique.

43. Évolution des capacités de calcul des machines. Une difficulté importante est engendrée par l'évolution des capacités de calcul des machines, ainsi que des technologies de « cassage » des algorithmes de sécurisation. Même si le WPA est encore relativement sûr aujourd'hui, surtout avec une clé conséquente, sa solidité diminue continuellement. En effet,

---

66 IEE Standards Association, Norme IEEE 802.11 relative aux réseaux sans fil, <http://standards.ieee.org/>, 1999-2005.

67 Amendement IEEE 802.11i de la norme IEEE 802.11, <http://standards.ieee.org/>, 2004.

68 S. R. Fluhrer, I. Mantin et A. Shamir, « Weaknesses in the Key Scheduling Algorithm of RC4 », Selected Areas in Cryptography, 2001.

ces derniers mois ont vu l'apparition de processeurs massivement parallèles[69] extrêmement performants et très bon marché[70] (quelques centaines d'euros dans n'importe quelle grande surface). Ces processeurs sont idéalement architecturés pour générer un très grand nombre de mots de passe à très grande vitesse. De plus, leur évolution étant très rapide (64 processeurs de flux[71] au premier trimestre 2008, pour 440 aujourd'hui), il est à prévoir qu'une sécurisation WPA passera bientôt par des clés très longues, impliquant une baisse des performances, pour ensuite suivre l'exemple du WEP et ne devenir qu'illusoire[72]. Une veille continue sur ce point doit donc être prévue, ainsi qu'une mise à jour régulière des spécifications et recommandations.

44. Évolution des spécifications. Jusqu'à aujourd'hui, les systèmes de sécurisation étaient mis en place par les constructeurs de matériel et de logiciel, puisqu'ils nécessitent une standardisation afin que le boîtier Internet, fourni par l'opérateur, soit compatible avec les cartes réseaux et les systèmes d'exploitation. Une évolution des ces spécifications est en conséquence un processus long et assez lourd, lieu de bataille industrielle pour imposer des standards. Des spécifications gouvernementales en surcroît nous paraissent problématique : il est à prévoir de lourdes mises à jours des boîtiers Internet, coûteuse pour les opérateurs, et de lourdes mises à jour des machines des internautes (de nombreuses cartes WIFI anciennes encore utilisées supportent uniquement le WEP et sont donc incompatibles avec le WPA). De plus, on peut aisément imaginer que les opérateurs se désengagent de cette réflexion, puisqu'aucune obligation ne leur est imposée par la loi. Tout au plus se contenteraient-ils de suivre les éventuelles recommandations de l'Hadopi : la sécurisation devient une contrainte pesant sur leurs clients, et une sécurisation de leur part sera faite *a minima*, respectant les

---

69 Ces processeurs, appelés GP-GPU (*General-Purpose Computation on Graphics Hardware*) et à l'origine dédiés au jeu vidéo, sont basés sur une architecture très performante lorsqu'il s'agit d'exécuter un très grand nombre de petits calculs (ce qui est le cas de la génération de mots de passe), contrairement aux processeurs classiques qui sont performants lorsqu'il s'agit d'exécuter un petit nombre de grands calculs. <http://gpgpu.org/>.

70 Ramené au nombre de mots de passe générés par seconde, les GP-GPU sont 30 fois moins cher que la solution autre la plus abordable (qui consiste à utiliser le processeur de la Sony *Playstation*). C. Blancher et S. Marechal, « Packin' the PMK - Of the robustness of WPA/WPA2 authentication », BA-Con, 2008, <http://ba-con.com.ar/>.

71 Un processeur de flux (« *shader processor* ») est l'unité effectuant les calcul au sein des GP-GPU. Chaque processeur de flux est capable d'effectuer un calcul indépendamment des autres. Grossièrement, 440 processeurs de flux permettent des calculs 6,9 fois plus rapides que 64.

72 Elcomsoft <http://www.elcomsoft.com/> est une société proposant un logiciel basé sur les GP-GPU permettant la « récupération de mots de passe » (présentation politiquement correcte souvent utilisée pour désigner le « cassage » des mots de passe). Des tests avec du matériel déjà ancien montrent un affaiblissement de 10 à 100 des protections WPA (Fabien B., « CUDA : Elcomsoft présente une arme de déprotection massive », <http://www.generation-nt.com/>, 17/10/2008).

recommandations de l'Hadopi, mais ne garantissant pas que le point d'accès ne soit pas utilisé pour s'adonner au téléchargement par pair-à-pair[73].

Par ailleurs la labellisation des systèmes de sécurisation par l'Hadopi pose deux problèmes majeurs pour les matériels anciens et pour les systèmes d'exploitation récents. En effet, les matériels anciens ne peuvent pas supporter les systèmes de sécurités modernes, pour des problèmes de performances et de compatibilité avec le système d'exploitation. Il s'agit, une fois encore, d'une rupture d'égalité devant la loi pénale[74], à moins de demander aux propriétaires de tels systèmes de mettre au rebut leur machine, trop ancienne pour respecter la loi[75].

b.- Filtrage des communications, paramétrage et inégalité des compétences.

45. Difficulté technique du paramétrage. Un deuxième volet de la sécurisation du point d'accès concerne le filtrage des communications : afin de se prémunir contre l'utilisation illégale de son accès par les autres internautes de son foyer, le titulaire de l'abonnement doit mettre en place un système de filtrage. Ce système, appelé pare-feu (ou *firewall* : « Dispositif informatique qui filtre les flux d'informations entre un réseau interne à un organisme et un réseau externe en vue de neutraliser les tentatives de pénétration en provenance de l'extérieur et de maîtriser les accès vers l'extérieur. »[76]) permet de bloquer les communications de certaines applications, comme par exemple les logiciels de pair-à-pair. Les pare-feux doivent être finement paramétrés afin d'autoriser les communications utiles tout en refusant les communications dangereuses ou

73 Rappelons que le pair-à-pair est, de fait, l'argument de vente historique sur lequel s'est construit le marché de l'ADSL : le développement des offres internet à haut débit s'est réalisé, pendant plusieurs années, sur fond de campagnes publicitaires au slogan quasi-unique : « téléchargez vos mp3 plus rapidement », à une époque où aucune offre officielle n'était disponible en France. Cette situation a nécessité que l'on exige des fournisseurs d'accès qu'ils s'engagent à abandonner ces pratiques, et à diffuser un message de prévention sur leurs pages d'accueil : « le piratage nuit à la création artistique » (Loi pour la confiance dans l'économie numérique, art.7).

74 V. à propos de la compatibilité des moyens de sécurisation avec les différents systèmes d'exploitation, E. De Marco, art. préc. : « La petite loi n'impose pas plus la compatibilité de ces logiciels avec l'ensemble des systèmes d'exploitation, ce qui pourrait encore conduire à une inégalité des citoyens devant la justice de l'Hadopi, selon le système d'exploitation que ces derniers utilisent. »

75 À l'opposé, les systèmes d'exploitation récents, lorsqu'il intègrent de nombreuses évolutions technologiques (tel que MS Windows Seven, actuellement en test ouvert, c'est à dire disponible pour tous sur simple demande), peuvent rester démunis de système de sécurité pendant plusieurs mois, en particulier pendant la période de test : pendant ces périodes tout individu (généralement informaticien ou utilisateur averti) peut installer gratuitement le système d'exploitation pour le tester et aider à sa stabilisation. Durant cette période, tout testeur se mettrait potentiellement hors la loi, ayant pour effet indésirable de limiter ce type d'initiative en France, et par conséquent de réduire la qualité des systèmes d'exploitation.

76 Comm. gén. term. JO 16 mars 1999 in Lamy Droit de l'Informatique et des Réseaux 2009 - Lexique relatif au vocabulaire informatique et à la terminologie des télécommunications et du réseau internet, v° « Barrières de sécurité ».

illégales.

Ce paramétrage peut s'avérer très complexe. Par exemple, les jeux en ligne nécessitent de nombreux canaux de communications qui sont bloqués par défaut ; les sites *web* bancaires ou gouvernementaux (impôt, sécurité sociale) utilisent des techniques de sécurité particulières également utilisées par des sites malveillants pour attaquer les machines et par conséquent sont rejetées par défaut par la plupart des systèmes de sécurité. Sans compter que les techniques de pair-à-pair sont utilisées par de nombreux sites pour distribuer à moindre coût des contenus légaux : la décision de les bloquer n'est donc pas triviale. Dans tous ces cas, il est très difficile de différencier une utilisation légitime de l'accès Internet, d'une utilisation malveillante ou illégale, voire impossible par exemple pour le *streaming* illégal qui est techniquement indissociable du *streaming* légal.

Par ailleurs, l'inégalité des compétences informatiques au sein d'un foyer est problématique : nombreux sont les pères de famille, titulaires de l'accès internet, qui délèguent ce paramétrage à leur enfant adolescent. Plus généralement, le système de sécurité, lorsqu'il n'est pas maîtrisé, est vécu comme une contrainte par l'internaute qui ne peut pas profiter pleinement de son système informatique : il n'est pas rare qu'un pare-feu empêche, sans que l'utilisateur ne sache pourquoi, des opérations simples telles que la communication avec l'imprimante. La réaction naturelle face à ce type de situation est évidemment de désactiver le système de sécurité. En d'autres termes, la sécurité n'est pas une science exacte et impose aux citoyens une contrainte forte dans leur utilisation quotidienne de l'outil informatique. En réalité, la sécurisation repose sur un ensemble de choix éminemment personnels.

46. La sécurité, un problème personnel. Il est important de noter que la mise en œuvre de la sécurité ne peut se résumer à l'installation du « bon logiciel », encore faut-il être capable de correctement le paramétrer pour qu'il réponde aux besoins de l'utilisateur sans devenir une contrainte. La sécurité est un compromis entre risque, performance et liberté d'utilisation, tout l'art est de :

- limiter les risques les plus importants : une sécurisation à 100% est totalement illusoire, ne serait-ce que par la découverte fréquente et continue de nouvelles failles,
- tout en limitant la perte de performance : utiliser du WPA plutôt que du WEP, ou encore utiliser une clé conséquente augmente la sécurité, mais présente un coût en ralentissant

les communications, il en va de même pour l'utilisation d'un pare-feu, qui ralentit non seulement les communications, mais plus globalement la machine qui les exécute,

– et en gardant une convivialité : un système de sécurité trop strict empêchera de nombreuses utilisations.

47. Deux risques sont donc impliqués par la sécurisation systématique des tous les accès Internet, et donc par des internautes peu compétents : soit le ralentissement du développement de nouveaux services sur Internet, ces derniers étant bloqués par le système de sécurité, soit la désactivation systématique du système de sécurité par l'internaute pour retrouver une convivialité suffisante. Surtout, les options à prendre relèvent d'un choix personnel de la part de l'utilisateur relatif à son mode d'utilisation de l'outil informatique, choix qui désormais risque de lui échapper du fait de la « labellisation » des « moyens de sécurisation » par l'Hadopi. Il faut en effet rappeler que la sécurité informatique est avant tout une affaire humaine, bien plus qu'une affaire technique, comme en témoignent « Les 10 commandements de la sécurité sur l'internet » du portail gouvernemental de la sécurité informatique[77] qui concernent tous sans exception des comportements humains. Dès lors, on peut s'interroger sur la « pertinence » de « spécifications fonctionnelles » d'un « moyen de sécurisation » purement technique.
Si la teneur de l' obligation de sécurisation de l'accès est indécise quant à l'impossibilité d'une sécurisation absolue, elle l'est aussi en raison des incertitudes de la notion d'accès.

2.- Notion d'accès

48. Lieu d'exécution du système de sécurité. Une question très importante concerne la machine exécutant la sécurisation. En effet, ces logiciels pourront être exécutés soit sur la « *box* » Internet, soit sur les machines des internautes. Plusieurs machines sont nécessaires à un accès Internet : le point d'accès, ou « *box* » Internet, et la machine de l'internaute, dite cliente.

49. Difficile sécurisation de la « *box* ». Dans ce cas, la sécurisation est exécutée sur le point d'accès, c'est-à-dire directement sur le nœud principal des communications. L'avantage de cette

77 SGDN, DCSSI, « Les 10 commandements de la sécurité sur l'internet » <http://www.securite-informatique.gouv.fr/gp_rubrique34.html>, 2009. Ces « dix commandements » sont : « Utiliser des mots de passe de qualité » ; « Avoir un système d'exploitation et des logiciels à jour : navigateur, antivirus, bureautique, pare-feu personnel, etc. » ; « Effectuer des sauvegardes régulières » ; « Désactiver par défaut les composants ActiveX et JavaScript » ; « Ne pas cliquer trop vite sur des liens » ; « Ne jamais utiliser un compte administrateur pour naviguer » ; « Contrôler la diffusion d'informations personnelles » ; « Ne jamais relayer des canulars » ; « Soyez prudent : l'internet est une rue peuplée d'inconnus ! » ; « Soyez vigilant avant d'ouvrir des pièces jointes à un courriel : elles colportent souvent des codes malveillants ».

approche est qu'il représente une meilleure sécurité et qu'il concentre tout le paramétrage en un seul endroit : il n'est pas alors obligatoire d'installer tout l'équipement de sécurité sur chacune des machines du domicile, qui peuvent parfois être assez nombreuses, ou encore comporter plusieurs systèmes d'exploitation (par exemple Windows et Linux) devant chacun être paramétré. Une première difficulté est, à nouveau, la compétence technique nécessaire : la plupart des internautes ne savent pas accéder à ces « boxes » (Car on peut parfaitement se contenter d'y brancher sa machine pour que cela fonctionne sans autre sorte d'intervention). Une seconde difficulté concerne les performances : si un pare-feu est déjà présent dans ces « *boxes* », il n'est pas conçu pour filtrer les actes du téléchargement illégal. L'exécution d'un système de sécurisation peut s'avérer trop lourd car les « *boxes* » sont de faible puissance. Il faudrait alors envisager un remplacement des ces « *boxes* » par des machines plus puissantes, ce qui représente un coût qui n'est pas à envisager.

Enfin, un problème important est que la « *box* » ne peut que surveiller les communications à leur plus bas niveau : impossible par exemple de savoir quelle est l'application utilisée par la machine de l'internaute, qui peut très bien être un logiciel de pair-à-pair sans que la « *box* » ne puisse le savoir. Difficile également de connaître à ce niveau la teneur des informations pour faire la différence entre un contenu légal et illégal. En conclusion, l'exécution sur la «box» Internet serait non seulement difficile et coûteux à mettre en œuvre, mais également incomplet au niveau protection. Pourtant, c'est à ce niveau de communication que la petite loi se réfère en mentionnant l' « *accès* » aux réseaux ; il semble néanmoins que dans l'esprit des rédacteurs du projet, ce soient les machines connectées à cet accès qui doivent être sécurisées.

50. Impossible sécurisation ? L'exécution de la sécurisation sur la machine client est beaucoup plus facile à recommander, puisque cette machine est administrée par l'internaute : l'opérateur peut alors se contenter de proposer, contre rémunération, des logiciels existants sans avoir à mettre à jour leur « *box* ». Si l'Hadopi suit cette voie, il faut noter que les Internautes seront tenu de sécuriser leur machine cliente afin d'assurer la sécurité de leur point d'accès. Or la machine principale du point d'accès est la « *box* », sécuriser la machine client ne semble donc pas très productif d'un point de vue purement technique. En réalité, une sécurisation de l'accès Internet satisfaisante implique une intervention sur toutes les machines impliquées, et donc un travail conséquent assorti d'importantes connaissances techniques.

Compte tenu de ces difficultés, la mission de sensibilisation au respect des droits de propriété intellectuelle sur les réseaux devrait se doubler en toute logique d'une sensibilisation aux

questions de sécurité informatiques. Mais la solution la plus simple consiste à proposer aux abonnés à Internet un « moyen de sécurisation » labellisé par la Haute autorité.

B.- Le « moyen de sécurisation »

51. Présentation. L'identification de ce que peut être ce « moyen de sécurisation » doit se réaliser par la publication de « spécifications fonctionnelles pertinentes », déterminées « après consultation des concepteurs de moyens de sécurisation » (nouvel art. L. 331-30, al. 1er). En fonction de ces spécifications sera établie par l'Hadopi « une liste labellisant les moyens de sécurisation dont la mise en œuvre exonère valablement le titulaire de l'accès de sa responsabilité au titre de l'article L. 336-3 » (al. 2), la procédure d'évaluation et de labellisation devant être précisée par un décret en Conseil d'Etat (al. 3).

Précisons que les spécifications que nous allons présenter concernent essentiellement les points d'accès domestiques : il semble très difficile d'établir des spécifications fonctionnelles pour les accès Internet d'entreprise. En effet, ces derniers sont beaucoup plus complexes, en particulier car ils concernent bien souvent beaucoup plus de machines, dont de certaines nomades (ordinateurs ou téléphones portables, PDA, etc.), appartenant éventuellement à des visiteurs temporaires, et ayant parfois des utilisations très particulières engendrant des besoins spécifiques. En raison des contraintes précédemment évoquées, de telles sécurisations ne peuvent se faire qu'au cas par cas, et font l'objet de contrats avec des entreprises spécialisées, qui devront sans doute se conformer à l' « état de l'art » tel que fixé par l'Hadopi.

Les difficultés de détermination des « spécifications fonctionnelles pertinentes » tiennent naturellement aux impératifs et aux aléas de la sécurité informatique. Du point de vue du « moyen de sécurisation » proprement dit, celui-ci prendra la forme d'un logiciel espion, qui peut voir sa fonction détournée (1) mais aussi constituer lui-même une faille de sécurité (2).

1.- Le logiciel espion et son possible détournement

52. Les « spécifications fonctionnelles pertinentes » de l'espion. Comme on l'a vu, les protections informatiques, même parfaitement maîtrisées et mise en place, ne protègent pas totalement contre un détournement de l'accès Internet. Et un accès, même non compromis, peut voir son adresse IP détectée à tort pour un acte de mise à disposition (*supra*, n°37). C'est pourquoi il a été proposé la mise en place d'un espion logiciel reportant à l'opérateur les

utilisations faites des machines connectées[78], ce dernier pouvant alors prouver qu'au moment de la détection, aucun téléchargement n'a été commis sur la machine de l'internaute accusé. Il s'agira d'un logiciel permettant de surveiller tous les logiciels exécuté sur sa machine hôte, ainsi que toutes les communications dans lesquelles elle est impliquée, capable de reporter en temps réel et de manière sécurisée ces informations au FAI et munis d'un contrôle d'intégrité, afin de prévenir toute manipulation des informations ou du logiciel espion en soi.

53. Détournement domestique. Cette approche présente une faiblesse d'autant plus importante qu'elle est à la portée de tout un chacun : le contrefacteur peut installer l'espion sur une machine « propre », tout en téléchargeant illégalement depuis une autre. Détecté par l'Hadopi, le contrefacteur pourra alors se dédouaner en prouvant que le logiciel estampillé « Hadopi » était installé sur son poste informatique, en demandant à son opérateur de fournir les journaux de sa connexion. En réalité, il n'est même pas obligatoire de disposer de deux machines, il suffit d'installer une machine virtuelle, qui simule une machine dans la machine. L'espion est installé dans cette machine virtuelle ne verra que les communications de celle-ci, et pas celle de la machine physique, pouvant alors servir à la contrefaçon. La technique est très commune, et l'on sait par exemple que la prochaine version de *MS Windows*, *Windows Seven*, est équipée de série avec une machine virtuelle.

54. Sécurisation de la sécurité. Un aspect important à noter, est que, pour assurer l'efficacité du mécanisme, d'importants efforts devront être fournis pour sécuriser le système de sécurisation : il est tout à fait envisageable que des contrefacteurs facétieux diffusent des équivalents des moyens de sécurisation recommandés, répondant aux mêmes spécifications à l'exception qu'ils ne bloqueront pas le piratages et ne reporteront rien d'illégal au FAI. Le contrefacteur pourra alors justifier de la sécurisation de son accès Internet, son FAI pourra

78 Révélé sous l'appellation « mouchard filtrant » dans le communiqué de presse de l'APRIL « L'Hadopi filtrera aussi le Logiciel Libre. L'April condamne. » (<http://www.april.org>, 5 mars 2009), basé sur le rapport N° IV-3.3-2008 du CGTI (Conseil Général des Technologies de l'information, décembre 2008) révélé par « Les Echos » <http://www.lesechos.fr/medias/2009/0304/300333937.pdf>. Cet espion a deux missions : (1) filtrer les communications pour prévenir toute contrefaçon et (2) permettre au FAI d'attester de la bonne foi de l'abonné, ce qui implique nécessairement de lui reporter diverses informations sur les agissements de l'abonné (tentatives de contrefaçon ou désactivation du « moyen de sécurisation »). Fait confirmé par Olivier Henrard, responsable de l'élaboration du projet de loi Création et Internet, lors d'un débat avec Jérémie Zimmermann, de la Quadrature du Net, organisé par 01net (« Des logiciels pour prouver que sa ligne est protégée ? » <http://www.01net.com>) : « Vous venez de démontrer que pour que l'on ait une quelconque façon de prouver sa bonne foi (…) le seul moyen est que ce soit des logiciels fermés qui renvoient des informations à leur fabricant. ».

témoigner que rien n'a été reporté par l'espion qui était bien actif au moment de la détection, et l'Hadopi ne pourra que conclure à une détection en faux-positif. Dès lors, l'intégrité du système de sécurisation doit faire lui-même l'objet d'une sécurisation et d'un contrôle d'intégrité, ce qui paraît difficile à mettre en œuvre et tend à rentrer dans une spirale « sécurisation de la sécurisation de la sécurisation »...

2.- Le « moyen de sécurisation » : une faille de sécurité ?

55. Un moyen de « désécurisation » ? Enfin, il faut insister le problème majeur induit par la recommandation d'une courte liste de logiciels de sécurisation, utilisés en conséquence par un très grand nombre d'internautes. On sait que ce sont les logiciels les plus communément utilisés qui deviennent inévitablement la cible privilégiée des attaquants. Car l'internaute malveillant, exploitant un des inévitables trous de sécurité qui sera découvert dans ces logiciels, aura à sa disposition des millions de cibles potentielles. Or les systèmes de sécurité sont exécutés avec des droits privilégiés, et leur détournement permet donc d'accéder en profondeur à leur machine d'exécution[79], pour par exemple voler des données comme les mots de passe qui servent à sécuriser l'accès Internet, installer des logiciels permettant de voler les données bancaires[80], ou asservir la machine pour contrefaire des contenus ou monter des attaques de grande envergure[81]. Plus dangereux encore serait le piratage de l'espion, qui permettrait non seulement d'accéder à de nombreuses informations personnelles sur l'utilisation des machines, mais également sur les logiciels exécutés et donc sur les attaques possibles à mener sur la machine. Le détournement des logiciels de sécurisation peut également être utilisé pour déclencher des détections par l'Hadopi, tout en en altérant l'espion pour qu'ils reportent des utilisations illégales.

Dans ces situations, qui ne sont pas selon nous des hypothèses d'école, l'internaute n'ayant pourtant rien à se reprocher n'aurait alors aucun moyen de se défendre : de la présomption irréfragable de culpabilité en action... Finalement, la sécurité n'étant jamais absolue sur les

---

79 Exemple découvert dans le pare-feu de MS Windows Vista : Symantec Advanced Threat Research, « Security Implications of Microsoft Windows Vista », 2007

80 Récent exemple de telles pratiques, par la chaîne de magasins américaine Sears : « Sears Settles FTC Charges Regarding Tracking Software », Federal Trade Commission, 2009, <http://www.ftc.gov/>.

81 V. un rapport alarmant sur l'augmentation exponentielle de ce type d'attaque : « Infrastructure Security Report », Arbor Network, 2008.

réseaux, il est inévitable que les moyens préconisés par l'Hadopi révèlent des failles. La faiblesse du mécanisme en son entier, qu'il ne nous paraît pas abusif de qualifier de « bricolage dangereux »[82], tient donc aux nombreuses carences dans la mise en œuvre de la riposte graduée qui, en plus d'être ineffective et inefficace, ne garantit ni l'égalité ni les droits de la défense des citoyens[83] devant la procédure mise en place.

82 M. Vivant et J.-M. Bruguière, Droit d'auteur, *op. cit.*, n°12 (l'expression traduisant la position de M. Vivant).

83 E. De Marco, art. préc., spéc. pp.9 et s. ; A. Gitton, art. préc., spéc. n°30 et s.