Le contrôle de la connexion Internet par l'utilisateur
La légitimité des atteintes portées par les lois HADOPI et LOPPSI 2

Par Fabien Pinard

Juriste diplômé du Master II professionnel de Droit des Nouvelles Technologies de l'Information et de la Communication de l'Université de Versailles Saint-Quentin (promotion 2010/2011)

e-mail : fab.pinard@gmail.com

Introduction

En très peu de temps, le cyberespace a connu une évolution extrêmement importante le conduisant comme un lieu désormais incontournable à l'échelle mondiale tant pour les particuliers que les professionnels. Le droit s'est attaché depuis plusieurs années à s'adapter à cet univers nouveau, libéré de toute frontière, enclin à de nouveaux usages, de nouvelles pratiques… S'il y est aujourd'hui relativement bien parvenu, de nombreuses problématiques demeurent. L'utilisateur est au cœur de ce bouleversement et le droit tend à se recentrer sur lui. Avec l'apparition du « *web 2.0* », il fait désormais partie des acteurs de ce changement. On appelle « *web 2.0* » l'évolution d'Internet qui a permis une *plus grande simplicité ne nécessitant pas de connaissances techniques pour y participer*[1]. Par conséquent, Internet est devenu un lieu bien plus attractif, participatif et interactif puisque tout internaute a la possibilité d'agir sur la diffusion des contenus proposés, d'en permettre l'échange et d'être ainsi à la fois l'émetteur de la communication et le récepteur de l'information.

Or le développement de cet espace dynamique a permis une multiplication exponentielle des échanges de contenus protégés. Les procès se sont multipliés à l'égard des utilisateurs[2] et des éditeurs de logiciels[3] permettant ces échanges. Ce contexte tumultueux a fait naître le besoin de recadrer les choses en protégeant les intérêts des bénéficiaires du droit d'auteur tout en assurant une sécurité juridique à l'égard des utilisateurs impliquées dans des affaires de téléchargements illicites.

La loi dite « *HADOPI 1* », intitulée *Création et Internet* du 12 juin 2009, a institué l'obligation pour le titulaire de l'accès à Internet de surveiller sa ligne afin qu'elle ne soit pas l'objet d'usages contrefaisants. Elle crée ainsi un dispositif autonome des régimes de responsabilité existants. C'est un mécanisme dit de « *désincitation* »[4] visant à prévenir dans le cadre d'une procédure de « *riposte graduée* » ce même titulaire que sa ligne laisse transiter des contenus sans autorisation des ayants-droit. Nous le décrirons dans le cadre de ce mémoire mais il est possible de noter dès à présent que le législateur vient véritablement obliger l'abonné à avoir un parfait contrôle de sa ligne Internet. L'une des sanctions mises en œuvre se caractérise par la suspension de ladite ligne. Nous nous situons dans un cadre de lutte contre les téléchargements illicites centrés notamment sur le phénomène de « *peer to peer* ». Il s'agit d'un modèle de réseau informatique permettant un échange de fichiers de « *pair à pair* », c'est-à-dire d'un utilisateur à un autre. Ces dispositions ont donc été adoptées afin de protéger le droit d'auteur. Cependant il faut préciser qu'il ne sera pas question de traiter des interrogations liées au débat sur la contrefaçon. Nous ne parlerons de cet aspect que par incidence au sujet qui nous intéresse.

Avant toute chose, il est fondamental de définir l'utilisateur puisqu'il est le protagoniste que nous suivrons tout au long de notre démonstration. Aujourd'hui, ce terme recouvre de multiples facettes: particulier, entreprise, collectivité territoriale, université, bibliothèque, etc. Noyé dans cette diversité, il est sans nul doute nécessaire de prendre garde de toujours l'identifier. Nous tenterons sur ce point d'établir en quelle mesure il est impossible de réserver une application uniforme de la loi à l'ensemble des utilisateurs. En effet, au-delà des

---

[1] <http://wikipedia.org/wiki/Web_2.0>

[2] Voir par exemple TGI Paris, ord. Réf., 14 août 1996, RG n°60139/96, Ed. musicales Pouchenel a. c/Ecole centrale de Paris a., D. 1996, jur.490, note Gautier ; JCP E 1996, II, n°881, note Edelman ; Degroote, « la chanson française à l'honneur sur le net », Lamy dr. Informatique et réseaux oct. 1996 (F) ; Olivier et Barbry, « la propriété intellectuelle occupe toujours nos esprits… et nos lectures », Expertises nov. 1996, p.387 ; <http://legalis.net/spip.php?page=jurisprudence-decision&id_article=117>.
Voir également TGI Paris, ord. Réf., 5 mai 1997, Jean-Marie Queneau c/ Christian L…, L'Université Paris VIII, l'assoc. Mygale Point Org, Frédéric C…, JCP 1997, II, 22906, note Olivier ; RDPI 1997, n°80, p53 ; <www.juriscom.net/jpc/visu.php?ID=213> ; Bréban et Rojinsky, « Internet : le TGI de Paris entrouvre la porte du domicile virtuel », Les Echos 7 juillet 1997, p.69

[3] Y. Gaubiac, La responsabilité des fournisseurs de logiciels dans la diffusion illégale des œuvres et autres prestations protégées, CCE, novembre 2006, étude 34

[4] Terme utilisé à plusieurs reprises dans le rapport sur « le développement et la protection des œuvres culturelles sur les nouveaux réseaux », daté de novembre 2007, dont la mission était confiée à Denis Olivennes <http://www.culture.gouv.fr/culture/actualites/conferen/albanel/rapportolivennes231107.pdf>

professions protégées par la loi[5], il va s'avérer essentiel d'adapter le traitement des points d'accès à Internet selon des critères qu'il conviendra de mettre en lumière.

Outre ces différentes natures, l'utilisateur se scinde principalement en deux catégories distinctes. La première d'entre elles se réfère à l'abonné du service de communication électronique[6]. Celui-ci est le titulaire de l'accès à Internet et doit notamment se procurer le matériel nécessaire, se conformer aux exigences techniques relatives à sa connexion, conserver les identifiants ainsi que les mots de passe de ce même accès pour ne pas qu'il tombe entre de mauvaises mains et, le cas échéant, payer le prix de son abonnement[7]. Il est donc celui qui jouit du droit, qui possède le titre pour accéder ou permettre l'accès au réseau. Il se distingue de l'utilisateur qui, sans être titulaire de l'accès, bénéficie de la possibilité d'utiliser le service Internet, celui à qui il est permis. Concrètement, dans une famille, les parents sont les titulaires de l'accès tandis que leurs enfants ne font qu'utiliser le service. De la même manière, le chef d'entreprise va endosser le rôle de l'abonné afin que les salariés puissent se connecter au réseau.

Ainsi donc, il revient *a priori* au titulaire de l'accès d'avoir le contrôle de la connexion à Internet. Cette connexion se définie comme étant l'accès même à un service de communication électronique. Toutefois, nous ne nous intéresserons qu'au réseau Internet puisqu'il est-ici question de la maîtrise de cet accès. On entend ainsi par maîtrise le pouvoir effectif de direction et de contrôle du gardien[8].

La question se pose de savoir pourquoi établir une telle distinction. En droit, bien évidemment, la réponse attrait à la notion de responsabilité. On pourrait d'ailleurs se demander finalement pourquoi la responsabilité du fait des choses[9] ne pourrait pas s'appliquer en la matière et en revenir au droit classique des obligations. La définition ci-dessus, empruntée à Gérard Cornu, fait d'ailleurs référence à la responsabilité du fait des choses si on y ajoute le critère de l'usage[10]. En effet, le titulaire de la ligne est considéré comme le gardien de l'accès internet dont l'utilisation par un tiers cause un dommage aux ayants droit du fait de la négligence dans sa surveillance. Mais comme le remarque Julia Heinich[11], « *cette qualification semble [...] devoir être écartée puisque le titulaire ne peut s'exonérer en prouvant qu'il n'avait plus la maîtrise de la chose au moment de la réalisation du dommage, comme c'est le cas en matière de responsabilité du fait des choses* ». Elle remarque également que « *le titulaire de la ligne peut s'exonérer par la preuve de l'absence de faute de surveillance, en prouvant qu'il avait bien protégé sa ligne, exonération impossible en matière de responsabilité du fait des choses depuis l'arrêt Jand'heur*[12] *le gardien de la chose ne peut s'exonérer par la preuve de l'absence de faute de sa part* ». Par ailleurs, il est peut-être réducteur de traiter comme une simple « *chose* » l'univers d'Internet[13].

On pourrait également se demander pourquoi ne pas appliquer la responsabilité du fait d'autrui comparable à la responsabilité des parents du fait de leurs enfants mineurs [14] ? Julia Heinich y répond en affirmant que « *le*

---

[5] Voir les professions énumérées aux articles 56-1 et suivants du Code de procédure pénale ainsi que l'article 100-7 du même Code

[6] A savoir, dans notre cas, Internet. La notion de communication électronique est venue remplacer celle de « *télécommunication* » par l'intermédiaire de la Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. La communication électronique y est définie comme étant « *toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée* »

[7] On retrouve ces obligations dans tout contrat liant l'utilisateur à son fournisseur d'accès Internet

[8] Gérard Cornu, Association Henri Capitant, « Vocabulaire Juridique », 7e éd. PUF

[9] Article 1384 du Code civil : « *On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde* »

[10] Cass. Ch. Réunies, 2 Décembre 1941, Arrêt Franck, S. 1941,1, 217 (notes H. Mazeaud) : La Cour a défini la garde de la chose comme l'usage, la direction et le contrôle de celle-ci

[11] Julia Heinich, « La nouvelle obligation de surveillance de sa ligne : nouvelle responsabilité civile ? », Revue Lamy Droit de l'Immatériel 2214, n°67, janvier 2011, p75 et s.

[12] Cass. Ch. réun., 13 févr. 1930, S. 1930, 1, 121 ; D. 1930, 1, 57

[13] Ainsi lors de la détermination du rôle causal du fait de la chose dans la survenance du dommage, il faudrait considérer qu'Internet est une chose inerte et la victime devra prouver le caractère actif de cette dernière. Traditionnellement, il faut établir soit l'anormalité de la chose elle même (défaut), soit l'anormalité de son comportement ou encore de sa position. Cette vision semble mal cadrer avec l'usage d'Internet

[14] Voir not. Gleize B., article précité, spéc. N° 9 et s. et Bruguière J.-M., De la responsabilité civile du fait d'autrui découlant du projet de loi « Création et internet », article précité ; du même auteur, Loi du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, La « petite loi » qui aurait pu être grande, article précité, spéc. n° 25

parallèle pouvait être tentant entre l'obligation de surveillance de la ligne et l'obligation de surveillance qui pesait sur les parents et justifiait la mise en jeu de leur responsabilité civile en cas de faute commise par l'enfant mineur, qui était censée avoir été permise par leur négligence dans la surveillance ». Toutefois, le délit de non sécurisation instauré condamne non plus le fait de télécharger mais le fait de ne pas avoir protégé son accès internet, chose que nous analyserons plus en détail au cours de notre étude mais qui permet d'ores et déjà d'éliminer l'idée d'une éventuelle responsabilité du fait d'autrui.

Outre ces interrogations, une autre disposition législative formera l'écueil de notre étude. Il est ici question de la *loi d'orientation et de programmation pour la performance de la sécurité intérieure* du 14 mars 2011. Ces dispositions ont été prises pour lutter contre les nouvelles formes de délinquance et de cybercriminalité. On peut d'ailleurs lire dans le projet de loi du Sénat que le texte[15] « *adapte, ensuite, les moyens d'enquête aux nouvelles technologies afin d'améliorer les procédures d'investigation techniques et scientifiques* ». En pratique, ce texte couramment appelé « *LOPPSI 2* » permet à la police d'introduire un dispositif technique permettant de capter des données informatiques en liaison avec une infraction. Selon Alain Bensoussan[16], « *c'est un nouveau moyen pour lutter contre la délinquance économique, technique et informatique* ». Il s'agit donc de détourner la connexion Internet au profit de l'investigation afin de récupérer un certain nombre de preuves d'une ou plusieurs infractions.

Au premier abord, il peut sembler étrange de porter l'étude de ce mémoire sur les lois *HADOPI* d'une part, et sur la *LOPPSI 2*, d'autre part. Les lois *HADOPI* ont vocation à protéger le droit d'auteur en créant de nouvelles obligations, elles mêmes sanctionnées par une nouvelle infraction. La *LOPPSI 2* ne vise quant à elle qu'à adapter la procédure pénale aux technologies de son époque.

Cependant, toutes deux portent atteinte, à leur manière, à la maîtrise de la connexion Internet par l'utilisateur. La première disposition permet la surveillance du flux de contenus ascendant et descendant qui transite par le biais de la connexion. Le cas échéant, le défaut de vigilance est sanctionné par la suspension de ladite connexion. La seconde permet également une surveillance de la ligne mais cette fois de manière accrue puisque, nous le verrons, les enquêteurs ont la possibilité de recueillir des informations s'affichant sur l'écran même de l'utilisateur, et ce aux fins de recherche de preuves.

Pourtant, l'utilisateur est supposé avoir le contrôle de sa connexion. Il est sensé prendre garde de manière permanente à l'utilisation qui en est faite, et il semble a priori impensable pour un citoyen *lambda* que des enquêteurs viennent espionner ses moindres faits et gestes.

Il convient cependant de définir le terme de maîtrise. Il recouvre deux acceptions. En premier lieu, elle est explicitement et législativement instituée par l'obligation de vigilance que nous tenterons de définir afin de déterminer en quelle mesure la sanction de coupure de l'accès à Internet peut-être prononcée. Cette suspension d'un important moyen de communication et d'information marque la première atteinte à ladite maîtrise. En second lieu, la maîtrise est dite *simple* car sans autres obligations, et l'atteinte va être portée au droit à la vie privée puisqu'il est permis de s'octroyer la possibilité de capter des contenus par l'intermédiaire de la connexion Internet. Ce détournement s'opère comme nous l'avons annoncé, et comme nous l'étudierons, dans un cadre lui aussi législatif.

Les atteintes auxquelles nous faisons référence peuvent plus généralement être définies comme étant une action dirigée contre quelque chose ou quelqu'un par des moyens divers[17]. Afin que ces dernières ne tendent pas à avoir un résultat préjudiciable de cette action, il est primordial qu'elles répondent à des objectifs précis, dans un cadre déterminé et qu'elles comportent de véritables garanties. C'est seulement à ces différentes conditions, qu'elles pourront bénéficier d'une légitimité. Cette notion est définie comme étant la conformité d'une institution à une norme supérieure juridique ou éthique, ressentie comme fondamentale par la collectivité qui fait accepter moralement et politiquement l'autorité de cette institution[18]. Or, tout ce qui est établi par la loi, et donc, tout ce qui relève de la légalité, n'est pas nécessairement légitime. Selon

[15] <http://www.senat.fr/dossier-legislatif/pjl09-292.html>
[16] Alain Bensoussan, Avocat, lors d'une interview par mydsitv.accenture.fr « Le média qui analyse et qui décrypte l'actualité des DSI »
<http://www.youtube.com/watch?v=PEbyxDvTrhs>
[17] Gérard Cornu, Association Henri Capitant, « Vocabulaire Juridique », 7e éd. PUF
[18] Gérard Cornu, Association Henri Capitant, « Vocabulaire Juridique », 7e éd. PUF

l'encyclopédie Universalis[19], « *Il arrive qu'un gouvernement soit tenu pour illégitime simplement parce que sa constitution n'a pas obéi en tous points à une régularité formelle* ». Les deux lois qui nous intéressent mettent en jeu certains droits et libertés fondamentaux comme la liberté d'expression et le droit à la vie privée. A propos de la LOPPSI 2, Christiane Féral-Schuhl a par exemple parlé d'un « *objectif sécuritaire au détriment des libertés individuelles* »[20]. Or, l'opinion publique craint d'ores et déjà que l'on crée un climat de surveillance généralisée, la crainte de « *Big brother* »[21]. Toute légitimité serait perdue si la procédure et les garanties n'étaient pas scrupuleusement assurées et respectées. Il faut que le principe de proportionnalité au regard de l'objectif poursuivi soit vérifié, ce que le Conseil constitutionnel ne manquera pas de contrôler[22].

L'ensemble de ces aspects démontre qu'il est essentiel de respecter les objectifs tenus par les lois *HADOPI* et *LOPPSI 2*. L'utilisateur doit pouvoir conserver la maîtrise de sa connexion Internet sans risquer de se la voir supprimer ou contourner pour des raisons ou des circonstances autres que celles législativement prévues.

Il conviendra donc d'étudier précisément les atteintes envisagées, le cadre législatif dans lequel elles s'inscrivent, les risques au regard des droits et libertés fondamentaux, les garanties apportées, et les difficultés techniques et juridiques auxquelles ces dispositions se confrontent.

L'ensemble de ces considérations nous mènent à poser la problématique suivante qui sera le fil conducteur de notre étude : quelle est la légitimité des atteintes portées par le législateur français en matière de contrôle de l'utilisation de la connexion Internet par l'utilisateur ?

Il faut souligner dans cette perspective que nous ne cantonnerons pas notre problématique à un champ strictement et purement légaliste. La légitimité sera ainsi entendue de la congruence avec la réalité des faits régulés par le système de droit.

Pour y répondre, il sera nécessaire de faire un état du droit antérieur aux lois HADOPI et LOPPSI 2 pour chacun des domaines qui les intéressent afin de faire ressortir le besoin de palier à de nouvelles difficultés et de s'adapter à l'ère du numérique. C'est à partir de ce moment que nous pourrons analyser la mise en œuvre des dispositions et l'extension qu'elles opèrent afin d'en analyser le principe, les conditions, les utilisateurs visés et parfois nécessairement triées pour enfin étudier les limites à cette expansion (Titre I). Cependant, nous verrons que l'élargissement mis en œuvre en la matière peut avoir des conséquences non négligeables. C'est la raison pour laquelle il sera nécessaire d'opérer une conciliation avec les libertés et droits fondamentaux, d'analyser les difficultés purement juridiques ou techniques rencontrées, en quelle mesure la LOPPSI 2 peut venir au secours de la HADOPI pour enfin s'interroger sur la bonne effectivité de ces lois au regard de l'utilisateur lui-même (Titre II).

A travers cet état des lieux, il sera possible pour l'utilisateur d'avoir un guide de lecture[23] sur les dispositions législatives qui attraient à la maîtrise de son accès à Internet. Il pourra se rendre compte du chemin parcouru par le législateur concernant sa connexion Internet, des obligations qui lui sont imposées, des risques engendrés par son comportement, des garanties apportées et des difficultés rencontrées. Qu'il soit une entreprise, un particulier, ou tout autre organisme, il pourra être conscient des enjeux liés à notre problématique et des moyens dont il dispose pour prévenir toute atteinte, voir le cas échéant s'exonérer de toute responsabilité.

---

[19] <http://www.universalis.fr/encyclopedie/legitimite/3-legalite-et-legitimite-du-pouvoir/>
[20] Christiane Féral-Schuhl, dans le cadre d'une interview pour lemondedudroit.fr <http://lemondedudroit.fr/decryptages-profession-avocat/17468-loppsi-2-un-objectif-securitaire-au-detriment-des-libertes-individuelles-selon-christiane-feral-schuhl.html>
[21] Personnage du roman intitulé « *1984* » de George Orwell. Il y est généralement fait référence pour dénoncer une atteinte aux libertés fondamentales et au droit à la vie privée
[22] Par exemple : Conseil constitutionnel – Décision n°2009-590 DC du 22 octobre 2009
[23] Voir annexe 1 – Tableau récapitulatif à l'attention de l'utilisateur, p59 et s.

Titre I - La mise en œuvre d'atteintes légitimes portées à la connexion Internet de l'utilisateur

Il y a encore quelques années, Internet s'érigeait en un espace nouveau mais n'en a pas pour autant bouleverser la législation. En effet, son avènement n'a *a priori* fait qu'accentuer certains phénomènes réprimés par la loi tels que la contrefaçon ou la criminalité en bande organisée. Ainsi, le droit que l'on connaissait avant l'ère d'Internet a pu s'y adapter mais a tout de même nécessité un aménagement afin de mieux prendre en considération la prolifération de certaines pratiques. Il convient dès lors d'analyser l'état du droit antérieur relativement à la connexion Internet et le besoin d'évolution (Chapitre I), afin d'observer les atteintes envisagées et mises en œuvres par les lois HADOPI et LOPPSI 2 (Chapitre II).

Chapitre I - Etat du droit antérieur et mise en perspective des difficultés liées à l'ère numérique

La connexion Internet de l'utilisateur a longtemps été à l'abri des regards du législateur puisqu'elle ne suscitait guère d'intérêt aux prémices de l'univers numérique. Au fil de l'évolution des usages sur Internet et des moyens technologiques, l'accès à Internet a rapidement suscité les convoitises. Nous étudierons en quelle mesure la connexion Internet relevait du contrôle naturel de son utilisateur sans autre risque d'atteinte (Section I). Cet état des lieux nous permettra de déterminer par la suite les besoins qui ont conduit le législateur à entreprendre les mesures impliquant de manière ambivalente une perte du contrôle par l'utilisateur en même temps qu'un renforcement de celui-ci (Section II).

Section I - Une connexion Internet initialement à l'abri de toute atteinte et sous le contrôle unique de l'utilisateur

En matière d'obligation de surveillance de l'usage de la connexion Internet, l'utilisateur en était le gardien naturel et ne dépendait d'aucune disposition législative expresse. Il sera ainsi nécessaire d'analyser comment ce dernier devait faire usage de connexion (I).
En matière de droit pénal, certaines dispositions législatives ont été prises à l'époque pour permettre aux enquêteurs de disposer de moyens efficients. Il conviendra d'observer en quelle mesure ces lois ont servi de socle aux moyens mis en œuvre part la LOPPSI 2 (II).

I. Des obligations classiques à la charge de l'utilisateur

Initialement, l'utilisateur était le maître incontesté de sa connexion « *par nature* ». En effet, nulle obligation n'était à sa charge quant au cas spécifique du contrôle de la connexion Internet. Celui-ci devait simplement prendre garde à ce que sa connexion ne soit pas un moyen pour quiconque dans son entourage de commettre une infraction, sans autre obligation spécifiquement et légalement imposée. Il était alors de son devoir, de se comporter en « *bon père de famille* », et d'être ainsi suffisamment diligent pour que l'utilisation de sa connexion Internet se fasse dans le cadre de la loi et dans le respect du droit des tiers.

C'est d'ailleurs dans ce dernier cadre que l'utilisateur se devait notamment de veiller à la bonne utilisation de son accès au réseau. Cela passait inévitablement par le respect, d'une part, des normes législatives et règlementaires, et d'autre part, via l'obligation de se conformer aux exigences contractuelles passées avec le fournisseur d'accès. Le premier cadre ne pose guère de difficulté. L'adage « *nul n'est sensé ignorer la Loi* » de Jean-Etienne-Maris Portalis illustre parfaitement que dans l'univers numérique, comme dans la vie réelle, nous sommes tous contraints d'avoir un comportement qui honore les normes législatives et règlementaires, Internet n'étant pas un espace de non-droit.

Le second cadre mérite cependant un éclaircissement et notamment pour la période antérieure à la Loi pour la Confiance en l'Economie Numérique du 21 juin 2004[24]. Aujourd'hui pratiquement obsolètes, les

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

fournisseurs d'accès ont malgré tout conservé l'habitude de faire référence dans les conditions générales d'utilisation au respect de la « *netiquette* »[25]. Celle-ci peut notamment se définir selon l'Association des Fournisseurs d'Accès et de Services Internet[26] comme étant « *la charte de bonne conduite des acteurs de l'Internet, qu'ils soient utilisateurs professionnels ou particuliers*[27] ». Plus généralement, la nétiquette est formée à partir des termes « éthique » et « Internet », et désigne l'ensemble des règles de savoir vivre à respecter dans l'usage des NTIC[28]. *A priori* donc, les règles édictées en la matière ne sont que très peu contraignantes du fait de leur caractère très général, cependant les sanctions peuvent s'avérer considérables. En effet, il est parfois explicitement spécifié que « *le non-respect de ce code par l'utilisateur peut entraîner la suspension ou la coupure de son compte* »[29]. La coupure de l'accès, qui nous le verrons est désormais une sanction législativement prévue[30], est l'atteinte la plus grave qui puisse être portée en la matière puisqu'elle va jusqu'à remettre en cause l'existence même de la connexion à Internet. C'est pourquoi l'utilisateur doit clairement être conscient des enjeux liés à la nétiquette. Il était d'ailleurs possible de lire dans certains contrats que « *le client s'engage expressément à ne pas utiliser le Service à des fins ou de manière frauduleuse, illégale et, en général, contraire à une disposition réprimée civilement ou pénalement*[31] ». La nétiquette peut donc servir à rappeler que l'utilisateur doit agir conformément aux droits des tiers et demeure susceptible d'être condamné sur ce fondement.

Cependant, la nétiquette est avant tout un code de bonne conduite, de respect mutuel entre utilisateurs et un guide pour mieux appréhender l'univers d'Internet. Elle fait en quelque sorte de chaque utilisateur du réseau un acteur de régulation. Elle tend d'ailleurs à ne plus avoir d'impact réel tant elle est peu usitée et mise à jour des dernières innovations (blogs, forums, wikis, etc.). De même, elle n'a été que très rarement source de jurisprudence car elle implique le signalement par les autres utilisateurs victimes du non respect de ces règles de courtoisie, et le caractère peu contraignant de ces règles participe à sa difficile mise en œuvre[32]. Il faut enfin qu'elle soit expressément insérée dans le champ contractuel pour qu'elle puisse trouver une force contraignante.

Outre la nétiquette aujourd'hui bien anecdotique mais toujours dans la sphère contractuelle, les conditions générales d'utilisation d'un site Internet pouvaient et peuvent encore avoir un réel impact. En effet, elles viennent contractualiser la relation entre le visiteur, qu'il soit enregistré ou non, et l'éditeur de service de communication au public en ligne. Ainsi ces conditions générales doivent par exemple obligatoirement faire apparaître, selon la Loi pour la Confiance dans l'Economie Numérique, les mentions légales[33]. Ces dernières

---

[25] J. Larrieu, « *Droit de l'Internet* », 2ème édition Ellipses, p118 et s.
Par exemple, voir l'annexe 1 « Netiquette » des conditions générales d'abonnement relatives aux forfaits bas débit Internet Orange
<https://docs.google.com/viewer?a=v&q=cache:wwDPiCcPNHwJ:boutique.orange.fr/doc/contrat2236.pdf+orange+acc%C3%A8s+internet+n%C3%A9tiquette&hl=fr&gl=fr&pid=bl&srcid=ADGEESj98_apeGnQ9JkfD8CXQSjGqJPH_oWvHXtc-0Gmx-nlZigehIacYhQmJagHWjM0aKICF4g58vTrOZzxQ_j_clhJzPfpVnhmdeQuCVzCxDI7FsDXGxU9ntuk2msdpDlcAMbRcT9w&sig=AHIEtbSBROt9IZ3jZ8tuNMetf7T14aca6A >
[26]< http://www.afa-france.com/netiquette.html>
[27] Voir Orange, Conditions générales, Annexe I - Netiquette
[28] Nétiquette : un code d'éthique pour Internet < http://oilq.org/fr/node/10733 >
[29] Voir Orange, Conditions générales, Annexe I – Netiquette – Article 9 : Résiliation
[30] Voir page 21 et s., *« l'extension de la Loi « HADOPI 2 » : Une obligation de vigilance sanctionnée sur le fondement de la négligence caractérisée* »
[31] Extraits de Contrat « *9 Telecom* », art. 7.3
[32] L' « *AFA* » a pour habitude de citer les décisions du Tribunal de Grande Instance de Rochefort-sur-Mer en 2001 et celle du Tribunal de Grande Instance de Paris en 2002.
[33] *Article 6 III. - 1. Les personnes dont l'activité est d'éditer un service de communication au public en ligne mettent à disposition du public, dans un standard ouvert :*
a) S'il s'agit de personnes physiques, leurs nom, prénoms, domicile et numéro de téléphone et, si elles sont assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription ;
b) S'il s'agit de personnes morales, leur dénomination ou leur raison sociale et leur siège social, leur numéro de téléphone et, s'il s'agit d'entreprises assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription, leur capital social, l'adresse de leur siège social ;
c) Le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction au sens de l'article 93-2 de la loi n° 82-652 du 29 juillet 1982 précitée ;
d) Le nom, la dénomination ou la raison sociale et l'adresse et le numéro de téléphone du prestataire mentionné au 2 du

font apparaître les informations qui doivent être portées à la connaissance de l'utilisateur sur le site ou la société. Elles peuvent également faire mention de l'objectif du site, de la description de son activité et surtout des conditions d'utilisation. Au regard du droit d'auteur, ces dernières permettront de spécifier les réserves de droit de propriété intellectuelle, notamment quant aux articles et images publiées par l'éditeur[34]. Elles le placent ainsi à l'abri de certains litiges puisqu'elles prévoient les sanctions liées à une éventuelle violation et peuvent également désigner la compétence d'un Tribunal.

Malgré tout, les conditions générales d'utilisation peuvent s'avérer inefficaces dans la lutte contre certains usages tels que la contrefaçon. En effet, l'éditeur d'un site Internet se borne généralement à protéger le site lui-même, sa structure et ses propres contenus. Il ne fait donc pas toujours obstacle aux contenus diffusés par le visiteur lui-même bien qu'il est toutefois possible pour l'ayant droit d'aller chercher la responsabilité de l'intermédiaire technique sur le fondement du régime instauré par la Loi pour la Confiance en l'Economie Numérique[35]. Cependant, il faut souligner que la jurisprudence adopte une interprétation restrictive concernant les conditions d'engagement de la responsabilité dans le cadre de la LCEN[36].

I.2. Les personnes éditant à titre non professionnel un service de communication au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné au 2 du I, sous réserve de lui avoir communiqué les éléments d'identification personnelle prévus au 1

[34] <http://www.cgv-expert.fr/articles/cgu-conditions-generales-utilisation.htm>

[35] Sur ce thème voir Ronan Hardouin – « La jurisprudence, les textes et la responsabilité des hébergeurs », dans Revue Lamy Droit de l'Immatériel, n°39, page(s) 67-71, publié le 1er juin 2008, et voir également pour application, du même auteur « Dailymotion hébergeur et... bon Samaritain ? », dans Revue Lamy Droit de l'Immatériel, n° 67, page(s) 16-18, publié le 1er janvier 2011, concernant la décision de la Cour d'appel de Paris, Pôle 5, première Chambre, 13 octobre 2010, arrêt numéro 07/12236

[36] Voir notamment Véronique Dahan et Howard Tempier : « Les sites participatifs du web 2.0 sont des hébergeurs : est-ce la fin d'une controverse ? », à propos de Cass. 1re civ., 17 févr. 2010, RLDI 2011/69, n° 2281
Voir également Arnaud Richard : « La responsabilité des hébergeurs sur Internet » http://www.lemondedudroit.fr/decryptages-profession-avocat/92227-la-responsabilite-des-hebergeurs-sur-internet.html

II. Les prémisses de la loi Perben II et de la loi de 2005 : interceptions judiciaires et captations d'images et de sons

L'extension opérée par loi LOPSSI 2 que nous analyserons[37] a d'abord pour origine la loi du 9 mars 2004 dite Perben II portant adaptation de la justice aux évolutions de la criminalité[38]. Elle fut mise en œuvre sous l'influence de la Convention sur la cybercriminalité du 8 novembre 2001 et prévoit à la requête du Procureur de la République sous le contrôle du juge des libertés et de la détention d'« *autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications […] pour une durée maximum d'un mois, renouvelable une fois dans les mêmes conditions de forme et de durée* »[39]. Cette voie est ouverte si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application de l'article 706-73 du Code de procédure pénale[40] l'exigent (et notamment dans le cadre du trafic de stupéfiants, des actes de terrorisme, certaines infractions commises avec la circonstance aggravante de bande organisée comme l'enlèvement et séquestration, le proxénétisme, le vol, l'aide à étranger en situation irrégulière, etc.).

Aux termes des dispositions de l'article 706-96 du Code de procédure pénale et après avis du procureur de la République, le juge d'instruction dispose d'un pouvoir identique dans le cadre d'une information judiciaire s'il s'agit d'un véhicule ou d'un lieu privé. S'il s'agit d'un lieu d'habitation et que l'opération intervienne hors des heures prévues à l'article 59 du Code de procédure pénale, soit avant six heures ou après vingt-et-une heures, c'est le juge des libertés et de la détention qui délivre l'autorisation de mise en place d'un dispositif de captations de paroles ou d'images, après saisine par le juge d'instruction.

Cette possibilité s'inscrit dans le cadre de la Loi du 12 décembre 2005 relative au traitement de la récidive des infractions pénales[41]. Elle prévoit en effet pour le même champ d'application que loi Perben II[42] de « *mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux ou véhicules privés ou publics, ou de l'image d'une ou plusieurs personnes se trouvant dans un lieu privé* »[43].

Ces lois servent de base à la LOPPSI 2 et ont déjà posé de multiples difficultés en matière de respect de la vie privée[44]. Les jurisprudences respectives de la Cour de cassation et de la Cour européenne des droits de l'Homme montrent d'ailleurs que la protection de la vie privée nécessite des garanties suffisantes en matière de clarté des dispositions législatives[45], de protection de l'identité[46], ou même de contrôle du juge d'instruction[47]. Nous verrons que ces difficultés ne font finalement que s'accentuer avec la LOPPSI 2, l'immixtion n'en étant que plus importante.

Ces aspects ayant été mis en exergue, il est désormais temps d'étudier les besoins nécessaires qui ont permis l'émergence des lois HADOPI et LOPPSI 2.

---

[37] Voir p.21 et s., « L'extension de la LOPSSI 2 : la captation de données informatiques »
[38] Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000249995>
[39] Article 706-95 CPP Modifié par LOI n°2011-267 du 14 mars 2011 - art. 35
[40] Article 706-73 CPP : Modifié par LOI n°2011-525 du 17 mai 2011 - art. 157
<http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006577780&cidTexte=LEGITEXT000006071154>
[41] Loi n° 2005-1549 du 12 décembre 2005 relative au traitement de la récidive des infractions pénales (1) <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000786845>
[42] Article 706-73 CPP : Modifié par LOI n°2011-525 du 17 mai 2011 - art. 157
[43] Article 706-96 CPP Modifié par Loi n°2005-1549 du 12 décembre 2005 - art. 39 JORF 13 décembre 2005
[44] Claudine Guerrier, « La LOPPSI 2 en 2011 », Revue Lamy droit de l'immatériel, n°70, pages 92-101, janvier 2011
[45] CEDH, Pl. 2 août 1984, Req. *Malone contre Royaume Uni*, n° 8691/79
[46] CEDH, 4ème chambre, 28 janvier 2003, *Peck contre Royaume-Uni*, Req. n°44647/98
[47] Cour de cassation, chambre criminelle, 21 mars 2007, n°06-89.444

Section II - Un besoin primordial d'atteindre des objectifs, une connexion Internet devenue le *nerf de la guerre*

Les dispositions étudiées précédemment vont vite se révéler insuffisantes au regard de nouveaux objectifs. C'est la raison pour laquelle on va, dans un sens, obliger l'utilisateur à avoir un meilleur contrôle de sa connexion Internet (I), et dans un autre sens permettre aux enquêteurs de disposer de nouveaux moyens en détournant ladite connexion (II).

I. Vers un renforcement du contrôle par l'utilisateur de sa connexion

La législation s'avérant insuffisante dans le cadre du contrôle de la connexion Internet(A), il a vite été nécessaire de procéder à de nouvelles mesures pour faire face à l'expansion de certains usages sur la toile pouvant porter atteinte aux droits des tiers (B).

A. L'insuffisance de la législation en matière de contrôle de la connexion Internet

Comme nous l'avons observé, la connexion Internet n'est initialement pas une priorité du législateur. Pendant longtemps, le droit s'est contenté des dispositions déjà existantes pour responsabiliser l'utilisateur. Cependant, avec l'essor des nouvelles technologies, le besoin de réprimer certains comportements s'est de plus en plus fait ressentir. C'est à travers les problèmes de téléchargements illicites d'œuvres protégées par le droit d'auteur que la connexion à Internet est peu à peu devenue le nerf de la guerre. Le code de bonne conduite édicté par la nétiquette a rapidement été écarté car jugé insuffisant, rarement mis en œuvre comme nous l'avons vu et surtout déclaré abusif[48] dans certains cas.

Dans le cadre de notre sujet, nous nous intéresserons à un comportement bien particulier à la source duquel est né le dispositif juridique spécial érigé par les lois HADOPI. Avec l'essor des NTIC, les problèmes de « *Peer to peer* » ont fait grand bruit dans la sphère du droit d'auteur. Cependant, malgré cet essor et la multiplication des mises à disposition d'œuvres sans autorisation des ayants droits, notre droit semblait adapté à appréhender ce phénomène nouveau et menaçant. En effet, dans le projet de loi favorisant la diffusion et la protection de la création sur internet, on pouvait d'ailleurs lire qu' « *une atteinte aux droits ou au droits voisins, y compris sur Internet et via les réseaux numériques, constitue, en l'état actuel du droit et au sens du code de la propriété intellectuelle, un acte de contrefaçon*[49] ». Ainsi, l'article L335-2 du CPI qualifie de contrefaçon « *toute édition d'écrits, de composition musicale (…) au mépris des lois et règlements relatifs à la propriété des auteurs* » et punit « *de 3 ans d'emprisonnement et de 300 000 euros d'amende* » le contrefacteur. L'article L335-3 précise d'ailleurs qu' « *est également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur* ».
La loi semblait donc bien rédigée de façon suffisamment large pour englober ces échanges de « *peer to peer* ». Pour autant, le délit classique de contrefaçon a souvent été remis en cause pour sa difficulté à s'adapter aux actes litigieux effectués sur le réseau Internet. A la lecture de la jurisprudence[50], il n'y a pas

[48] Selon la recommandation n°07-01 (considérant n°1) de la Commission des clauses abusives, est de nature à déséquilibrer de manière significative le contrat au détriment du particulier la clause qui stipule que la « *netiquette* » fait partie des documents contractuels que le consommateur s'engage à respecter, une telle clause obligeant, sous peine de sanctions contractuelles, le consommateur en vertu de ce code de bonne conduite indépendamment de toute acceptation de sa part et le cas échéant, sans qu'il en ait eu connaissance.
Voir aussi TGI Paris – 1ère Chambre – Section sociale – n° 04/02910 : « […] *que cette clause est abusive puisqu'elle a pour effet d'obliger le consommateur à respecter un code de bonne conduite qui n'est pas annexé à son contrat et qu'il n'a pas de ce fait accepté de façon expresse ; qu'il importe peu que le document soit accessible à l'usager* […]»

[49]< http://www.senat.fr/dossierleg/pjl08-498.html >

[50] Voir par exemple TGI Paris, ord. Réf., 14 août 1996, RG n°60139/96, Ed. musicales Pouchenel a. c/Ecole centrale de Paris a., D. 1996, jur.490, note Gautier ; JCP E 1996, II, n°881, note Edelman ; Degroote, « la chanson française à l'honneur sur le net », Lamy dr. Informatique et réseaux oct. 1996 (F) ; Olivier et Barbry, « la propriété intellectuelle occupe

vraiment d'hésitation quant à l'individu qui met à disposition un contenu sans autorisation des titulaires de droits. L'article 1er de la LCEN dispose qu'il faut entendre par communication au public par voie électronique « *toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée* ». Les juges ont ainsi souvent sanctionné le fait de reproduire et de mettre en ligne des œuvres protégées sans l'autorisation des titulaires des droits.

En revanche, la doctrine se trouve divisée sur le point de savoir si celui qui télécharge le contenu est lui aussi contrefacteur. La doctrine et la jurisprudence ont parfois parlé de « *licéité de la source* » comme condition d'application de l'article L122-5 2° du code de propriété intellectuelle relatif à la copie privée, mais ce fondement demeurait incertain[51] et discuté[52] car inexistant dans les textes législatifs.

Ces raisons ont conduit le Gouvernement à mettre en œuvre un arsenal juridique spécifique plus apte à contrôler et endiguer ladite menace afin d'apporter dans le même temps une sécurité juridique à ce sujet. C'est pourquoi il a été décidé de se tourner vers la source du problème à savoir l'utilisateur lui-même.

B. Le besoin d'obliger l'utilisateur à se responsabiliser

L'utilisateur est au cœur des difficultés rencontrées par les titulaires de droits pour faire respecter leur monopole d'exploitation. En effet, c'est lui qui bien évidemment contrôle son accès Internet et va décider de, soit mettre à disposition un contenu au public en ligne, soit au contraire télécharger ledit contenu. L'idée du législateur est donc très simple puisqu'elle consiste à forcer l'utilisateur a réellement prendre garde aux contenus qui circulent par le biais de sa connexion. Par exemple, il appartient aux parents de superviser l'usage qui est fait de la connexion par leurs enfants ainsi que de toute personne amenée à utiliser la ligne, les adolescents étant souvent visés comme étant des acteurs majeurs des échanges illicites faits sur la toile. L'élaboration de l'arsenal juridique que nous développerons plus tard se fonde dès lors sur l'idée qu'un réel contrôle de la connexion par l'utilisateur de son accès au réseau va permettre de ralentir, voire mettre fin aux échanges de contenus litigieux.

Ainsi, il a été instauré via la loi *Création et Internet* l'article L336-3§1er du CPI qui met à la charge de la personne titulaire de l'accès Internet « *l'obligation de veiller à ce que ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition, ou de communication au public d'œuvres protégées par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres I et II lorsqu'elle est requise* »[53].

---

toujours nos esprits… et nos lectures », Expertises nov. 1996, p.387 ; http://legalis.net/spip.php?page=jurisprudence-decision&id_article=117
Voir également TGI Paris, ord. Réf., 5 mai 1997, Jean-Marie Queneau c/ Christian L…, L'Université Paris VIII, l'assoc. Mygale Point Org, Frédéric C…, JCP 1997, II, 22906, note Olivier ; RDPI 1997, n°80, p53 ; www.juriscom.net/jpc/visu.php?ID=213 ; Bréban et Rojinsky, « Internet : le TGI de Paris entrouvre la porte du domicile virtuel », Les Echos 7 juillet 1997, p.69

[51] La jurisprudence n'a jamais clairement tranché en faveur d'une vision ou d'une autre. La Chambre criminelle de la Cour de cassation avait, dans son arrêt du 30 mai 2006 relatif à l'affaire « *Aurélien D.* », renvoyé à la Cour d'Appel d'Aix en Provence afin d'être fixée, mais cette dernière a malheureusement pris soin d'éviter de se prononcer le 5 septembre 2007. En revanche, depuis un arrêt du Conseil d'État du 11 juillet 2008 n°298779, la Commission sur la Rémunération pour copie privée doit exclure de l'assiette de rémunération les copies dont la source est illicite. Le législateur a définitivement tranché en faveur de la source licite par l'intermédiaire de la loi n° 2011-1898 du 20 décembre 2011 relative à la rémunération pour copie privée qui dispose en son article 1er : "*Au second alinéa, après le mot : « "réalisée", sont insérés les mots :* "*à partir d'une source licite*" *»*

[52] Dussolier Séverine, « L'utilisation légitime de l'œuvre : un nouveau sésame pour le bénéfice des exceptions en droit d'auteur », Communication Commerce électronique, n°11, novembre 2005, étude 38. A propos de la décision Cass. Crim., 30 mai 2006, n°05-83.335, F-D, SEV et al. c/ Aurélien D, Juris-Data n°2006-033837 - Christophe CARON – « La source de la copie privée doit-elle être licite ? », dans Communication Commerce électronique n°9, Septembre 2006, comm.118, et à propos de la décision CA Versailles, çe ch. Corr., 16 mars 2007, O. : Juris-Data n°2007-331563 « Source licite et usage privé du copiste », dans Communication Commerce électronique n°7, juillet 2007, comm.91

[53] Article L336-3 du CPI - Modifié par la loi n°2009-1311 du 28 octobre 2009 – article 10 <http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=68F56F93716C200F2DD6F9680DAD7859.tpdjo15v_1?idArticle=LEGIARTI000021212163&cidTexte=LEGITEXT000006069414&dateTexte=20110808&categorieLien=id>

Désormais, il est du devoir de l'utilisateur de filtrer les contenus circulant au moyen de son accès au réseau, obligeant celui-ci à se responsabiliser et à respecter les droits des tiers.

La sanction du non respect de cette obligation est envisagée par la loi « *HADOPI 2* » qui prévoit, via les articles L335-7[54] et L335-7-1[55], la possibilité d'engager la responsabilité du titulaire de l'accès susvisé en le condamnant à *« la peine complémentaire de suspension de l'accès à un service de communication au public en ligne pour une durée maximale d'un an, assortie de l'interdiction de souscrire pendant la même période un autre contrat portant sur un service de même nature auprès de tout opérateur* » en cas « *de négligence caractérisée* ».

Ainsi, outre cette nouvelle obligation dite de vigilance, l'accès à un service de communication au public en ligne est d'abord mis en péril par cette sanction que nous ne manquerons pas de décrire et d'analyser lors des chapitres suivants. Il convient désormais de s'intéresser au cas de la loi LOPPSI 2 qui va caractériser la seconde grande atteinte au contrôle de la connexion Internet par l'utilisateur.

II. Vers une perte du contrôle de la connexion Internet par l'utilisateur ?

Les moyens technologiques ne cessant de se développer, les enquêteurs sont contraints de s'y adapter en permanence (A). De ce fait, la connexion Internet est apparue comme un moyen incontournable pour donner à ces derniers les ressources nécessaires pour combattre la criminalité (B).

A. Le besoin de nouveaux moyens pour combattre la cybercriminalité

Nous avons observé que, depuis 2005, le législateur profite des nouveaux moyens technologiques pour les placer entre les mains des enquêteurs. Comme le souligne très justement Daniel Zenaty[56], « *il faut que les services d'enquête spécialisés disposent de moyens pour combattre la cybercriminalité* ». Ce besoin s'avère compréhensible à l'aune de différentes raisons.

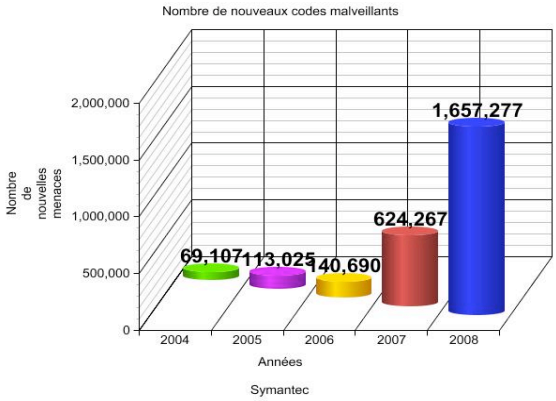
Pour commencer, Internet semble être une cible de choix pour la cyber délinquance. Par exemple, dès le lendemain de la promulgation des lois permettant les interceptions légales de télécommunications, l'enquête annuelle de Symantec Corporation[57] publiée en 2008 révélait une explosion de la cybercriminalité.

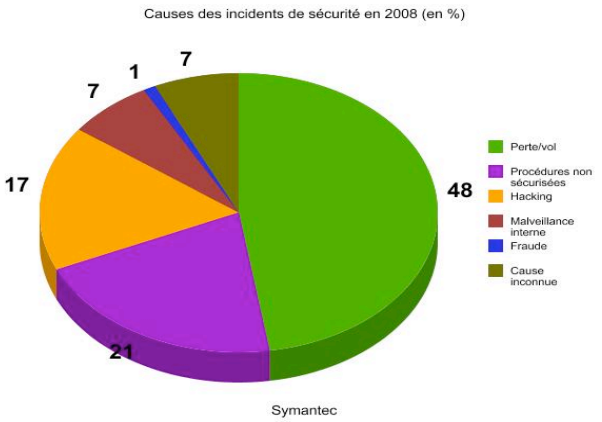
[54] Article L335-7 CPI - Modifié par la loi n°2009-1311 du 28 octobre 2009 – article 7 <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000021212151&cidTexte=LEGITEXT000006069414&dateTexte=20110808&fastPos=1&fastReqId=174910909&oldAction=rechCodeArticle>

[55] Article L335-7-1 Créé par la loi n°2009-1311 du 28 octobre 2009 - article 8 <http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=68F56F93716C200F2DD6F9680DAD7859.tpdjo15v_1?idArticle=LEGIARTI000021212156&cidTexte=LEGITEXT000006069414&dateTexte=20110808&categorieLien=id>

[56] Daniel Zenaty, Expert en informatique, Conférence du 17 mars 2011 organisé par le Master 2 Droit du Multimédia et de l'Informatique Université Panthéon-Assas Paris 2 en partenariat avec l'association française des juristes d'entreprise et juriscom.net — « *La perquisition à distance par l'introduction de mouchards informatiques* »

[57] Symantec Corporation, société américaine de renom spécialisée dans les logiciels informatiques, la recherche et le développement. Elle publie un rapport annuel et une analyse détaillée de l'activité des menaces sur Internet, des programmes malveillants et des vulnérabilités connues <http://eval.symantec.com/mktginfo/enterprise/white_papers/bwhitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf>





Le schéma ci-dessus nous démontre clairement qu'au-delà du développement des techniques, la fréquence et la diversité de la cybercriminalité ne cesse de s'accroitre et c'est pour cette raison que les moyens donnés aux enquêteurs vont vite se révéler peu efficaces, voir impuissants. Ainsi, pour combattre la cybercriminalité, il devient primordial de développer des techniques permettant d'endiguer les infractions commises sur les réseaux numériques et par ce biais, adapter la procédure pénale au rythme de ces évolutions technologiques. Myriam Quéméner précise sur ce point que « *dénoncer de façon systématique le projet de loi LOPPSI 2 est le signe d'une ignorance du fait que la cybercriminalité n'est plus aujourd'hui un épiphénomène mais bien une délinquance « industrialisée », s'inscrivant dans des groupes criminels internationaux* »[58]. Les enquêteurs n'ont que peu de prise sur le développement de ces nouvelles techniques et le journal « *Le Figaro* » rapportait par exemple que la police judiciaire « *ne pouvait pas capter les conversations des trafiquants qui communiquent désormais via leur ordinateur grâce au protocole du logiciel Skype, entièrement crypté* »[59].

Mais avec l'essor des technologies numériques, ce sont désormais des opportunités inouïes de mettre en œuvre des moyens performants et peu coûteux. En matière d'écoutes classiques, il est nécessaire d'obtenir le matériel permettant la capture des images et sons désirés. Ainsi, dans le cadre des nombreuses enquêtes qui s'effectuent chaque année, les enquêteurs doivent se fournir notamment en micros et en caméras, ce qui devient très rapidement extrêmement lourd financièrement[60] dès lors que ces enquêtes se développent à grande échelle sur l'ensemble du territoire national. En revanche, dans le monde numérique, tout est dématérialisé et reproductible à l'infini.

Pour ces raisons stratégico-financières, le législateur a décidé de permettre aux officiers de police judiciaire de disposer de nouveaux moyens d'investigation afin de leur permettre une plus grande efficience dans la lutte contre la cybercriminalité. Inévitablement, ce nouveau moyen devait tôt ou tard passer entre les mains des forces de l'ordre car la raison la plus importante est bien évidemment le fait qu'« *aussi surprenant que cela puisse paraître, la justice, qui (pouvait) placer des caméras et des micros partout, n'avait aucun droit d'accès aux ordinateurs, sanctuarisés par un vide juridique* »[61]. En effet, jusqu'à présent, l'accès aux ordinateurs ne s'effectuait que par l'intermédiaire de perquisitions des systèmes informatiques dans le cadre d'une enquête de flagrance[62], d'une enquête préliminaire[63] ou d'une enquête sur commission rogatoire[64].

---

[58] <http://www.e-juristes.org/les-perspectives-penales-de-la-loppsi-2-en-matiere-de-cybercriminalite/>
[59] <http://actualite.lefigaro.fr/stupefiants-trafic-armes.html>
[60] <http://www.numerama.com/magazine/15076-loppsi-l-installation-de-mouchards-chez-les-suspects-est-adoptee.html>
[61] <http://www.lefigaro.fr/actualite-france/2009/05/24/01016-20090524ARTFIG00098-la-police-va-pouvoir-pirater-les-ordinateurs-des-voyous-.php>
[62] Article 57-1 du Code de procédure pénale <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006575037&cidTexte=LEGITEXT000006071154&dateTexte=20111228&oldAction=rechCodeArticle>
[63] Article 76-3 du Code de procédure pénale <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006575129&cidTexte=LEGITEXT000006071154&dateTexte=20111228&oldAction=rechCodeArticle>
[64] Articles 94 et 97-1 du Code de procédure pénale

B. Un moyen incontournable : le passage par la connexion Internet de l'utilisateur

La connexion au réseau est un point tactique fondamental. Comme nous l'avons observé, Internet est désormais profondément ancré dans le quotidien des français. L'ARCEP a d'ailleurs publié le 1er juin 2011 une actualité[65] démontrant clairement cette croissance, puisqu'au 31 mars 2011, le nombre d'abonnements Internet à haut et très haut débit sur les réseaux fixes s'élevaient à 21,8 millions, soit une hausse de 8% par rapport à 2010. Environs un tiers de la population française est donc désormais connecté à la toile, outre les multiples accès wifi, téléphonie mobile, etc. La stratégie liée à la LOPPSI 2 semble dès lors limpide comme le remarque Guillaume Champeau[66] en établissant que « *pour le Gouvernement, il s'agit d'adapter à l'ère informatique les dispositifs d'écoute téléphonique* ». Si Internet est à ce point devenu incontournable, il serait dommage que la loi n'y prête guère attention.

Désormais, l'article 706-96 du code de procédure pénale prévoit expressément que lorsque « *les nécessités de l'information relative à un crime ou un délit entrant dans le champ d'application de l'article 706-73 l'exigent, le juge d'instruction, peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique qui a pour finalité, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux ou véhicules privés ou publics, ou de l'image d'une ou plusieurs personnes se trouvant dans un lieu privé* ».

Cet article que nous présenterons plus précisément par la suite[67] nous permet d'observer que c'est bel et bien par le biais de la connexion Internet de l'utilisateur qu'il est désormais possible pour les investigateurs de procéder au recueillement d'éléments propres à façonner leur enquête. Le contrôle de la connexion Internet est ici mis en péril par ce texte qui octroie aux officiers de police judiciaire la possibilité de s'emparer de l'accès au motif impérieux de rassembler les preuves suffisantes et nécessaires à la caractérisation de l'infraction

Il semble essentiel d'entrer dans les arcanes de ces dispositions pour en analyser les tenants ainsi que les aboutissants afin d'en déterminer et d'en juger l'équilibre. C'est pourquoi nous allons désormais nous intéresser aux extensions opérées par les lois susvisées afin d'en déterminer le mécanisme procédural général et les premières réelles difficultés rencontrées.

Conclusion

Malgré des objectifs distincts, les deux lois tendent véritablement à se resserrer sur l'utilisateur de la connexion Internet. Le contrôle qu'il détient est plus que jamais le dénominateur commun visant à combattre les infractions proliférant dans le cyberespace. Il est donc indispensable de jauger l'impact de ces nouvelles dispositions afin d'en établir les risques et les garanties.

[65] <www.arcep.fr/index.php?id=10295>
[66] <http://www.numerama.com/magazine/15076-loppsi-l-installation-de-mouchards-chez-les-suspects-est-adoptee.html>
[67] Voir « l'extension de la LOPPSI 2 : la captation de données informatiques », p.21 et s.

Chapitre II – L'épineuse mise en œuvre des lois HADOPI et LOPPSI 2

Le besoin de nouveaux moyens permettant de lutter efficacement contre le téléchargement illicite d'œuvres culturelles sur Internet se caractérise par la promulgation de la loi *Création et Internet* n°2009-669 du 12 juin 2009, complétée par la loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur Internet. Par ailleurs afin de permettre une meilleure lutte contre la criminalité, la loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure repousse les limites de l'intrusion dans la vie privée de l'utilisateur. Il convient d'étudier la portée de ces lois (section I) pour en déterminer les limites (section II).

Section I - La mise en œuvre de lois extensives

L'obligation de vigilance sanctionnée par la suspension de l'accès au réseau a été instituée par les lois HADOPI. Cette sanction marque une véritable atteinte à l'accès au réseau Internet (I). La LOPPSI 2 vient quant à elle concrétiser la possibilité pour les autorités judiciaires de détourner la ligne de l'utilisateur. Cette extension marque également une atteinte au contrôle de la connexion Internet qu'il conviendra d'analyser (II).

I. L'extension des lois HADOPI : une obligation de vigilance sanctionnée sur le fondement de la négligence caractérisée

Les lois HADOPI ont créé une véritable obligation de contrôle de l'usage fait de la connexion Internet. Cette toute nouvelle obligation de vigilance ne tombe sous le coup de la sanction qu'à certaines conditions précises (A) et semble bien s'adresser à tout titulaire d'accès à Internet (B).

A. Conditions préalables, faits constitutifs et sanction de l'infraction

Désormais, et par le biais de l'article L.331-21 du Code de la propriété intellectuelle, la Haute autorité est en mesure d' « obtenir des opérateurs de communications électroniques l'identité, l'adresse postale, l'adresse électronique et les coordonnées téléphoniques de l'abonné ». Cette identification était auparavant uniquement dévolue au juge judiciaire qui pouvait seul ordonner la communication de l'identité du titulaire de l'abonnement par l'intermédiaire des données préalablement collectées par des organismes assermentées. Une fois l'utilisateur identifié, la procédure dirigée à son encontre peut s'ouvrir.

Comme nous l'avons posé plus haut, c'est sur le fondement de l'obligation dite de vigilance instituée à l'article L.336-3§1 du code de propriété intellectuelle et mise en œuvre dans le cadre de la loi HADOPI 1 que l'utilisateur va faire l'objet d'une procédure dissuasive. Plusieurs décrets sont venus définir les modalités d'application de cette disposition, et notamment le décret n°2010-872 publié au journal officiel le 26 juillet 2010 « relatif à la procédure devant la Commission de protection des droits de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet ». Ce décret ajoute ainsi un article R335-5[68] à la partie réglementaire du code de la propriété intellectuelle en application des articles insérés dans le code par la loi du 28 octobre 2009 dite HADOPI 2 afin de définir les conditions préalables et les éléments constitutifs de la négligence caractérisée.

[68] Article R335-5 CPI - Créé par Décret n°2010-695 du 25 juin 2010 - art. 1
<http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000022402015&cidTexte=LEGITEXT000006069414&dateTexte=20110808&fastPos=1&fastReqId=1992602857&oldAction=rechCodeArticle>

Les dispositions prévues à l'article R.335-5, II constituent selon une partie de la doctrine[69], un rappel des conditions préalables à la constitution de l'infraction de négligence caractérisée. En effet, cette dernière ne sera constituée que si le titulaire de l'accès à un service de communication au public en ligne « s'est vu recommander par la commission de protection des droits de mettre en œuvre un moyen de sécurisation de son accès permettant de prévenir le renouvellement d'une utilisation de celui-ci à des fins de reproduction, de représentation ou 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 » et si « dans l'année suivant la présentation de cette recommandation, cet accès est à nouveau utilisé aux fins mentionnées » ci-dessus.

Il faut en outre respecter les exigences de forme prévues par l'article L.331-25[70] du CPI et l'article R.331-40[71] du même code, issu du décret susvisé. Ainsi, l'infraction ne sera constituée qu'une fois que le mail d'avertissement a bien été envoyé, de même que la lettre recommandée remise contre signature (ou tout autre moyen permettant d'établir la preuve de la date de présentation[72]) en cas de réitération de l'acte délictueux. C'est ici que prend forme la fameuse procédure dite de « riposte graduée » qui prend soin d'avertir l'utilisateur qu'il n'a pas le contrôle suffisant de sa connexion et/ou de le dissuader dans la poursuite de ses actes. C'est sur ce point que prend toute l'ampleur de la locution *errare humanum est, perseverare diabolicum* qui signifie *se tromper est humain* ; *persévérer est diabolique*.

Il s'agit ici d'une infraction dite d'habitude car l'infraction n'est constituée que par la répétition de plusieurs actes identiques. Cependant, elle parvient à trouver son originalité dans la mesure où le renouvellement de l'élément matériel doit être précédé d'une recommandation de la Commission de protection des droits, et ce dans l'année suivant ladite recommandation. Les délais sont établis concrètement comme suit :

- A compter du premier avertissement, un délai de six mois sans nouvelle infraction doit s'écouler pour que l'internaute soit complètement déchargé de tout manquement.
- Pendant les douze mois suivant la seconde recommandation, aucun manquement ne doit être constaté.

Par conséquent, passé chacun de ces délais, il est fait table rase du passé et les compteurs sont remis à zéro.

Une fois cette procédure engagée, il faut bien évidemment que les faits constitutifs de l'infraction de négligence caractérisée soient rassemblés. Le *nerf de la guerre* se trouve précisément ici puisque la négligence caractérisée sera constituée si l'utilisateur, soit n'a pas mis en place un moyen de sécurisation de son accès, soit a manqué de diligence dans la mise en œuvre de ce moyen[73]. Ces dispositions se révèlent suffisamment larges pour permettre une constitution de l'infraction *facilitée*[74]. Comme l'a très justement remarqué une partie de la doctrine[75], est sanctionné le fait de ne pas avoir sécurisé son accès et le fait d'avoir effectivement installé un moyen de sécurisation mais qui se révèle finalement inefficace. L'utilisateur doit donc veiller à bien sécuriser son accès et rendre ce moyen, en temps et en heures, suffisamment opérant, en « *bon père de famille* », référent classique en matière de diligence. C'est donc ici que se concentrent les nouvelles obligations de contrôle inscrites dans le marbre de la loi du titulaire de l'accès Internet.

---

[69] Florence Gaullier, Elise Pascal-Heuze, Gilles Vercken, « Les derniers décrets d'application des lois HADOPI », dans Revue Lamy Droit de l'Immatériel, pages 6 et s., n°63 août-septembre 2010

[70] <http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=68F56F93716C200F2DD6F9680DAD7859.tpdjo15v_1?cidTexte=LEGITEXT000006069414&idArticle=LEGIARTI000020738173&dateTexte=&categorieLien=cid>

[71] Article L331-25 modifié par la loi n°2009-1311 du 28 octobre 2009 - article 12 et article 3 <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000022525410&cidTexte=LEGITEXT000006069414&dateTexte=20110809&fastPos=1&fastReqId=74238138&oldAction=rechCodeArticle>

[72] Nicolas Catelan, « La protection du droit d'auteur : une négligence caractérisée ? », Revue Lamy Droit de l'Immatériel, numéro 67, pages 81 et s., janvier 2011

[73] Article R335-5 I - Créé par Décret n°2010-695 du 25 juin 2010 - art. 1 <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000022402015&cidTexte=LEGITEXT000006069414&dateTexte=20110809&fastPos=1&fastReqId=209330435&oldAction=rechCodeArticle>

[74] Le législateur a souhaité étendre les dispositions du texte à l'ensemble des possibilités existantes et à venir afin de prendre en considération toute évolution technologique. Nous le démontrerons dans la suite de notre exposé.

[75] Florence Gaullier, Elise Pascal-Heuze, Gilles Vercken, « Les derniers décrets d'application des lois HADOPI », dans Revue Lamy Droit de l'Immatériel, pages 6 et s., n°63 août-septembre 2010

Si les conditions préalables et les faits constitutifs sont réunis, l'article L.335-7 et L.335-7-1 du Code de la propriété intellectuelle prévoient la possibilité pour le titulaire de la ligne d'être condamné à la peine complémentaire de suspension de l'accès à un service de communication au public en ligne pour une durée maximale d'un mois.

Il faut noter que ce sont bien les manquements aux obligations de contrôle et de surveillance des moyens d'accès à Internet, et non la contrefaçon en elle-même résultant du téléchargement illégal, que le législateur sanctionne. La « *négligence caractérisée* » constitue une infraction spécifique directement mise en parallèle avec celle de contrefaçon. Au regard du droit commun de la responsabilité délictuelle traditionnelle, cette nouvelle forme de responsabilité a d'ailleurs une particularité. En effet, la notion de dommage est le préalable à toute distinction pour engager la responsabilité puisque, contrairement au droit pénal, on ne peut envisager une responsabilité civile s'il n'y a pas de dommage. Or, les caractères du dommage réparable exigent que celui-ci soit certain, ce qui implique qu'il soit présent et donc réalisé. Or en la matière, la responsabilité de l'utilisateur peut-être engagée, alors même que le dommage n'est pas réalisé. En imaginant que le préjudice soit futur, il n'a nullement le caractère d'être certain. L'article L331-25 du Code de la propriété intellectuelle[76] dispose ainsi que « *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 application des articles L. 335-7 et L. 335-7-1* ». Ainsi, entre la version du 30 octobre 2008[77], et celle du 20 avril 2009[78], l'article L. 331-24 a été modifié à trois endroits pour remplacer « *lorsqu'elle est saisie de faits constituant un manquement à l'obligation définie à l'article L. 336-3* ». L'utilisateur pourra donc engager sa responsabilité dans le cadre de cette nouvelle procédure pour des faits simplement susceptibles de constituer un manquement, le dommage n'est donc pas certain.

Enfin cette procédure est évidemment portée à la connaissance de l'utilisateur par l'intermédiaire de son fournisseur d'accès Internet dans le corps même du contrat par une mention claire et lisible[79].

B. A la recherche d'un responsable : la nécessaire sanction du titulaire de l'accès Internet

La Loi HADOPI a été mise en œuvre principalement pour lutter contre les téléchargements illicites d'œuvres mises à la disposition du public sans autorisation des ayants-droit. Comme nous venons de l'évoquer, il peut sembler étrange de ne pas sanctionner l'individu mis en cause par l'infraction de contrefaçon. Cependant, bien que les dispositions législatives ne visent pas expressément les personnes auxquelles seraient reprochés ces actes de contrefaçon, il s'avère que les titulaires de l'accès à Internet sont, bien souvent, les mêmes individus. C'est pourquoi il a été instauré cette obligation de surveillance et celle de se conformer aux recommandations adressées par la Commission de protection des droits afin de mieux contrôler l'usage fait de ladite connexion.

Il faut rappeler que la peine complémentaire de suspension de l'accès Internet va pouvoir s'appliquer « *lorsque l'infraction est commise au moyen d'un service de communication au public en ligne* » ce qui est extrêmement large. En effet, la notion de « *communication au public en ligne* » est définie à l'article 1-IV de la loi n°2004-575 du 21 juin 2004 sur la confiance en l'économie numérique comme « *toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur* ». Ainsi, tout moyen permettant une telle mise à disposition se trouve dans le champ d'application de la loi. Nul ne pourra contester qu'une telle notion est suffisante pour appréhender tous les phénomènes de

[76] Article L331-25 du Code de la propriété intellectuelle modifié par la loi n°2009-1311 du 28 octobre 2009 - art. 12 et la loi n°2009-1311 du 28 octobre 2009 - art. 3
[77] <http://www.assemblee-nationale.fr/13/projets/pl1240.asp>
[78] <http://www.assemblee-nationale.fr/13/projets/pl1618.asp>
[79] Article L331-27 CPI - Créé par LOI n°2009-1311 du 28 octobre 2009
<http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000021212108&cidTexte=LEGITEXT000006069414&dateTexte=20111228&fastPos=1&fastReqId=1843033008&oldAction=rechCodeArticle>

téléchargements illicites à travers le moyen premier de commission ce qui permet d'étendre le champ bien au-delà du simple « *Peer to peer* ». En d'autres termes, tout utilisateur est potentiellement passible de la sanction de suspension d'accès à Internet.

Si ce système peut apparaître comme plus simple et bien plus efficace que la procédure de contrefaçon, il n'en est pas moins confronté à des difficultés pratiques non négligeables. La question se pose de savoir comment l'utilisateur autre que le particulier titulaire d'un abonnement auprès de son FAI est traité par le droit. En effet, l'article R335-5 du Code de la propriété intellectuelle est rédigé de façon suffisamment large pour s'adapter à tout titulaire d'accès Internet sans autre distinction entre personnes physiques et personnes morales. En vertu du principe de généralité mis en place par la Loi Perben II[80] et au détriment du principe de spécialité, les personnes morales sont responsables de toutes les infractions. Partant, en qualité de titulaire d'un accès Internet, toute entreprise est donc susceptible d'être condamnée à la peine complémentaire de suspension de l'accès Internet dès lors que cette dernière serait le moyen d'échanges illicites.

Cependant, une entreprise peut-elle réellement voir sa responsabilité engagée sur le fondement de la négligence caractérisée du fait des agissements délictueux de ses employés ? La question est des plus épineuses car condamner une société à la peine complémentaire de la suspension Internet engendre un danger pour sa survie. La question n'est pas seulement juridique mais économique du fait de la dépendance accrue de nombreuses entreprises à Internet. Nonobstant ces considérations, les personnes morales peuvent se voir priver de toute connexion internet pour une durée maximale d'un mois, au titre de la sanction complémentaire de l'infraction de négligence caractérisée[81], l'article 131-42 du Code pénal disposant que « *pour toutes les contraventions de la cinquième classe, la peine d'amende peut être remplacée par une ou plusieurs des peines privatives ou restrictives de droits suivantes (…) 2° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit* ».

Par ailleurs, les FAI proposent depuis longtemps la possibilité de se connecter via des points d'accès wifi aux utilisateurs de terminaux mobiles (PC portables, PDA, tablettes, etc.). Une fois cette modalité d'utilisation dite « *communautaire* » ou « *hotspot* » activée et acceptée par l'utilisateur, elle permet par exemple aux autres abonnés du même FAI de se connecter à Internet partout en France dès lors qu'il a entré avec succès ses identifiants ainsi que son mot de passe. Le titulaire de la ligne ouverte pourra à son tour utiliser une partie de la bande passante d'un autre abonné dès lors que ce dernier a, lui aussi, activé son « *hotspot* ». Cette pratique n'est pas en marge et il est désormais très simple de se connecter à un tel service. On pourrait croire que le titulaire de l'accès Internet risque de se voir suspendre sa connexion au titre de la négligence caractérisée alors même que c'est un autre utilisateur qui est à l'origine de l'acte délictueux et que ce dernier lui est totalement étranger. Il n'en est rien. En effet, comme nous l'avons exposé, il est nécessaire de s'identifier pour bénéficier de l'accès. Il suffira donc de discerner le titulaire de l'accès de la personne qui en bénéficie par le simple recours à ses identifiants, ces deux individus possédant leurs propres adresses IP.

Dans le même esprit, on peut également se poser la question de savoir ce qu'il en est pour les points d'accès publics en général. Le titulaire de l'accès à Internet peut ainsi être une bibliothèque, un restaurant, un bar ou encore une université. La CNIL a éclairci cet aspect et pose, sans exception, la responsabilité des bibliothèques[82]. Ainsi, on peut lire dans les conclusions du bulletin des bibliothèques de France de mars 2011 que « *les obligations issues du Code des postes et des communications électroniques et de la loi 'informatique et libertés' engagent la responsabilité des organismes mettant à disposition du public un accès à Internet* ».

Le risque d'engager sa responsabilité existe donc pour le cas des bibliothèques et on peut légitimement penser qu'il peut s'étendre à l'ensemble des points d'accès publics, comme Christine Albanel l'avait annoncé en 2008[83] ce qui est peu encourageant pour le développement de tels accès.

---

[80] Article 121-2 du Code pénal <http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006417204&dateTexte=20110809>

[81] Florence Gaullier, Elise Pascal-Heuze, Gilles Vercken, « Les derniers décrets d'application des lois HADOPI », dans Revue Lamy Droit de l'Immatériel, pages 6 et s., n°63 août-septembre 2010

[82] <http://bbf.enssib.fr/consulter/bbf-2011-03-0053-011>

[83] <http://www.numerama.com/magazine/9984-hadopi-les-lieux-publics-pourront-etre-prives-d-internet.html>

Cette diversité de situations montre que le titulaire de l'accès Internet est de plus en plus exposé à engager sa responsabilité. Comme nous l'avons vu, la négligence caractérisée est une infraction spécifique distincte de la contrefaçon qui sanctionne davantage l'abonné au service d'accès Internet que le contrefacteur, ce qui peut se révéler problématique dans bien des cas. Finalement, l'abonné peut être sanctionné alors même qu'il n'a jamais souhaité réaliser un acte de contrefaçon. C'est pourquoi il semble plausible que dans certains cas, si l'auteur de l'infraction est identifié, seule la procédure de contrefaçon sera engagée[84]. Cette possibilité demeure cependant contestable dans la mesure où les lois HADOPI ont justement été érigées pour palier aux difficultés d'application de la contrefaçon.

II. L'extension de la loi LOPPSI 2 : la captation de données informatiques

La loi LOPPSI 2 permet désormais aux enquêteurs de s'immiscer dans la vie privée de l'utilisateur, ce qui demeurait impossible auparavant. Bien évidemment, il a fallu déterminer des conditions et un champ d'application rigoureusement précis (A) et il semble cette fois difficilement concevable que tout utilisateur puisse être l'objet d'une telle procédure (B).

A. Principe: présentation d'une nouvelle arme de lutte contre la cybercriminalité

Depuis le 14 mars 2011, date de promulgation de la loi LOPPSI 2, les enquêteurs disposent de nouveaux moyens d'investigation dans le cadre du même champ d'application que la procédure de captations d'images et de sons mis en œuvre par la Loi Perben II[85]. Cependant ce champ a désormais été élargi[86] à dix-huit infractions relevant de la criminalité organisée.

Comme nous l'évoquions, les officiers de police judiciaire disposeront, pour ces infractions restrictivement énumérées, des moyens techniques leur permettant de capter en temps réel les données informatiques telles qu'elles s'affichent sur l'écran d'ordinateur d'un utilisateur. Le juge d'instruction peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur. Certains soutiennent même qu'il serait possible de recueillir certaines données sensibles indispensables à une enquête comme un mot de passe ou un identifiant à partir du moment où ceux-ci s'affichent à l'écran[87]. Ces nouvelles modalités dites de captation des données à distance ou de « *cyberperquisition* » sont prévues de l'article 706-102-1 à l'article 706-102-9 du Code de procédure pénale. Il faut enfin préciser que, si les possibilités d'interceptions prévues dans le cadre de la loi Perben II permettaient d'intervenir quelque soit le mode d'enquête, la captation de données informatiques n'est envisagée qu'au stade de l'instruction, et non pour l'enquête préliminaire.

Concrètement, les officiers de police judiciaire peuvent désormais utiliser deux méthodes[88], à savoir l'ajout d'un composant matériel dans l'unité centrale de l'utilisateur ou l'installation d'un « *logiciel espion* » plus connu sous le nom de « *mouchard* » ou « *cheval de Troie* ».

Concernant la première méthode, il s'agit d'un composant qui est installé sur l'ordinateur de l'utilisateur par un accès physique à l'insu de son propriétaire. Le juge d'instruction peut donc autoriser l'officier de police

---

[84] Julien Couard, « Interview d'un praticien », dans Revue Lamy Droit de l'Immatériel, numéro 67, pages 67 et suivants, janvier 2011

[85] Article 706-73 du code de procédure pénale <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000024041521&cidTexte=LEGITEXT000006071154&dateTexte=20111228&oldAction=rechCodeArticle>

[86] Dans le cadre de la Loi n°2004-204 du 9 mars 2004 la procédure applicable à l'enquête, la poursuite, l'instruction et le jugement des crimes et des délits s'appliquait pour quinze infractions restrictivement énumérées

[87] Philippe Belloir, « LOPPSI : un projet pour la captation de données informatiques », dans Revue Lamy Droit de l'Immatériel, numéro 50, pages 94 et suivantes, juin 2009

[88] <http://www.valhalla.fr/2010/02/13/loppsi-2-les-spywares-judiciaires/>

judiciaire à s'introduire dans les lieux de l'intéressé sans son consentement et en dehors des heures légales[89]. Cependant pour les lieux à usage d'habitation et si l'opération s'effectue en dehors des heures légales, c'est au juge des libertés et de la détention qu'il revient d'en autoriser la mise en œuvre, après saisie par le juge d'instruction.

En cas d'impossibilité d'accéder physiquement à l'ordinateur, la Loi prévoit que le juge d'instruction peut autoriser la transmission par un réseau de communications électroniques de ce dispositif. Il est alors possible d'utiliser des « *keyloggers* »[90] qui enregistrent instantanément les frappes au clavier ou des « *spywares* »[91] permettant de récupérer le contenu de certains fichiers. Ces modalités transitent par le biais de la connexion Internet de l'utilisateur et permettent de s'adapter aux nouveaux moyens de communication comme les logiciels de voix sur IP (VoIP). Il est même possible d'étendre cette procédure à tout système de traitement automatisé de données reliés à Internet (ordinateur portable, tablettes, etc.). Dès lors, toute connexion à Internet semble pouvoir être détournée au profit de l'investigation et au détriment d'un plus grand nombre d'utilisateurs.

Outre ces moyens, la manœuvre se déroule au stade de l'instruction et par voie d'ordonnance motivée, c'est pourquoi « *le juge d'instruction peut, après avis du procureur de la République, autoriser (…) les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un* [tel] *dispositif technique* » et ceci seulement lorsque les nécessités de l'information l'exigent[92].

Concernant la durée, les opérations ne peuvent aller au-delà d'une durée de quatre mois. Cependant, si les nécessités de l'instruction l'exigent, de manière exceptionnelle et dans les mêmes conditions de forme, un renouvellement de quatre mois peut-être autorisé.

B. A la recherche d'un responsable : l'inéluctable tri des titulaires d'accès Internet

Par nature, l'ingérence permise par les dispositions de la LOPPSI 2 est redoutable puisque potentiellement, toute donnée informatique transitant par le biais de la connexion Internet peut-être contrôlée par les enquêteurs en charge de la procédure. C'est pour cette raison qu'un tri est nécessaire entre les personnes qui sont expressément protégées par la Loi (1) et les autres points d'accès au réseau (2).

1. Une indispensable exclusion des professions protégées

Dans le but de sauvegarder le secret professionnel, le Code de procédure pénale opère une protection de certaines professions devant se trouver à l'abri des procédures de captation de données informatique. Ainsi, concernant les avocats[93], les entreprises de presse ou de communication audiovisuelle[94], les médecins, les notaires, les avoués, les huissiers[95] ainsi que les députés et sénateurs[96], la mise en œuvre du dispositif technique visant à opérer une telle captation de données informatiques est impossible.

---

[89] Sur ce point, voir l'article 59 du Code de procédure pénale <http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=0098134D89DD038FACB30A89F2900E0A.tpdjo15v_1?cidTexte=LEGITEXT000006071154&idArticle=LEGIARTI000006575042&dateTexte=&categorieLien=cid>

[90] Enregistreur de frappe

[91] Logiciels espions

[92] Article 706-102-1 du Code de procédure pénale <http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=0098134D89DD038FACB30A89F2900E0A.tpdjo15v_1?idArticle=LEGIARTI000023712497&cidTexte=LEGITEXT000006071154&dateTexte=20110811&categorieLien=id>

[93] Article 56-1 du Code de procédure pénale <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000021662499&cidTexte=LEGITEXT000006071154&dateTexte=20111228&oldAction=rechCodeArticle>

[94] Article 56-2 du Code de procédure pénale <http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=93450D5041D7F382A53C10D011EF054E.tpdjo15v_1?idArticle=LEGIARTI000021662497&cidTexte=LEGITEXT000006071154&dateTexte=20111228&categorieLien=id>

[95] Article 56-3 du Code de procédure pénale <http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=93450D5041D7F382A53C10D011EF054E.tpdjo15v_1?idArticle=LEGIARTI000006575035&cidTexte=LEGITEXT000006071154&dateTexte=20111228&categorieLien=id>

Initialement le dernier alinéa de l'article 706-102-6 était rédigé ainsi : « *La mise en place de la captation de données informatiques mentionnée au premier alinéa ne peut concerner les systèmes automatisés de traitement de données se trouvant habituellement dans les lieux visés aux articles 56-1, 56-2 et 56-3 ou habituellement utilisés par les personnes visées à l'article 100-7* ».

Sur cet aspect, la CNIL s'est inquiétée[97] de l'emploi du terme « *habituellement* » dans l'article instaurant l'interdiction de l'usage des captations de données informatiques pour ces dernières professions en posant qu'il existerait un risque « *d'aléa et un risque d'insécurité juridique disproportionnés au regard des finalités poursuivies* ». En effet, par ce biais, il existerait le danger de capter des données qui s'affichent sur les écrans de ces différentes personnalités ce qui est contraire au secret protégé par la loi de leurs professions. En somme, la CNIL considérait que la rédaction du projet de loi n'était pas conforme aux principes de collecte adéquate, pertinente et non excessive posés par l'article 6 de la loi « *informatique et libertés* » du 6 janvier 1978 modifiée en 2004.

Finalement, le législateur est intervenu pour supprimer ce péril afin qu'il n'y ait pas d'ambigüité et permettre ainsi de respecter de manière certaine le secret bien gardé desdites professions. Il appartiendra cependant aux enquêteurs de s'assurer de l'identité et de la qualité de personnes faisant l'objet de la procédure en cause ce qui n'est pas forcément aisé en réalité car nul ne sait véritablement qui se trouve devant l'écran d'ordinateur.

2. Une nécessaire distinction des points d'accès à Internet

Dans le cadre des dispositions envisagées par la LOPPSI 2, nous nous situons dans un cadre de criminalité organisée qui tend à restreindre le nombre d'utilisateurs potentiels. Cependant, quid des membres d'une telle organisation agissant par le biais de la connexion Internet d'une entreprise ? A priori, la connexion Internet de l'entreprise n'échappera pas aux dispositions de la LOPPSI 2. D'après Etienne Papin[98], dans le cas où un salarié éveillerait de tels soupçons en utilisant les moyens informatiques mis à disposition par son employeur, le système informatique se verrait alors l'objet d'une telle mesure d'infiltration et « *on peut penser que dans une telle hypothèse, les enquêteurs agiraient en concertation avec l'employeur* ».

Cependant, pour de tels crimes et délits, il n'est pas forcément judicieux de prévenir le responsable de l'entreprise afin de ne pas créer un climat de suspicion. C'est pourquoi, même une entreprise pourra faire l'objet de captation de données informatiques sur le réseau de l'entreprise sans que l'employeur en soit averti du simple fait que la loi prévoit de manière aussi large que neutre que cette procédure s'effectue « *sans le consentement de l'intéressé* ».

Bien que les dispositions de la loi LOPPSI 2 semblent pouvoir s'appliquer à de nombreux cas, il semble opportun d'opérer une distinction vis-à-vis des connexions disponibles dans les lieux publics. Si les dispositions de la loi HADOPI semblent bien pouvoir s'adapter sans commune mesure aux réseaux wifi mis à la libre disposition des utilisateurs, il semble difficile de concevoir que la LOPPSI 2, qui est autrement plus intrusive, puisse également s'y étendre. Ainsi, il semble nécessaire de nuancer le propos exprimé plus haut, visant à poser que de nombreuses connexions à Internet semblent pouvoir être détournées au profit de l'investigation et au détriment d'un plus grand nombre d'utilisateurs. En effet, si les moyens de réception peuvent effectivement être visés sans distinction, il convient de distinguer selon que ce système est mis à la disposition de toute personne ou non.

---

[96] Article 100-7 du Code de procédure pénale

[97] Délibération n° 2009-200 du 16 avril 2009 portant avis sur sept articles du projet de *loi d'orientation et de programmation pour la performance de la sécurité intérieure*
< http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/207/>

[98] Etienne Papin – « La captation des données informatiques : enjeux et conséquences pour les entreprises de la LOPPSI 2 », cio-online.com , contributions, paroles d'expert, 27 sept. 2010
<http://www.cio-online.com/contributions/lire-la-captation-des-donnees-informatiques%C2%A0-enjeux-et-consequences-pour-les-entreprises-de-la-loppsi-2-408-page-1.html>

Pourtant, initialement, le projet de Loi prévoyait la possibilité de capter les informations affichées sur l'écran de tous les ordinateurs d'un point d'accès public à Internet (cybercafés ou bornes d'accès publiques). Sur demande formulée par le Président de la Commission des Lois de l'Assemblée Nationale, la CNIL a pu émettre son avis et ses craintes vis-à-vis de cette disposition dans sa délibération du 16 avril 2009[99].

En effet, « *la Commission souligne la portée de cette disposition, qui pourrait permettre l'enregistrement pendant une durée d'au plus huit mois, de tous les caractères saisis au clavier et de toutes les images affichées sur l'écran de tous les ordinateurs d'un point d'accès public à Internet, et ce à l'insu des utilisateurs. […] La Commission estime nécessaire que cette décision d'installation ainsi que les modalités d'utilisation de ces dispositifs particulièrement intrusifs, fassent l'objet d'une vigilance particulière, afin de garantir la proportionnalité de la mesure de surveillance aux objectifs poursuivis* ».

Par ailleurs elle « *relève que si l'installation de dispositifs de captation de données informatiques demeure une mesure d'investigation exceptionnelle, sa mise en œuvre dans des points d'accès publics d'accès au réseau Internet présente un caractère particulièrement sensible* ».

Enfin, et c'est sans doute l'un des points les plus importants soulevés par la CNIL lors de cette délibération, elle rappelle que le Conseil constitutionnel a considéré, dans sa décision n°2003-467 du 13 mars 2003 relative à la loi pour la sécurité intérieure, qu'il appartenait au législateur *« d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent la liberté d'aller et venir et le respect de la vie privée, protégés par les articles 2 et 4 de la Déclaration des droits de l'homme et du citoyen de 1789, ainsi que la liberté individuelle, que l'article 66 de la Constitution place sous la surveillance de l'autorité judiciaire*. »

Ces craintes ont été entendues et la mention relative aux points d'accès publics à Internet a disparu afin de garantir la proportionnalité de la mesure de surveillance aux objectifs poursuivis comme le désir la CNIL.

Si ces extensions sont significatives, elles ne sont pas sans limites, ce qu'il convient d'étudier.

[99] Délibération n° 2009-200 du 16 avril 2009 portant avis sur sept articles du projet de *loi d'orientation et de programmation pour la performance de la sécurité intérieure*
http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/207/

Section II - Les limites à une extension significative et audacieuse

Ces législations peuvent s'avérer extrêmement préjudiciables pour l'utilisateur puisqu'il peut se voir suspendre sa connexion Internet par le biais de la loi HADOPI, ou se faire espionner à son insu *via* son propre ordinateur. C'est la raison pour laquelle il existe des moyens lui permettant d'éviter d'être pris dans l'engrenage de la procédure de sanction (I) ou de rendre nulle la procédure d'immixtion (II).

I. HADOPI : la diligence de l'utilisateur comme moyen d'exonération

Les moyens d'exonération ont été une difficulté majeure dans la mise en place de la loi HADOPI. Désormais, si la sécurisation de l'accès est un moyen de prouver son innocence (A), des systèmes préventifs peuvent toutefois s'avérer efficaces notamment pour les entreprises (B).

A. Une exonération par la démonstration de la mise en œuvre de la sécurisation de la ligne

Nous avons pu observer que l'utilisateur engageait sa responsabilité sur le fondement de la négligence caractérisée dès lors qu'il n'avait, soit pas sécurisé son accès, soit sécurisé de manière inefficace ou tardive. C'est notamment sur ce point précis que va se concentrer l'un des moyens pour l'utilisateur de prouver son innocence. La question de la charge de la preuve est pour le moins houleuse et ne cesse de faire grand bruit. Dans le cadre de la loi *Création et Internet*, il appartenait à l'utilisateur mis en cause de démontrer qu'un tiers avait détourné sa ligne, entrainant une « *présomption de culpabilité* »[100]. Le Conseil Constitutionnel a rappelé[101] qu'en matière répressive une telle présomption ne peut être instituée, d'où la censure immédiate sur le fondement de la présomption d'innocence. C'est à l'occasion du considérant 19 que le Conseil Constitutionnel pose que cette présomption de culpabilité pouvait « *conduire à prononcer contre (l'utilisateur) des sanctions privatives ou restrictives de droit* » « *en méconnaissance des exigences résultant de l'article 9 de la Déclaration de 1789* »[102].
Hubert Bitan[103] illustre ce mécanisme par l'exemple suivant : « *contrairement aux radars automatiques permettant de sanctionner les automobilistes qui ne respectent pas les limitations de vitesse prévues par le Code la route, l'internaute profane (ou avisé d'ailleurs) qui protège son accès par un code mais dont sa ligne se fait tout de même pirater rapportera difficilement la preuve du contraire. L'automobiliste, pour sa part, pourra faire valoir que son véhicule a été volé et que, par conséquent, il n'est pas l'auteur de l'infraction qu'on lui attribue* ».

En réponse à la censure, il appartient dorénavant à l'autorité de poursuite, soit le ministère public devant le tribunal de police, de prouver que le titulaire de l'accès a failli à son obligation de vigilance. C'est au juge qu'il appartiendra d'apprécier si l'utilisateur a été suffisamment diligent ou non dans la mise en œuvre de la sécurisation de sa connexion. Dans ce cas, pour aider l'utilisateur, l'article L331-26 du CPI prévoit qu' « *au terme d'une procédure d'évaluation certifiée prenant en compte leur conformité aux spécifications visées au premier alinéa et leur efficacité, la Haute Autorité établit une liste labellisant les moyens de sécurisation* ». La Haute autorité précise d'ailleurs que l'utilisation d'un moyen de sécurisation labellisé sera un élément positif dans le cadre de son appréciation des faits si l'internaute est concerné par le processus de réponse graduée.

---

[100] Voir le dossier réalisé par la Quadrature du net : « HADOPI, riposte graduée : une réponse inefficace, inapplicable et dangereuse à un faux problème », v1.0, 9 février 2009, page 6 http://www.laquadrature.net/files/LaQuadratureduNet-Riposte-Graduee_reponse-inefficace-inapplicable-dangereuse-a-un-faux-probleme.pdf
[101] Conseil Constitutionnel, 10 juin 2009, Décision n°2009-580 DC <http://www.conseil-constitutionnel.fr/decision//2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html>
[102] « *Tout homme étant présumé innocent jusqu'à ce qu'il ait été déclaré coupable, s'il est jugé indispensable de l'arrêter, toute rigueur qui ne serait pas nécessaire pour s'assurer de sa personne doit être sévèrement réprimée par la loi* »
[103] Hubert Bitan, Dossier spécial Loi « CREATION ET INTERNET » - Réflexions sur la loi « Création et Internet » et sur le projet de loi « *HADOPI 2* », dans Revue Lamy Droit de l'Immatériel, pages 121 et suivants, n°51, juillet 2009

Pour identifier les différents moyens de sécurisation existants, la Haute autorité est censée attribuer un label permettant de connaître les dispositifs les plus sécurisants, qui répondront à des objectifs de sécurité et d'usages déterminés appelés « *spécifications fonctionnelle »*[104].

Cependant, à ce jour, aucun moyen de sécurisation labellisé n'a été diffusé par la Haute autorité. Sur le site web de cette dernière, une consultation publique[105] a été lancée jusqu'au 30 octobre 2010 « *à toutes les personnes qui pourraient être intéressées par le sujet* ». Il serait bon d'en faire parvenir la liste au plus vite car il est très difficile de savoir à l'heure actuelle si la sécurisation est effective ou non au regard de la loi. Ce vide actuel n'a pas pour autant pour conséquence la création d'une présomption d'irresponsabilité au bénéfice de l'utilisateur puisque celui-ci reste tenu à son obligation de vigilance. Cependant, la démonstration de sa diligence dans le cadre de l'engagement hypothétique de sa responsabilité sera quelque peu aléatoire, incertaine et confuse. Cette absence est donc particulièrement regrettable et préjudiciable à la sécurité juridique sur le terrain probatoire. C'est pourquoi l'utilisateur pourra, si sa responsabilité est engagée, essayer de remettre en cause la procédure. En effet, à chaque étape de la procédure graduée enjoignant l'utilisateur de respecter son obligation de sécurisation, l'article L331-25 du Code de la propriété intellectuelle[106] impose à la commission de protection de l'informer sur "*l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation (de sécurisation)*". Il serait donc envisageable de se prévaloir de ce vice de forme qui pourrait tout à fait entacher de nullité la procédure. L'article L331-26 du Code de propriété intellectuelle pose l'obligation pour la Haute Autorité de « *(rendre) publiques les spécifications fonctionnelles pertinentes que (les) moyens (de sécurisation) doivent présenter* ». L'utilisateur n'ayant aucune possibilité de connaître le niveau d'exigence demandé en matière de sécurisation, le juge pourra donc lui octroyer le bénéfice de la présomption d'innocence.

Enfin, si le parquet parvient malgré tout à prouver le manque de diligence dans la sécurisation de la connexion, l'article R335-5 I 1° du CPI prévoit la possibilité pour le titulaire d'un accès à Internet de s'exonérer de sa responsabilité par un « *motif légitime* ». Toutefois, ledit motif légitime n'est pas défini et sa détermination demeure pour le moins incertaine. On peut dans un premier temps penser aux causes d'irresponsabilité pénale prévues aux articles 122-1 et suivants du Code pénal mais il est vraisemblable que cela puisse s'étendre bien au-delà afin d'adapter la diversité de situation des utilisateurs. Il appartiendra à la jurisprudence d'en définir les contours mais on peut imaginer que les points d'accès publics puissent en bénéficier dans la mesure où le nombre d'utilisateurs de la ligne peut ne pas être négligeable. On peut aussi se poser la question du novice en informatique qui ne connait absolument rien à la matière. Il y a pléthore de circonstances et les interrogations seront certainement légion mais il faudra trouver un juste équilibre afin que l'utilisateur ne puisse pas se défaire trop facilement de son obligation.

[104] La rédaction de ces spécifications a été confiée à Michel Riguidel, expert et professeur à l'école Télécom-ParisTech.
[105] <http://www.hadopi.fr/download/sites/default/files/page/pdf/Consultation_sur_les%20specifications_fonctionnelles_des_moyens_de_securisation.pdf>
[106] Article L331-25 du Code de la propriété intellectuelle Article L331-25 Modifié par LOI n°2009-1311 du 28 octobre 2009 – art. 3 et 12
<http://legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006069414&idArticle=LEGIARTI000020740325>

B. Des moyens de prévention au secours de moyens d'exonération nébuleux

Outre les moyens de sécurisation de l'accès, il semble qu'il y ait peu de possibilités pour l'utilisateur permettant de s'exonérer de sa responsabilité. Mis à part la démonstration que l'accès a été utilisé frauduleusement ou la démonstration de la force majeure[107] traditionnelle, très peu de portes de sorties s'offrent à lui, d'autant plus que ces derniers moyens seront extrêmement difficiles à rapporter et relèveront certainement de la « *probatio diabolica* »[108].

Pour y remédier, il convient de jouer la carte de la prévention. C'est d'ailleurs pour les entreprises que plusieurs réponses ont été apportées. Par exemple, il est recommandé de mettre en place un système de filtrage qui s'avère être une « *solution unifiée des postes de travail*[109] » regroupant un antivirus classique ainsi que d'autres services complémentaires permettant de réguler l'accès aux sites de téléchargement et filtrer les contenus transitant par le biais de la connexion Internet de l'entreprise. Ainsi par exemple, il sera impossible de télécharger des fichiers contenant les extensions suivantes : .mp3, .avi ou encore .wma qui visent les contenus musicaux.

Il est également recommandé aux entreprises de paramétrer leur pare-feu afin d'empêcher la bonne application de logiciels de « *peer to peer* » désormais bien connus du grand public. Ce système permet par exemple un blocage de certaines applications et peut rendre l'accès impossible aux serveurs de « *téléchargements directs* » (à savoir *Megaupload, Rapidshare*, etc.) ou aux serveurs de « *peer to peer* ».

Ces moyens de filtrage permettront d'attester des diligences accomplies par l'entreprise dans le but de sécuriser sa connexion Internet. Cependant, malgré une sécurité du réseau de l'entreprise renforcée, ces efforts auront un coût pour l'entreprise qui sera certainement le prix de son innocence.
Il existe une autre limite qui concerne le droit des données à caractère personnelle puisque les moyens devront être proportionnés au but recherché et en conformité avec la loi HADOPI. Certains juristes soulignent en effet que des procédés de surveillance appliqués pour surveiller les temps de pause ou les boîtes mail des salariés ne pourront pas être utilisés devant la Haute juridiction, car « *l'objectif initial étant de faire cesser les atteintes au droit d'auteur, la mesure portant atteinte de manière disproportionnée à la vie privée du salarié sera considérée comme illégitime, inadaptée et donc non conforme à la Loi* [110]».

De manière moins coûteuse et plus traditionnelle, l'entreprise pourra se doter d'une Charte d'utilisation d'Internet et des systèmes d'informatique en général. Celle-ci doit être annexée au règlement intérieur et permettra de circonscrire les usages faits d'Internet au sein de l'entreprise. Selon la CNIL, elle permettra de sensibiliser les salariés « *à un usage raisonnable, non susceptible d'amoindrir les conditions d'accès professionnel au réseau et ne mettant pas en cause la productivité* ».

---

[107] Il faudra alors démontrer, conformément à une jurisprudence constante et comme l'a réaffirmé pour la matière extracontractuelle la Cour de cassation dans un arrêt rendu en Assemblée Plénière le 14 avril 2006, que l'évènement était irrésistible et imprévisible.
[108] « *Preuve diabolique* » dite impossible à rapporter
[109] <http://www.commentcamarche.net/faq/28041-hadopi-les-consequences-pour-l-entreprise>
[110] <http://www.lexatic.com/droit-du-travail-dans-un-environnement-numerique/lapplication-de-la-loi-hadopi-par-les-entreprises-et-la-suspension-de-leur-connexion-internet.html>

II. LOPPSI 2 : des cas de recours limités

La LOPPSI 2 n'offre par nature pas de moyens d'exonération à l'utilisateur puisqu'il s'agit en l'espèce de rechercher des preuves de culpabilité. C'est la raison pour laquelle il faut se rattacher aux cas de nullité de la procédure (A). Cependant, si cette limite peut s'avérer très efficace dans la mesure où les enquêteurs ont manqué de rigueur dans la mise en place de la procédure, le cas des opérations incidentes peut rapidement étendre les limites au-delà de ce qui était prévu initialement (B).

A. Une procédure dépendant d'une parfaite rigueur

Afin de rendre caduque la procédure, il n'existe que les cas de nullité (1) et un cas d'irrecevabilité (2).

1. Les cas de nullité de la procédure

Le détournement de la connexion Internet de l'utilisateur est une mesure grave qui met en péril le droit à la vie privée comme nous l'analyserons ce qui par conséquent nécessite une délimitation précise. La captation des données à distance n'y fait pas exception et comme dans toute procédure, il est capital de respecter strictement l'ensemble des formalités qui vont appuyer l'enquête et dessiner les contours. C'est notamment par ce biais que l'avocat de l'utilisateur mis en cause devra travailler sa défense pour soulever la nullité de la procédure.

C'est l'article 706-102-2 du CPP[111] qui vient définir à peine de nullité les éléments qui vont motiver les décisions prises par le juge d'instruction. Ainsi, il sera nécessaire de préciser l'infraction qui motive le recours de chaque opération, la localisation exacte ou la description détaillée des systèmes de traitement automatisé de données ainsi que la durée des opérations.

Outre ces formalités préliminaires, le juge d'instruction ou l'officier de police judiciaire commis par lui devront par la suite dresser un procès verbal pour chaque opération qui a nécessité une mise en place du dispositif technique et des opérations de captation de données informatiques[112]. Ce procès verbal devra faire état de toutes les données utiles à la manifestation de la vérité. Celui-ci devra également faire mention de la date et de l'heure de début et de fin desdites opérations, et l'ensemble des données informatiques qui auront été recueillies seront placées sous scellés fermés afin de conserver les pièces à conviction à la disposition de la justice.

2. Le cas d'irrecevabilité

Enfin, les données informatiques recueillies dans le cadre de la captation de données informatiques ne doivent pas être gardées pour une durée indéterminée par les enquêteurs. Il est prévu à l'article 706-102-9 du Code de procédure pénale que les enregistrements des données informatiques soient détruits à la date de prescription de l'action publique, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique. Il est cependant reproché sur ce point que l'effacement total des données est difficile car il reste bien souvent des traces plus ou moins conséquentes. C'est certainement pour cette raison que le législateur a tenu à préciser malgré tout cette obligation, afin que ces traces soient inutilisables.

---

[111] Article 706-102-2 – Code de procédure pénale créé par LOI n°2011-267 du 14 mars 2011 - art.36 <http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=E7AB76DEDEF87E26992386FB7156A6ED.tpdjo15v_1?idArticle=LEGIARTI000023712500&cidTexte=LEGITEXT000006071154&dateTexte=20110817&categorieLien=id>

[112] Article 706-102-7 du Code de Procédure pénale créé par LOI n°2011-267 du 14 mars 2011 - art. 36 <http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=BABFE6065C8935109A390509054CF405.tpdjo15v_1?idArticle=LEGIARTI000023712510&cidTexte=LEGITEXT000006071154&dateTexte=20110817&categorieLien=id>

B. Le cas des opérations incidentes

Une question peut rapidement être mise en exergue : quid des infractions relevées dans le cadre de l'enquête qui n'ont pas été préalablement spécifiées dans le cadre des motivations de la décision du juge d'instruction ? Ceci d'autant plus que l'article 706-102-4 du Code de procédure pénale[113] prévoit expressément que les opérations mises en œuvre ne peuvent avoir un autre objet que la recherche et la constatation des infractions visées dans les décisions du juge d'instruction. En effet, bon nombre d'informations de différentes natures transitent sur l'écran de l'utilisateur et il n'est certainement pas rare que d'autres infractions se révèlent aux yeux des enquêteurs.

C'est pourtant le même article 706-102-4 qui prévoit ce cas et pose expressément « *le fait que ces opérations révèlent des infractions autres que celles visées dans ces décisions ne constitue pas une cause de nullité des procédures incidentes* ».

Selon certains spécialistes[114], ce système permettra de sanctionner toutes les infractions qui auront été constatées à l'occasion de cette surveillance, même si cela ne concerne pas des infractions commises en bande organisée. En effet, si de nouveaux éléments sont découverts il est tout à fait envisageable d'engager une nouvelle procédure notamment par le biais d'un réquisitoire supplétif auprès du procureur de la République[115].

En somme, cette limite demeure pour le moins ambigüe en ce qu'elle cadre suffisamment la procédure de captation de données informatiques mais n'exclut pourtant pas de prendre en compte de nouvelles infractions qui pourront faire l'objet de poursuites.

Conclusion

Il est désormais certain que l'utilisateur est au centre des préoccupations du législateur qui a pris conscience de la place fondamentale occupée par ce dernier. Acteur premier de l'univers numérique, il est, au sens général, un nouveau moyen de combattre les infractions. A la condition de l'identifier, il est possible de lui inculquer l'obligation de contrôler l'usage de sa ligne pour combattre les téléchargements illicites et de le sanctionner le cas échéant en lui ôtant toute possibilité d'accéder à ce réseau mondial. A la même condition, il est aussi possible de détourner la ligne pour des raisons d'investigation. A priori, tout semble en ordre puisque l'utilisateur a la possibilité de s'exonérer de sa responsabilité dans le cadre de la riposte graduée et a également la possibilité de rendre nulle ou irrecevable une procédure qui ne respecte pas les formalités nécessaires. Les limitations de ces atteintes sont nécessaires à la protection du mis en cause.

Cependant, elles peuvent s'avérer insatisfaisantes. La raison première concerne leur incertitude puisque les moyens de sécurisation labellisés du dispositif HADOPI n'ont toujours pas été publiés et que les opérations incidentes dans le cadre de la LOPPSI 2 risquent d'augmenter le nombre d'infractions à la charge de l'utilisateur. Par ailleurs, ces simples limitations ne sont pas insuffisantes en tant que telles. Nous verrons que les droits de l'utilisateur vont être mis en péril et que plusieurs obstacles seront abordés. Dès lors un certain

---

[113] Article 706-102-4 du Code de procédure pénale créé par LOI n°2011-267 du 14 mars 2011 - art. 36 <http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=BABFE6065C8935109A390509054CF405.tpdjo15v_1?idArticle=LEGIARTI000023712504&cidTexte=LEGITEXT000006071154&dateTexte=20110817&categorieLien=id>

[114] Myriam Quéméner, « Projet de *loi d'orientation et de programmation pour la performance de la sécurité intérieure* (LOPPSI 2) : les réponses en matière de cybercriminalité », dans Communication Commerce électronique n°11, pages 2-3, Novembre 2010, alerte 101

[115] Article 80 du Code de procédure pénale : Lorsque des faits, non visés au réquisitoire, sont portés à la connaissance du juge d'instruction, celui-ci doit immédiatement communiquer au procureur de la République les plaintes ou les procès-verbaux qui les constatent. Le procureur de la République peut alors soit requérir du juge d'instruction, par réquisitoire supplétif, qu'il informe sur ces nouveaux faits, soit requérir l'ouverture d'une information distincte, soit saisir la juridiction de jugement, soit ordonner une enquête, soit décider d'un classement sans suite ou de procéder à l'une des mesures prévues aux articles 41-1 à 41-3, soit transmettre les plaintes ou les procès-verbaux au procureur de la République territorialement compétent. Si le procureur de la République requiert l'ouverture d'une information distincte, celle-ci peut être confiée au même juge d'instruction, désigné dans les conditions prévues au premier alinéa de l'article 83.

nombre d'institutions doivent intervenir afin d'apporter de véritables garanties à l'utilisateur qui ne sera, malgré tout, pas à l'abri de menaces.

Titre II - Conséquences et critiques d'une extension à la légitimité controversée

Les lois qui font l'objet de notre étude doivent se confronter à des difficultés de différentes natures. Nécessitant le recours à la connexion Internet, la technique est une problématique inévitable et le droit peut parfois peiner à s'y adapter (chapitre I). Ces éléments vont d'ailleurs provoquer une crise de légitimité engendrant des incertitudes quant à l'effectivité des lois (chapitre II).

Chapitre I - Une effectivité contestable au regard du droit et de la technique

Les atteintes portées à la connexion Internet de l'utilisateur vont doivent nécessairement être garanties et circonscrites à un périmètre délimité. Confrontées aux libertés et droits fondamentaux (section I), elles devront également faire face à des difficultés à la fois techniques et juridiques de taille (section II).

Section I - Une délicate conciliation des extensions avec les libertés et droits fondamentaux

La loi HADOPI tout d'abord, en sanctionnant l'accès à l'un des principaux moyens d'expression va susciter de vifs débats. En effet, les détracteurs de ce nouveau dispositif législatif n'ont pas hésité à le juger disproportionné au regard de l'objectif poursuivi. L'apport du Conseil constitutionnel va s'avérer essentiel en érigeant l'accès à Internet en tant que *« composante de la liberté d'expression »*[116]. Cependant, il ne paraît pas évident de concilier une telle composante avec une sanction aussi drastique (I).

La loi HADOPI rejoint la LOPPSI 2 sur le thème de l'immixtion dans la vie privée. En effet, il est recouru dans le premier cas à un logiciel espion afin de contrôler les contenus transitant par le biais de la connexion Internet, tandis que dans l'autre cas le logiciel permet de récupérer des données informatiques. La conciliation avec le droit à la vie privée peut alors s'avérer conflictuelle (II).

I. Une sanction difficilement conciliable avec un accès à Internet reconnu comme « *composante de la liberté d'expression* »

Concernant la connexion Internet, le projet de loi HADOPI a suscité de vives critiques (A) nécessitant ainsi de véritables garanties par l'intermédiaire du juge judiciaire (B).

A. Des contestations aux fondements multiples

Les contestations qui se sont élevées relevaient principalement de deux ordres à savoir la sanction elle-même (1) et la possibilité pour une autorité administrative de la prononcer (2).

1. Une sanction contestée

La sanction de la suspension de l'accès à Internet est une sanction qui fut et reste à ce jour contestée sous différents aspects. En effet, comme nous l'évoquions, tout utilisateur manquant à son obligation de vigilance est passible de se voir retirer sa connexion Internet. Cependant la diversité des utilisateurs (particuliers, professionnel, collectivités territoriales, etc.) est une complication qui subsiste et qui mérite réflexion.

A propos de l'utilisateur lui même, est contesté le fait que la sanction s'applique également à l'ensemble des autres individus qui avaient accès à ladite connexion. Ainsi, une famille, une entreprise ou tout un ensemble

[116] Conseil constitutionnel - Décision n° 2009-580 DC du 10 juin 2009 <http://www.conseil-constitutionnel.fr/decision//2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html>

d'étudiants peuvent se voir suspendre leur connexion à Internet du fait d'un manquement répété à une obligation de vigilance.

Le choix de la sanction est en lui-même discuté. Si l'accès à Internet est à ce point incontournable, est-il légitime de choisir cette sanction ? Internet est un outil contemporain d'information et de communication essentiel à tel point que tout se fait désormais par voie numérique (comme répondre à un appel d'offre, s'inscrire à certains concours, déclarer ses impôts, consulter ses comptes, etc.). Il est alors disproportionné de s'en prendre à un moyen aussi largement répandu au bénéfice du respect du droit d'auteur.

Enfin, est reproché le mécanisme de la « *double pleine* » par lequel le titulaire de l'accès doit continuer malgré la sanction à payer le service pendant la durée de la suspension, sauf cas de résiliation. En effet, la sanction de la suspension d'Internet étant déjà particulièrement conséquente, il semble excessif de condamner en plus l'utilisateur à cette seconde sanction.

Les députés de l'opposition ont invoqué parmi leurs moyens de saisine du Conseil constitutionnel le fait que la coupure de l'accès à Internet affecterait l'exercice de la liberté d'expression, l'accès à la culture, le droit à l'éducation et la liberté d'entreprendre et nous analyserons en quelle mesure cette sanction doit être garantie.

2. Un organe à l'origine du prononcé de la sanction contesté

En cas de manquements répétés à l'obligation de vigilance malgré l'envoi d'un premier mail d'avertissement et d'une lettre recommandée, il était prévu dans le projet de Loi « *HADOPI 1* » la possibilité pour la Commission de protection des droits de la HADOPI de suspendre l'accès à Internet pendant un délai s'étendant de deux mois à un an.

L'organe prononçant la sanction est l'un des grands points qui sera contesté devant le Conseil Constitutionnel. La doctrine émet d'ailleurs ses premières inquiétudes[117] à ce sujet dès la publication du projet de Loi en attirant l'attention sur le fait que « *l'éviction du juge est sans doute l'un des éléments les plus déroutants du projet de loi* » puisque le « *juge judiciaire est le gardien naturel des libertés individuelles et du droit de propriété* ».

Par ailleurs, en mai 2009, le « *Paquet Telecom* » voté par le Parlement consacre l'accès à Internet au rang des droits fondamentaux[118] obligeant ainsi l'autorité judiciaire à prononcer la sanction de suspension de l'accès Internet.

Enfin, une résolution du 10 avril 2008 des eurodéputés engage les membres « *à éviter l'adoption de mesures allant à l'encontre des droits de l'homme, des droits civiques et des principes de proportionnalité, d'efficacité et d'effet dissuasif, telles que l'interruption de l'accès à Internet* ».

Malgré l'ensemble de ces considérations, le texte fut adopté en l'état. Il est alors principalement invoqué devant le Conseil Constitutionnel deux volets différents à savoir la disproportion de la sanction d'une part, et le fait que le prononcé d'une telle sanction devrait relever uniquement de la compétence du juge judiciaire d'autre part.

[117] Voir l'article collectif réunissant onze coauteurs tels que Mélanie Clément-Fontaine (maître de conférence à l'Université de Versailles - Saint-Quentin), Gilles Vercken (avocat), Michel Vivant (professeur à Sciences Po) – « DADVSI 2, HADOPI, « Création et internet »... De bonnes questions? De mauvaises réponses », dans Recueil Dalloz 2008, p. 2290

[118] Amendement 138/46 qui a, depuis l'adoption du « *Paquet Telecom* » le 24 novembre 2009, été amoindri et ne comporte plus cette mention

B. L'encadrement d'une sanction garantie par le juge judiciaire

C'est à l'occasion du contrôle de la loi au regard de la Constitution que le Conseil constitutionnel semble bien avoir érigé l'accès à Internet au rang des droits fondamentaux (1) impliquant nécessairement « rejudiciarisation » de la procédure afin d'apporter de véritables garanties quant au prononcé de la sanction (2).

1. L'avènement d'une nouvelle composante à la liberté de communication ?

Lors de la saisine du Conseil constitutionnel dans le cadre du projet de loi « *HADOPI 1* » s'est posée la problématique de la conciliation entre la sanction de la coupure de l'accès à Internet et le droit de propriété intellectuelle des auteurs. En réalité, il va vite devenir question de concilier la sanction avec une nouvelle composante de la liberté d'expression, l'accès à Internet étant un moyen d'information et de communication incontournable à ce jour.

Le Conseil constitutionnel a eu un apport très innovant dans sa décision 2009-580 DC du 10 juin 2009[119]. Il a ainsi établi dans le cadre de ses considérants 12 et 13 *« qu'aux termes de l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 : "La libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme" […] qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services ;*

Considérant que la propriété est au nombre des droits de l'homme consacrés par les articles 2 et 17 de la Déclaration de 1789 ; que les finalités et les conditions d'exercice du droit de propriété ont connu depuis 1789 une évolution caractérisée par une extension de son champ d'application à des domaines nouveaux ; que, parmi ces derniers, figure le droit, pour les titulaires du droit d'auteur et de droits voisins, de jouir de leurs droits de propriété intellectuelle et de les protéger dans le cadre défini par la loi et les engagements internationaux de la France ; que la lutte contre les pratiques de contrefaçon qui se développent sur internet répond à l'objectif de sauvegarde de la propriété intellectuelle ».

Le Conseil Constitutionnel, s'inspirant de la jurisprudence de la Cour européenne des droits de l'homme relative à la liberté d'expression[120], semble bien ériger l'accès à Internet en tant que composante de la liberté de communication par extension de l'article 11 de la Déclaration des droits de 1789. Selon certains, il serait même consacré « *en quelque sorte, au nom de la liberté de communication, (une) « liberté d'accéder » à l'Internet (en tant que) droit fondamental* »[121]. D'autres demeurent plus prudents en posant qu' « *il n'a aucunement consacré en l'espèce un prétendu droit fondamental à l'internet, se contentant d'étendre la protection constitutionnelle renforcée de la liberté de communication à ses modalités contemporaines d'exercice* »[122].

Au titre de composante de la liberté d'expression, le Conseil pose au considérant 15 que « *les atteintes portées à l'exercice de cette liberté doivent être nécessaires, adaptées et proportionnées à l'objectif poursuivi »*, ce qu'il a reconnu dans sa décision du 22 octobre 2009[123]. Cependant selon le considérant

---

[119] Conseil Constitutionnel - Décision n° 2009-580 DC du 10 juin 2009 <http://www.conseil-constitutionnel.fr/decision//2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html>

[120] Voir notamment Derieux, E. et Granchet, A., « Jurisprudence de la Cour européenne des droits de l'Homme », Droits des médias. Droit français, européen et international, LGDJ, 5e éd., 2008, p.945-962

[121] Emmanuel Derieux et Agnès Granchet – « Lutte contre le téléchargement illégal - Loi Dadvsi et Hadopi »

[122] A. Gautrons – « "La riposte graduée" (à nouveau) épinglée par le Conseil Constitutionnel. Ou la délicate adéquation des moyens aux fins », RLDI/51, juillet 2009 p.66)

[123] Conseil Constitutionnel – Décision n°2009-590 DC du 22 octobre 2009 – *« l'instauration d'une peine complémentaire destinée à réprimer les délits de contrefaçon commis au moyen d'un service de communication au public en ligne et consistant dans la suspension de l'accès à un tel service pour une durée maximale d'un an, assortie de l'interdiction de*

suivant, la suspension de l'accès à Internet peut « *conduire à restreindre l'exercice par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile* ». C'est pour cette raison que le Conseil constitutionnel déclare inconstitutionnel les articles instituant la Commission de protection des droits à couper l'accès à Internet, puisqu'elle n'est pas une juridiction.

Quoi qu'il en soit, il est tout de même question de suspendre un accès à un moyen d'expression très largement répandu ce qui nécessite des garanties, chose que le Conseil Constitutionnel saura également rappelé.

Enfin, concernant la sanction elle-même, le Conseil Constitutionnel a considéré au considérant 21 qu'elle « *ne méconnait pas le principe de nécessité des peines* » pour en conclure au considérant 31 qu'elle n'est donc pas « *manifestement disproportionnée* ».

2. Une nécessaire « rejudiciarisation » de la procédure

Prenant en compte l'importance du moyen de communication en jeu comme composante de la liberté d'expression, le Conseil constitutionnel déclare, dans sa même décision du 10 juin 2009, contraire à la Constitution les articles autorisant la coupure de l'accès à l'Internet par la Commission des droits qui demeure une autorité administrative et non une juridiction. En effet, il pose en son considérant 16 que le législateur « *ne pouvait confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins* ».

On assiste dans le cadre de la loi HADOPI 2 du 28 octobre 2009 à une « *rejudiciarisation* » du prononcé des sanctions afin d'apporter de véritables garanties, respecter les principes fondamentaux du droit et satisfaire les exigences du Conseil constitutionnel. La peine complémentaire étant considérée comme pouvant porter atteinte à la liberté de communication, il revient à l'autorité judiciaire de la prononcer. Ainsi, il est possible de statuer soit à juge unique selon une procédure traditionnellement contradictoire pour les délits de contrefaçon « *commis au moyen d'un service de communication au public en ligne* » conformément à l'article 398-1 du Code de procédure pénale[124] et une procédure simplifiée via le recours à l'ordonnance pénale prévue aux nouveaux articles 495 à 495-6 du Code de procédure pénale[125]. La suspension de l'accès internet peut en outre et à titre de peine complémentaire être prononcée tant pour des faits de contrefaçon que pour « *négligence caractérisée* » dans la surveillance de l'usage fait de la connexion Internet.

C'est donc au juge qu'il reviendra d'apprécier si la peine complémentaire doit s'appliquer. Pour garantir la proportionnalité de la durée de la sanction et de son quantum, celui-ci dispose d'une marge de manœuvre, l'article L.335-7-2 du CPI[126] disposant sur ce point que « *la durée de la peine prononcée doit concilier la protection des droits de la propriété intellectuelle et le respect du droit de s'exprimer et de communiquer librement, notamment depuis son domicile* ».

En outre, il devra prendre en compte « *les circonstances et la gravité de l'infraction ainsi que la personnalité de son auteur, et notamment l'activité professionnelle ou sociale de celui-ci, ainsi que sa situation socio-économique* ».

Ce dernier aspect permet d'apporter une réelle garantie face aux craintes des utilisateurs dont la diversité a été démontrée plus haut. Certains parlent d'un *« vrai rempart contre le prononcé massif de cette peine*

---

souscrire pendant la même période un autre contrat (…) ne méconnaît pas le principe de nécessité des peines ». Il en conclut que la peine n'est pas « manifestement disproportionnée » et, en conséquence, que l'article en cause « *n'est pas contraire à la Constitution* »

[124] Article 398-1 du Code de procédure pénale <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000023717726&cidTexte=LEGITEXT000006071154&dateTexte=20110818&oldAction=rechCodeArticle>

[125] Article 495 du Code de procédure civile <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006410769&cidTexte=LEGITEXT000006070716&dateTexte=20110818&fastPos=1&fastReqId=730226478&oldAction=rechCodeArticle>

[126] Article L335-7-2 du CPI créé par LOI n°2009-1311 du 28 octobre 2009 - art. 9 <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000021212160&cidTexte=LEGITEXT000006069414&dateTexte=20110818&oldAction=rechCodeArticle>

complémentaire tant le pouvoir d'appréciation du juge est rigoureusement encadré[127] ». Il est essentiel que la peine complémentaire de suspension de l'accès Internet ne soit pas systématiquement prononcée. Par exemple, si une entreprise vient à être enrôlée dans ce type de procédure, il y a fort à parier que le juge modulera la sanction en prenant en compte le fait qu'elle est actrice de l'économie et que sa survie demeure fondamentale. En somme, le juge a la faculté d'appliquer cette peine et il serait surprenant de mettre en péril son fonctionnement à cause d'une infraction commise par un seul salarié. Il est également vraisemblable que les collectivités territoriales, les universités ou les bibliothèques ne devraient en théorie pas être inquiétées bien qu'elles soient effectivement passibles d'une telle sanction, ou alors il faudrait que les « *circonstances soient exceptionnelles* »[128].

Malgré cette garantie juridictionnelle, cette sanction demeure cependant contestée au rang mondial. Dans un rapport rendu public le 2 juin 2011[129], l'ONU demande aux différents Etats de modifier ou d'abroger leur législation afin que les internautes ne soient pas sanctionnés par le biais de la suspension de leur accès, et ce même au nom de la propriété intellectuelle, et de s'abstenir de promulguer de telles lois. L'article 19, paragraphe 2 du Pacte International relatif aux Droits Civiques et Politiques pose en effet que « *toute personne a droit à la liberté d'expression; ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen de son choix* ».

Le Rapporteur Spécial considère en effet que « *couper des utilisateurs de l'accès à Internet, quelle que soit la justification avancée, y compris pour des motifs de violation de droits de propriété intellectuelle, est disproportionné et donc contraire à l'article 19, paragraphe 3, du Pacte International relatif aux Droits Civiques et Politiques* ».

II. Une atteinte par le biais de témoin de connexion difficilement conciliable avec le droit au respect à la vie privée

Le droit à la vie privée est reconnu de toutes parts, à commencer au niveau international, puisqu'il est protégé par l'article 12 de la déclaration universelle des droits de l'homme de 1948. De la même façon, la Cour Européenne des droits de l'Homme se réfère à l'article 8 de la Convention européenne des droits de l'homme. Egalement, la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 prévoit dès sont préambule « *qu'il est souhaitable d'étendre la protection des droits et des libertés fondamentales de chacun, notamment le droit au respect de la vie privée, eu égard à l'intensification de la circulation à travers les frontières des données à caractère personnel faisant l'objet de traitements automatisés* ». En matière de droit de l'union européenne, le droit des données personnelles est protégé par l'article 8 de la Charte des droits fondamentaux de l'Union européenne130, ceci d'autant plus que le traité de Lisbonne du 13 décembre 2007 prévoit en son article 6.1 que « *l'Union reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, telle qu'adaptée le 12 décembre 2007 à Strasbourg, laquelle a la même valeur juridique que les traités* ». Enfin, en droit interne, le Conseil constitutionnel considère que le droit à la vie privée découle implicitement du principe constitutionnel de la liberté individuelle garantie par l'article 66 de la Constitution, et de la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789. Il a pu trancher et confirmer sa position à l'occasion de plusieurs décisions[131]. Cependant il n'existe pas de définition

---

[127] Nicolas Catelan, « La protection du droit d'auteur : une négligence caractérisée ? », dans Revue Lamy Droit de l'Immatériel, n°67, pages 81-83, janvier 2011

[128] <http://www.numerama.com/magazine/18848-l-acces-a-internet-dans-les-bibliotheques-menace.html>

[129] <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>

[130] L'article 8 de la Charte des droits fondamentaux de l'Union européenne prévoit que :

1. Toute personne a droit à la protection des données à caractère personnel la concernant

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante

[131] Le Conseil constitutionnel dans sa décision 99-416 DC du 23 juillet 1999, en affirmant dans son considérant 45 sur la carte vitale que « *la liberté proclamée par (l'article 2 de la Déclaration des droits de l'homme et du citoyen implique le respect de la vie privée ».* Dans sa décision n° 94-352 DC du 18 janvier 1995, le Conseil constitutionnel avait déjà

légale de la vie privée, c'est pour cette raison qu'il appartient à la jurisprudence d'en définir le contenu. Cette dernière se fonde généralement en matière civile sur l'article 9 du Code civil qui pose que « *toute personne a le droit au respect de sa vie privée », tandis qu'en matière pénale l'article 226-1 du Code pénal prévoit une peine d'un an d'emprisonnement et de 45000 euros d'amende « le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui* ».

Afin de mettre en application les lois HADOPI et LOPPSI 2, il a été nécessaire que le législateur permette l'utilisation de logiciels espions (A). Ce moyen fortement intrusif met en péril le droit à la vie privée, c'est pourquoi il a fallu l'encadrer par le contrôle de différentes autorités (B).

A. Une infiltration législativement reconnue

Bien qu'œuvrant pour des objectifs différents, la loi LOPPSI 2 (1), comme les lois HADOPI (2) impliquent l'utilisation de témoins de connexion.

1. Le logiciel espion mis en œuvre par la loi LOPPSI 2

Dans le cadre de cette loi, le moyen semble particulièrement intrusif. En effet, il s'agit de témoin de connexion, plus communément appelé « *mouchard* » ou « *cheval de Troie* » et dont l'équivalent étranger se nomme « *cookie* ». On en trouve la définition dans un Avis de la Commission générale de terminologie et de néologie[132] en le désignant comme une appliquette envoyée par un serveur de la toile mondiale à un utilisateur, parfois à l'insu de celui-ci, au cours d'une connexion, afin de caractériser cet utilisateur. Par extension, cela désigne également l'information que l'appliquette peut enregistrer sur le disque de l'utilisateur et à laquelle le serveur peut accéder ultérieurement. C'est donc par le biais de ce témoin de connexion que les officiers de police judiciaire vont pouvoir requérir les enregistrements des données informatiques à l'insu de l'intéressé, elles mêmes placées sous scellées et retranscrites dans un procès verbal qui sera versé au dossier. Cependant, comme nous l'avons étudié, il est fondamental que seules les données « *utiles à la manifestation de la vérité* » fassent l'objet de cette démarche.

Au stade du projet de loi, ce dernier point a suscité des inquiétudes de la CNIL car le fait que soient placés sous scellés « *les enregistrements de données informatiques* » sans autre distinction aurait pu amener à des dérives[133]. En effet, l'expression est suffisamment large pour englober toutes les informations et non pas uniquement celles « *utiles à la manifestation de la vérité* ». Or, le Conseil constitutionnel a déjà précisé le 2 mars 2004[134] dans le cadre de son examen de la loi portant adaptation de la justice aux évolutions de la criminalité que « *l'article 706-101 nouveau du code de procédure pénale limite aux seuls enregistrements utiles à la manifestation de la vérité le contenu du procès-verbal* » et que « *le législateur a nécessairement entendu que les séquences de la vie privée étrangères aux infractions en cause ne puissent en aucun cas être conservées dans le dossier de la procédure* ». On peut donc se féliciter de cette limite suffisamment affinée pour ne pas craindre des dérives. Ceci d'autant que la loi précise expressément qu' « *aucune séquence relative à la vie privée étrangère aux infractions visées dans les décisions autorisant la mesure ne pourra être conservée dans le dossier de la procédure* ».

---

considéré que *« la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle »*. Dans sa décision plus récente n° 2008-562 DC du 21 février 2008, il a affirmé que *« la liberté d'aller et venir et le respect de la vie privée, protégés par les articles 2 et 4 de la Déclaration de 1789 »,* faisaient partie des libertés constitutionnellement garanties.

[132] Publié au Vocabulaire de l'informatique et de l'Internet – Journal Officiel du 16 mars 1999

[133] <http://www.zdnet.fr/actualites/loi-loppsi-2-la-cnil-craint-des-derives-39703031.htm+tout+type+de+point+d%E2%80%99acc%C3%A8s+public+%C3%A0+Internet+lopssi+2+2011&cd=1&hl=fr&ct=clnk&gl=fr&source=www.google.fr>

[134] Décision n° 2004-492 DC du 02 mars 2004 - Loi portant adaptation de la justice aux évolutions de la criminalité, Journal officiel du 10 mars 2004, p. 4637, Recueil, p. 66
<http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/depuis-1958/decisions-par-date/2004/2004-492-dc/decision-n-2004-492-dc-du-02-mars-2004.897.html>

Cependant, il faut se montrer prudent car rien n'indique que les informations perçues par les enquêteurs ne pourront pas donner lieu à des poursuites. En effet, si une pratique illégale autre que celle pour laquelle la procédure a été engagée est constatée, les enregistrements ne pourront peut-être pas être utilisées dans le cadre de la procédure en question, mais il y a fort à parier que le mis en cause sera inquiété par le biais d'un réquisitoire supplétif auprès du Procureur de la République comme nous l'avons plus haut[135].

Dans la même veine, la CNIL s'est inquiétée[136] du fait que « *le dispositif vise à capter en continu des données informatiques utilisées ou saisies sur un ordinateur, que ces données soient ou non destinées à être émises, et qu'elles empruntent ou non un réseau de communications électroniques* ». En effet, cette captation engendre à nouveau le risque de recueillir des informations qui ne soient pas « *utiles à la manifestation de la vérité* ». Sur ce point, elle s'appuie sur une décision du 27 février 2008 de la Cour constitutionnelle allemande (*Bundesverfassungsgericht*[137]) qui a invalidé les dispositions d'une loi permettant à un service spécialisé d'opérer une surveillance d'internet et de procéder à des perquisitions en ligne[138].

Dans le cadre de cette décision, la Cour analyse le fait que les perquisitions en ligne menacent de façon inédite les droits des individus car elles permettent à un enquêteur de bénéficier d'une somme d'informations extrêmement large dont l'étendue est incomparable avec tout ce qu'elle a pu connaître dans sa jurisprudence antérieure. C'est pourquoi la Cour a dégagé un principe général de garantie de la confidentialité et de l'intégrité des systèmes informatiques, lequel est rattaché au droit de la personnalité afin de permettre une meilleure protection des internautes face aux lacunes du droit applicable et à la croissance des nouvelles technologies. Ainsi, ce nouveau principe n'est pas absolu et doit être concilié avec les objectifs liés à la lutte contre la cybercriminalité. Ce point permet de préciser dans quels cas l'intrusion de témoins de connexions est ainsi possible. Des perquisitions en ligne peuvent être mises en œuvre mais « *uniquement face à une situation présentant des indices concrets démontrant l'existence d'un danger réel menaçant un droit d'un importance extrême* »[139]. Ainsi, constituent, selon la Cour, des droits d'une telle importance « *l'intégrité physique, la vie, la liberté d'une personne ou encore des biens communs d'une importance telle que leur mise en danger affecterait l'existence ou les fondements de l'Etat, voire les bases mêmes de l'existence humaine* » ce qui est pour le moins restrictif conformément au principe d'interprétation de la loi pénale.

En résumé, selon cette jurisprudence, dans un premier temps, les perquisitions en ligne doivent donc être autorisées par un juge. En outre, ces perquisitions en ligne ne sont permises par la Cour Constitutionnelle de Karlsruhe que pour deux motifs : menaces concrètes contre la vie humaine, menaces concrètes contre l'Etat. Enfin, les données recueillies lors de ces cyberperquisitions ne pourront pas être utilisées par la justice si elles touchent à la vie privée des suspects.

Malgré cette référence à une jurisprudence au combien innovante de la Cour constitutionnelle de Karlsruhe, la lettre de l'article 706-102-1 du Code de procédure pénale est restée inchangée. Il ne reste pour garde fou que l'obligation de collecter des données utiles à la manifestation de la vérité excluant ainsi les risques de dérives.

2. Le logiciel espion mis en œuvre par la loi HADOPI

A également été mis en œuvre un logiciel espion permettant de reporter à la Commission de protection des droits les utilisations faites *via* l'accès Internet afin de s'assurer qu'elles ne soient pas contrefaisantes. Concrètement, on confie le dépistage des infractions à des sociétés privées qui ont pour mission de constater les manquements à l'obligation de vigilance par l'intermédiaire du logiciel espion installé via la sécurisation de l'accès à Internet. Une fois cette étape effectuée, l'adresse IP[140] des intéressés est communiquée à la

[135] Voir « le cas des opérations incidentes », page 29
[136] Délibération 2009 – 200 du 16 avril 2009
[137] Traduction allemande, abrégé en « BVerfG »
[138] Sur ce point, voir l'analyse de la décision par Marcel Moritz – « Les perquisitions en ligne et la surveillance d'internet, de Karlsruhe à Paris, similitude des enjeux, divergences des solutions ? », Revue Lamy Droit de l'Immatériel, n°41, pages 53 à 62, août 2008
[139] Point 247 de l'arrêt
[140] Une adresse IP (avec IP pour Internet Protocol) est un numéro d'identification qui est attribué à chaque branchement d'appareil à un réseau informatique utilisant l'Internet Protocol. Il existe des adresses IP de version 4 et de version 6. La

Commission de protection des droits de la HADOPI. L'une des critiques porte notamment sur le fait que l'on ne peut contrôler l'intégrité desdites sociétés. Très logiquement, la CNIL a porté son contrôle sur cette utilisation, mais son avis n'a été communiqué qu'au Gouvernement en avril 2008 et n'a jamais été officiellement rendu public, celui-ci n'ayant pas donné son autorisation. Ce n'est que par le biais d'une « *fuite* » dans la presse que l'avis a été porté à la connaissance du public. Il n'a donc jamais été possible de connaître officiellement l'avis de la CNIL sur l'utilisation de ce logiciel espion. Il est cependant ressorti de cette divulgation que la CNIL s'est prononcée contre le projet de loi, estimant qu'il poserait un problème de proportionnalité entre l'atteinte, la vie privée et le respect du droit de propriété des ayants droits.

Aussi, on a pu lire en doctrine les inquiétudes vis à vis de cette utilisation. Franck Macrez a, dès 2009[141], prévenu du risque de 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 les attaques possibles à mener sur la machine* » et parlait déjà de « *bricolage dangereux* ». Il existe donc également des risques concernant le droit au respect des données personnelles. Julien Couard considère à cet égard que « *le fait de légitimer la mise en place de moyens de surveillance aussi étendus paraît disproportionné au but recherché et dangereux dans son potentiel de déviance* »[142].

B. L'encadrement d'atteintes garanties par plusieurs autorités

Les atteintes prévues dans la lettre des dispositifs législatifs nécessitent l'apport de garanties rigoureusement encadrées. Dans un cas comme dans l'autre, la CNIL intervient pour protéger le droit des données personnelles. Outre cette intervention, le juge d'instruction opère un contrôle à priori pour juger de l'opportunité de la procédure et du respect des règles d'application (1), tandis que le juge judiciaire n'intervient qu'a posteriori dans le cadre d'une procédure de contestation (2).

1. LOPPSI 2 : une garantie par le juge d'instruction à l'existence menacée

L'extension des moyens envisagée par la loi LOPPSI 2 n'est pas sans poser de problématique au regard du droit à la vie privée.

Bien évidemment, le domicile fait partie intégrante de la vie privée[143] et comme le droit qui la protège n'est pas absolu, il va devoir être concilié avec des objectifs à valeur constitutionnelle. En l'occurrence, il s'agit de « *renforcer ses capacités dans l'anticipation, la prévention, la protection, la lutte et l'intervention contre les menaces et les risques susceptibles de porter atteinte aux institutions, à la cohésion sociale nationale, à l'ordre public, aux personnes et aux bien, aux installations et aux ressources d'intérêt général sur le territoire de la République* »[144].

Dans la décision de la Cour Constitutionnelle allemande du 28 février 2008, la Cour impose que les cyberperquisitions s'opèrent dans un cadre délimité et fixé par le législateur avec le recours systématique à une autorisation juridictionnelle. Ces deux points sont effectivement respectés en France puisque la loi est intervenue pour encadrer la pratique des perquisitions en ligne par l'intermédiaire de la LOPPSI 2 et que le juge d'instruction est la clé de voute de l'ensemble du processus.

---

version 4 est actuellement la plus utilisée : elle est généralement représentée en notation décimale avec quatre nombres compris entre 0 et 255

[141] Franck Macrez et Julien Gossa, « surveillance et sécurisation : ce que l'HADOPI rate », dans Revue Lamy Droit de l'Immatériel, n°50, pages 79 à 91, juin 2009

[142] Julien Couard, « Interview d'un praticien », dans Revue Lamy Droit de l'Immatériel, numéro 67, pages 67 et suivants, janvier 2011

[143] Article 8 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* »

[144] Assemblée nationale - Projet de *loi d'orientation et de programmation pour la performance de la sécurité intérieure* n°1697 - Enregistré à la Présidence de l'Assemblée nationale le 27 mai 2009 – Extrait de l'exposé des motifs, page 3

Il demeure cependant une inquiétude grandissante. Le juge d'instruction occupe une place à ce point importante qu'il est celui qui autorise la mise en place du dispositif d'interception, qu'il peut en ordonner l'interruption à tout moment, et qu'il dresse les actes requis à peine de nullité tout au long de la procédure comme le procès verbal. Or, il est bon de rappeler que ce dernier risque d'être supprimé. Son contrôle est pourtant essentiel et il représente un gage d'indépendance face au ministère de la Justice qui n'est pas négligeable. En effet, il ne peut recevoir l'ordre d'installer ce type de dispositif de témoin de connexion de la part du Gouvernement ou au contraire se refuser à demander son installation pour des affaires plus ou moins sensibles. Comme le résume Guillaume Champeau[145], « *le juge d'instruction est libre, et agit en proportion des nécessités de l'enquête* ».

Si le juge d'instruction est supprimé, d'après le projet de réforme de la justice c'est certainement le Procureur de la République qui pourra jouer ce rôle dont la prééminence a été démontrée. Celui-ci étant placé sous l'autorité de la chancellerie, et par voie de conséquence, du Gouvernement, son impartialité fait à l'heure actuelle l'objet de débats vifs dont l'issue reste pour le moins incertaine. A l'heure actuelle une chose est sûre, c'est une garantie qui se fragilise et qui pourra selon certains faire l'objet d'une requête devant la CEDH[146] d'autant plus que celle-ci a clairement exprimé que le Procureur ne pouvait être qualifié d'autorité judiciaire car « *il lui manque en particulier l'indépendance à l'égard du pouvoir exécutif pour pouvoir être ainsi qualifié* »[147].

Ce point est d'ailleurs parfaitement résumé[148] par Jean-Pierre Dubois, Président de la Ligue des droits de l'homme, qui parle de « *garanties qui ne garantissent rien* ». Il explique ainsi que « *la seule garantie présentée par le gouvernement, c'est que ce sera sous le contrôle du juge d'instruction. On veut justement supprimer le juge d'instruction, donc c'est une garantie post mortem. Il faut confier ça à une autorité judiciaire indépendante, et fixer des limites sur les types d'affaires concernées. Là, la police peut le faire pour n'importe quoi et pour n'importe qui.* » Il faudra donc attendre l'issue de la réforme sur la procédure pénale pour être définitivement fixé sur l'amplitude des risques de dérive.

2. HADOPI : Une garantie apportée par la CNIL et le juge judiciaire

Le Conseil constitutionnel a rappelé dans sa décision n° 2009-580 DC du 10 juin 2009 relative à la loi favorisant la diffusion et la protection de la création sur internet que la collecte de données à caractère personnelle encadrée par la législation du 6 janvier 1978 doit être conforme au droit au respect de la vie privée.

On peut ainsi lire au considérant 27 que « *la lutte contre les pratiques de* contrefaçon *sur internet répond à l'objectif de sauvegarde de la propriété intellectuelle et de la création culturelle ; que, toutefois, l'autorisation donnée à des personnes privées de collecter les données permettant indirectement d'identifier les titulaires de l'accès à des services de communication au public en ligne conduit à la mise en œuvre, par ces personnes privées, d'un traitement de données à caractère personnel relatives à des infractions ; qu'une telle autorisation ne saurait, sans porter une atteinte disproportionnée au droit au respect de la vie privée, avoir d'autres finalités que de permettre aux titulaires du droit d'auteur et de droits voisins d'exercer les recours juridictionnels dont dispose toute personne physique ou morale s'agissant des infractions dont elle a été victime* ». Ainsi donc, la sécurisation mettant en œuvre un logiciel espion ne peut avoir d'autres objectifs que la recherche d'infractions liées à la violation de l'obligation de vigilance.

Le traitement de données personnelles est avant tout contrôlé par la CNIL. Au travers de ses différents pouvoirs, la CNIL est une véritable garantie contre les erreurs faites par les auteurs d'un traitement de données personnelles dans la mise en œuvre concrète de la loi « *Informatique et libertés* » et des conséquences du recours à l'informatique des administrations. En tant qu'autorité en charge de veiller à la protection des données personnelles, elle a notamment un pouvoir de contrôle qui lui permet de surveiller la sécurité des systèmes d'information en s'assurant que toutes les précautions sont prises pour empêcher que les données ne soient déformées ou communiquées à des personnes non-autorisées. Lorsqu'elle constate

[145] http://www.numerama.com/magazine/15076-loppsi-l-installation-de-mouchards-chez-les-suspects-est-adoptee.html
[146] Claudine Guerrier, « La LOPPSI 2 en 2011 », Revue Lamy droit de l'immatériel, n°70, pages 92-101, janvier 2011
[147] CEDH, 18 juillet 2008, Medvedyev contre France, Req. n°3394/03
[148] http://www.rue89.com/2010/02/10/comment-la-loppsi-legalise-lespionnage-des-ordinateurs-137662?page=8

une irrégularité, elle peut émettre un avertissement rendu public ou non à l'issue duquel s'ouvre une phase en formation contentieuse lui permettant de sanctionner financièrement, de former une injonction de cesser le traitement ou de retirer l'autorisation. Ces deux pouvoirs de contrôle et de sanction lui permettent de veiller à ce que le développement des nouvelles technologies ne porte pas atteinte à la vie privée.

Or, en mai 2011, un serveur insuffisamment sécurisé de la société Trident Media Guard, chargé de collecter les adresses IP des contrefacteurs, a permis à un internaute de divulguer des fichiers qui comprenaient des listes d'œuvres surveillées depuis 2008, ainsi que les adresses IP des internautes mis en cause. Un contrôle a été effectué par la CNIL les 17 et 18 mai 2011 et a permis de constater la mauvaise application de la loi « *Informatique et Libertés* » par la société à ses propres traitements. Malgré le secret qui repose sur l'utilisation du logiciel espion mis en œuvre par la loi HADOPI, « la CNIL a décidé, au regard des éléments techniques contenus dans ces mises en demeure, de ne pas les rendre publiques ». Pour autant, « *elle juge utile d'informer le public de son action* »[149] via une synthèse diffusée le 6 juillet 2011.

La CNIL est une garantie importante de la protection des données personnelles. Elle a ainsi pu mettre la société TMG en demeure d'un délai de trois mois, de pallier les lacunes constatées et de respecter l'ensemble des dispositions de la loi "*Informatique et Libertés*".

Outre la CNIL, le juge judiciaire peut vraisemblablement s'avérer être une garantie pour l'utilisateur. L'hypothèse n'est pas à écarter et celui-ci pourrait tout à fait faire valoir la violation de ses droits devant le juge. C'est pour cette raison que l'on parle de contrôle a posteriori puisque le juge n'a pas la possibilité de décider si la mise en œuvre du logiciel espion est nécessaire ou non, tout comme il ne peut vérifier que les règles de bonne conduite relatives à la procédure sont rigoureusement respectées pour protéger le droit à la vie privée antérieurement à la mise en place du logiciel espion. Ceci s'explique par le caractère moins intrusif du logiciel utilisé dans le cadre de la loi HADOPI. En effet, celui-ci ne vise qu'à contrôler que les téléchargements ne portent pas atteinte aux droits des tiers. Il sera ainsi nécessaire de contester les constats opérés par les entreprises privées devant le juge judiciaire pour bénéficier de son contrôle. L'utilisateur pourra se rassurer par le fait que les sociétés privées ne risquent pas de transmettre une infraction liée à un objectif autre que celui visé par le Conseil constitutionnel, le juge sera là pour s'en assurer[150].

Au-delà des libertés et droits fondamentaux, les dispositions qui font l'objet de notre étude doivent se confronter à des difficultés techniques et juridiques, ce qu'il convient de développer.

[149] <http://www.cnil.fr/la-cnil/actu-cnil/article/article/dispositif-de-reponse-graduee-la-cnil-met-en-demeure-les-societes-de-perception-et-de-repa/>
[150] Cf. supra, Considérant 27

Section II - Deux extensions sources de difficultés

Au delà des droits et libertés fondamentales, les deux lois vont se trouver confrontées d'une part, à des problématiques d'ordre purement juridique (I), et vont d'autre part, entrer en contrariété avec des considérations techniques très complexes (II).

I. Des difficultés juridiques embarrassantes

L'extension des « *atteintes légitimes* » portées à la maîtrise de la connexion Internet par l'utilisateur suscite une gêne en matière de garantie procédurale dans le cadre du dispositif HADOPI qui pose clairement la question de l'égalité devant la loi ce que nous tâcherons de démontrer (A). Par ailleurs, la LOPPSI 2 s'appliquant à un espace par nature transfrontalier, il est nécessaire de se demander comment sont traitées les données se trouvant hors du territoire national (B).

A. Le cas de la loi HADOPI, des garanties procédurales insuffisantes

Nous avons constaté que, pour satisfaire aux exigences du Conseil Constitutionnel édictées dans sa décision du 10 juin 2009, la peine complémentaire de suspension de la connexion Internet peut être prononcée via une dualité de procédures relevant toutes deux de la compétence du juge judiciaire. La première hypothèse résulte du recours au juge unique du tribunal correctionnel tandis que la seconde hypothèse relève de l'ordonnance pénale.

Malgré cette garantie judiciaire, il semble que plusieurs critiques subsistent dans la mise en œuvre de chacune des procédures. Comme le remarque Diane de Bellescize[151], dans les deux cas, le principe de collégialité n'est pas respecté. Or ce principe « *permet au magistrat de se former et d'enrichir sa réflexion au contact de ses collègues et lui assure en outre une protection qui garantit la sérénité des délibérés et l'indépendance de sa décision* ». D'autre part, la collégialité « *assure au justiciable une décision mesurée, peu susceptible d'avoir été influencée par la partialité d'un juge, et dotée d'une plus grande autorité* »[152].

Outre cet aspect, la voie de l'ordonnance pénale induit deux critiques reposant sur une atteinte au principe du contradictoire et une atteinte à l'obligation de motivation. En effet, dans le cadre de l'ordonnance pénale prévue aux termes de l'article 495-1 du Code de procédure pénale, le président statue sans débat préalable et n'est pas tenu de la motiver. Pour respecter le principe du contradictoire, le même article prévoit que si le juge « *estime qu'un débat contradictoire est utile […], le juge renvoie le dossier au ministère public* ». De même, aux termes de l'article 495-3 du Code de procédure pénale « *le prévenu est informé qu'il dispose d'un délai de quarante-cinq jours […] pour former opposition à l'ordonnance et que cette opposition (permette) que l'affaire fasse l'objet d'un débat contradictoire* ». On peut déjà craindre que la plupart des utilisateurs engagés dans cette procédure n'hésiteront pas à faire opposition, ce qui engendrera nécessairement l'encombrement des tribunaux correctionnels. C'est donc l'objectif de célérité de la procédure qui est mis à mal. Pourtant, l'article 6-1 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales dispose que « *toute personne a droit à ce que sa cause soit entendue […] dans un délai raisonnable* ». Il est donc primordial de veiller à respecter ce principe.

A cet titre, la circulaire diffusée le 6 août 2010 précise que la procédure de l'ordonnance pénale devra être privilégiée dans le cadre de la poursuite de la contravention de négligence caractérisée du titulaire d'un accès à Internet.

Le Conseil Constitutionnel a pourtant validé ces dispositions, mais le doute subsiste quand à l'efficience des garanties et à l'efficacité de la procédure. Il avait d'ailleurs été soutenu une rupture du principe d'égalité

[151] Diane de Bellescize, « Hadopi 1 et Hadopi 2, en attendant Hadopi 3 ? », dans Rec. Dalloz 2010, p293
[152] <http://www.vie-publique.fr/decouverte-institutions/justice/definition/principes/qu-est-ce-que-collegialite.html>

devant la justice[153] selon lequel « *tous les citoyens sans distinction plaideront en la même forme et devant les mêmes juges, dans les mêmes cas* » puisque certains internautes seraient poursuivis par voie d'ordonnance pénale tandis que d'autres bénéficieraient du recours au juge unique. Cependant, le Conseil n'y a pas fait droit au regard de l'ampleur du phénomène justifiant ainsi des mesures dérogatoires permettant une meilleure fluidité et un désengorgement des tribunaux. Cependant, comme nous l'avons exposé, il n'est pas certain que ce moyen soit au service de la célérité de la procédure.

B. Le cas de la Loi LOPPSI 2 : les données situées hors du territoire national

Les données captées sur un écran d'ordinateur peuvent être de différentes natures, mais peuvent aussi, et très souvent en matière de criminalité organisée, se trouver en dehors du territoire national. En effet, bien que les dispositions législatives ne visent pas particulièrement la cybercriminalité en tant que telle, elle touche à un point dont le milieu naturel tend à se développer au niveau mondial. La question s'est donc posée de savoir si les autorités judiciaires avaient une emprise sur ce type de données.

On peut trouver une réponse via les dispositions des articles 57-1, 776-3 et 97-1 du Code de procédure pénale qui disposent qu'à l'occasion d'une perquisition, il est possible d'accéder aux données contenues dans un système informatique distant accessible depuis le système initial lorsqu'il est préalablement avéré que le système distant est en dehors du territoire français. Ainsi, les données peuvent être recueillies « *sous réserve des conditions d'accès par les engagements internationaux en vigueur* ».

Vraisemblablement, il est possible d'adapter le même raisonnement dans le cas de la LOPPSI 2. Il sera sûrement question de mettre en œuvre l'ouverture d'une information judiciaire et par ce biais se faire délivrer une commission rogatoire internationale[154] par le juge d'instruction saisi[155]. Cependant cette procédure n'est pas très efficace en terme de diligence ce qui pourra ralentir considérablement l'enquête. « *Les autorités judiciaires sont soumises au strict respect des règles territoriales en matière de perquisition* », et c'est certainement là que le bât blesse puisqu'il faudra nécessairement améliorer la cohésion internationale dans la lutte contre la cybercriminalité pour rendre véritablement effective ce type de procédure.

Les difficultés juridiques ne sont pas les seules car la législation doit également affronter le rempart de la technique, ce qu'il convient d'étudier.

II. Des difficultés techniques insurmontables ?

Le dispositif HADOPI ne semble pas parfaitement apte à s'adapter à toute situation. Nous verrons que l'on peut considérer que cette loi peut-être considérée comme victime de son mécanisme, les difficultés techniques demeurant pour les moins imposantes (A). La LOPPSI 2 peut quant à elle se retrouver totalement inadaptée à une défense de l'utilisateur doué en informatique (B).

A. La Loi HADOPI confrontée à son propre mécanisme

Les difficultés techniques sont redoutables et les experts en informatique n'ont pas hésité à émettre bon nombre de critiques à l'égard de la loi HADOPI qui, à la lecture de ces avis, risque fort de s'appliquer au détriment des utilisateurs. C'est tout d'abord la sécurisation qui pose problème (1), mais également la difficulté à pouvoir identifier les contrefacteurs (2).

1. Une sécurisation ardue

[153] Lois des 17 et 24 août 1790
[154] C'est également l'avis de Guillaume Lovet, expert en cybercriminalité et responsable de recherche dans le domaine des anti-menaces, lors d'un « *chat* » organisé par lemonde.fr en juin 2009
[155] Sur ces questions, voir Philippe Belloir, « Perquisition et saisie en matière de lutte contre la cybercriminalité », dans Revue Lamy Droit de l'Immatériel, 2010

Le problème technique fondamental demeure la sécurisation de l'accès à Internet par l'utilisateur. Le législateur a pris soin de prévoir une labellisation des moyens de sécurisation afin de contrôler d'une part, que l'usage fait de l'accès ne porte pas atteinte aux droits des tiers, et d'autre part, de permettre à l'utilisateur mêlé à la procédure de riposte graduée, de se disculper en arguant qu'il a mis en œuvre le moyen permettant le contrôle de cet usage. Or il est bien connu dans le monde informatique que la sécurité absolue n'existe pas. Par exemple, les clés WEP[156] ou WAP[157] sont aujourd'hui assez répandues et ne sont peut être pas suffisantes. Cependant, la clé WEP est appelée par les spécialistes du milieu « *Weak Encryption Protocol* » (Protocole de cryptage faible) du fait de sa simplicité à être détournée. Le risque de détournement existe bel et bien. Dans ce cas on parle d'usurpation de l'adresse IP puisque le « *pirate* » a l'intention de masquer son identité et d'usurper celle d'un autre utilisateur pour commettre l'infraction. L'UFC-Que Choisir[158] a d'ailleurs fait un test devant huissier lors du projet de loi HADOPI pour démontrer à quel point il peut être élémentaire de réaliser un tel détournement. On peut lire dans le rapport qui a été rendu public[159] que « *par un constat d'huissiers et un rapport d'expert, l'UFC-Que Choisir a fait la preuve qu'il est à la portée de tous de pirater la connexion internet sans fil de n'importe qui, et ainsi d'usurper une adresse IP pour télécharger* ».

La clé WPA est a priori efficiente si sa taille est conséquente et qu'elle est générée de façon aléatoire[160]. Cependant les technologies ne cessent d'évoluer et avec elles les techniques de « *piratage* ». Cette évolution des techniques pèse sur l'utilisateur.

Celui-ci doit par ailleurs subir le coût de la sécurisation. Par exemple, les sécurisations labellisées ne pourront certainement pas s'adapter à tous les ordinateurs des différents utilisateurs puisque les capacités et les systèmes d'exploitation peuvent être dépassés et incapables de s'adapter à un tel dispositif. Ce dernier point soulève la question de savoir s'il y a rupture du principe d'égalité devant la loi puisque tous les utilisateurs ne disposent pas des mêmes moyens. La sécurisation en elle même peut également s'avérer onéreuse puisque bon nombre de développeurs travaillent à rendre la sécurisation meilleure et au gout du jour ce qui n'est pas sans coût.

L'utilisateur n'est par ailleurs pas forcément informaticien. Bien au contraire ! La question de sa compétence est inévitable puisqu'on présuppose que celui-ci sait parfaitement comment paramétrer les moyens de sécurisation, ce qui n'est pas le cas dans la grande majorité des cas. Par exemple, pour le cas des pare-feu qui désigne un « *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* »[161]. Ce système permet de filtrer les applications illégales ou dangereuses, or il devient quasi-impossible pour l'utilisateur lambda de le paramétrer de manière à empêcher le transit et l'échanges de contenus litigieux. Ceci d'autant plus que les logiciels de « *pair à pair* » sont notamment utilisés pour les échanges de contenus légaux. C'est à l'utilisateur qu'il revient de savoir lui même faire le tri et distinguer les échanges qui relèvent ou non de la contrefaçon tout en lui permettant de naviguer sur le réseau Internet comme il l'entend sans que la sécurisation ne le bride.

A l'attention de l'utilisateur, Franck Macrez et Julien Gossa posent ainsi que[162] « *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 ;*

[156] Wired Equivalent Privacy – Protocole d'échange sécurisé permettant de partager une connexion wifi entre plusieurs ordinateurs
[157] Wifi Protected Access – Norme de sécurité définie par la Wifi Alliance
[158] Association à but non lucratif créée en 1951, doyenne des associations de consommateurs d'Europe occidentale
[159] <http://static.pcinpact.com/pdf/annexe1-constat-ufc-que-choisir-wifi.pdf>
[160] Franck Macrez et Julien Gossa, « surveillance et sécurisation : ce que l'HADOPI rate », point n°42 « *protection de l'accès sans fil* », dans Revue Lamy Droit de l'Immatériel, n°50, pages 79 à 91, juin 2009
[161] 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, voir « *Barrières de sécurité* », p. 1946
[162] Franck Macrez et Julien Gossa, « surveillance et sécurisation : ce que l'HADOPI rate », point n°46 « la sécurité, un problème personnel», Revue Lamy Droit de l'Immatériel, n°50, pages 79 à 91, juin 2009

- *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* ».

Visiblement, cette difficulté majeure est avant tout une contrainte pour l'utilisateur puisque la sécurisation est avant tout l'affaire d'un expert. Il appartiendra à l'HADOPI d'offrir une lecture claire et détaillée afin de permettre à l'ensemble des abonnés de pouvoir sécuriser son accès comme il se doit.

2. Une identification parfois difficile des contrefacteurs

Enfin, l'identification du contrefacteur peut être très difficile, voir impossible. Dans un premier temps, il existe le risque évoqué plus haut de l'usurpation de l'adresse IP. Dans ce cas précis, l'utilisateur floué risque de se voir condamné alors même qu'il n'a commis aucun acte de contrefaçon.

Outre l'usurpation de l'adresse IP, il convient de distinguer si l'utilisateur utilise une adresse IP statique ou dynamique. A chaque connexion au réseau Internet, le fournisseur d'accès à Internet attribue à l'utilisateur une adresse IP. Si celle-ci est statique, l'utilisateur sera toujours identifié sous la même adresse. Si au contraire l'adresse IP est dite dynamique, elle varie à chaque connexion et se trouve redistribuée à un autre internaute. Or, c'est par ce biais que l'utilisateur est mis en cause puisqu'il appartient au fournisseur d'accès Internet de communiquer l'adresse par laquelle il y a un constat de manquement à l'obligation de vigilance. Il n'est pas illusoire qu'un utilisateur se voit attribuer une adresse avec laquelle un autre utilisateur a commis un acte de contrefaçon. On parle alors de problèmes d'horodatage[163]. Il revient à la Commission de protection des droits de redoubler de prudence et de ne pas condamner systématiquement les utilisateurs en ayant une particulière vigilance sur ce point.

Par ailleurs il existe bon nombre de moyens pour les utilisateurs afin de se rendre « *invisible* »[164] sur la toile. Par exemple, « *hidemyass.com* » est un moyen qui a fait sa renommée en permettant à l'utilisateur de se rendre anonyme sur la toile en empruntant l'adresse du serveur lui-même. On parle alors de serveur « *proxy* ». Dès lors, toutes les communications sont réputées provenir de ce serveur qui se trouve être la plupart du temps hors de la compétence de la Commission de protection des droits et l'utilisateur est mis à l'abri. Il est aussi possible d'utiliser un logiciel permettant de brouiller toute trace.

B. La loi LOPPSI 2 confrontée à une haute délinquance organisée

La LOPPSI 2 visant à lutter principalement contre la criminalité organisée, il n'est pas exclu que cette forme particulièrement structurée de délinquance puisse compter parmi ses rangs des professionnels de l'informatique qui sauront trouver des solutions pour empêcher toute captation de données informatiques. « *La réponse à la machine, c'est la machine* », c'est pourquoi, afin de se défendre, certains pourront mettre en œuvre des moyens cryptologiques (1), tandis que d'autres pourront essayer de retourner le logiciel contre les enquêteurs (2).

---

[163] Franck Macrez et Julien Gossa, « surveillance et sécurisation : ce que l'HADOPI rate », dans Revue Lamy Droit de l'Immatériel, point n°37 « faux positifs », n°50, pages 79 à 91, juin 2009. Il y explique notamment que cela peut être causé du fait des horaires d'été ou de l'utilisation des heures GMT ou locales

[164] L'invisibilité totale sur Internet demeure illusoire car à chaque branchement d'appareil à un réseau informatique utilisant l' « *Internet Protocol* » est attribuée une adresse IP qui est un numéro d'identification. Or, il faut bien permettre la communication entre les ordinateurs et donc nécessairement utiliser le même protocole. Par conséquent, et même si c'est parfois difficile, chaque ordinateur connecté à Internet est toujours identifiable.

1. La cryptologie comme obstacle à la bonne application de la loi

La procédure de captation peut se retrouver confrontée à des remparts techniques qui rendront sa bonne application bien compliquée. Comme le remarque David Zenaty[165], la grande délinquance utilise des techniques de cryptage difficiles à casser. La loi pour la Confiance en l'économie numérique a très largement participé à la démocratisation de l'usage de la cryptologie. Son utilisation était autrefois règlementée comme celle des armes de guerre. En vertu de l'article 30 de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, l'utilisation des moyens de cryptologie est libre en France. Les moyens de cryptologie y sont définis[166] comme « *tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète* ». Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité. Ce bouclier peut-être un véritable obstacle au bon déroulement de la procédure et mettre l'utilisateur à couvert de cette dernière.

2. Un logiciel espion nécessairement compatible avec le système informatique et protégé contre le « *reverse engineering* »

Par ailleurs, le « *mouchard* » utilisé par les enquêteurs pour capter les données informatiques à l'insu de l'utilisateur n'est peut-être pas compatible avec l'antivirus de ce dernier. La plupart d'entre eux peuvent désormais recourir à des outils de nettoyage systématique et de détection des spywares. Il faudra donc une concertation entre les éditeurs de logiciels antivirus pour permettre l'invisibilité et la bonne application des logiciels espions.

Il existe également des doutes quant à l'efficacité même des « *mouchards* ». L'utilisation de logiciels espions est un moyen qui se distingue clairement des systèmes d'écoute traditionnels. Cette évolution marque par le même temps sa faiblesse puisque ledit logiciel peut être victime de « *reverse engineering* » (rétro-ingénierie). Cette technique consiste à étudier le fonctionnement du logiciel afin d'en déterminer le fonctionnement, et pourquoi pas de le modifier, voir de le détourner à son profit. Cette technique s'est notamment popularisée pour sa capacité à détourner les protections anti-copies des jeux vidéo. Les experts en la matière affirment que le risque de voir le logiciel détourné existe bel et bien et pourrait permettre de faire accuser des innocents[167]. Il appartient donc aux éditeurs du logiciel de tout mettre en œuvre pour protéger le code source afin d'en empêcher la décompilation. Par exemple, il est possible de recourir au processus dit d' « *obfuscation* » qui peut se définir comme étant une transformation appliquée au code en vue de le rendre inintelligible tout en le préservant. Cette technique n'est certainement pas isolée et les experts devront prendre à garde à être sans cesse à la pointe de la technologie pour ne pas se laisser dépasser et tenter de garder une longueur d'avance.

Nous nous situons bien évidemment ici dans le cas où le « *hacker* » (pirate informatique) a conscience que ses actes sont punis par la loi. En effet, l'article 434-4 du Code pénal punit de trois ans d'emprisonnement et de 45 000€ d'amende le fait, « *en vue de faire obstacle à la manifestation de la vérité, de détruire, soustraire, receler ou altérer un objet de nature à faciliter la découverte d'un crime ou d'un délit, la recherche des preuves ou la condamnation des coupables* »[168].

---

[165] Daniel Zenaty, Expert en informatique, « La perquisition à distance par l'introduction de mouchards informatiques », lors de la Conférence du 17 mars 2011 organisé par le Master 2 Droit du Multimédia et de l'Informatique Université Panthéon-Assas Paris 2 en partenariat avec l'association française des juristes d'entreprise et juriscom.net

[166] Loi n° 2004-575, 21 juin 2004, art. 29, pour la confiance dans l'économie numérique <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=>

[167] Guillaume Lovet, expert en cybercriminalité et responsable de recherche dans le domaine des anti-menaces, lors d'un « *chat* » organisé par lemonde.fr en juin 2009

[168] Point mis en exergue par Etienne Papin – Avocat associé du cabinet Féral-Schuhl / Sainte Marie - « La captation des données informatiques : enjeux et conséquences pour les entreprises de la LOPPSI 2 »

Bien évidemment, si l'intention délictuelle n'est pas effective et que le logiciel espion est supprimé par hasard, il sera impossible pour les enquêteurs de reprocher à la personne mise en cause cette destruction.

Conclusion

En conclusion de ce chapitre, il est certain que les garanties apportées dans le cadre des atteintes étudiées restent encore fébriles. Dans le cas de la sanction complémentaire de suspension de l'accès à Internet, bien que le Conseil Constitutionnel soit intervenu pour rejudiciariser la procédure, le manque de garanties procédurales tend à fragiliser la situation de l'utilisateur mis en cause. De plus, la sanction est encore contestée et semble, malgré la lecture du Conseil Constitutionnel, disproportionnée à l'objectif poursuivi. De même, le mécanisme de sécurisation semble bien compliqué pour l'utilisateur profane qui ne voit dans l'Internet qu'un outil de travail et de recherches. Il s'avère de plus quelque peu inadapté à ce milieu qui par nature ne garantit jamais une protection parfaite. D'autant plus qu'à l'opposé, il existe une catégorie d'utilisateurs experts en informatiques qui sont conscients des moyens pour échapper à la loi.

Dans le cas du recours au logiciel espion, si le mécanisme de sécurisation HADOPI est limité à la détection des téléchargements illicites, l'inquiétude persiste. En effet, le fait de confier la détection des contrefacteurs à des sociétés privées et le manque de transparence sur l'utilisation des « *mouchards* » tendent à augmenter la méfiance des utilisateurs.

Quant à la LOPPSI 2, elle est également génératrice de craintes. Le juge d'instruction, principal organe de garantie, est sur la sellette. Qu'adviendra t-il si ce dernier n'est plus ? Doit-on craindre du Gouvernement qu'il donne l'ordre à son remplaçant d'aller au-delà des limites fixées ? Cela paraît tout de même déraisonnable et le marbre de la Loi est là pour interdire les excès.

Quoi qu'il en soit, dans tous les cas, les lois se heurtent à la forteresse de la technique. S'il peut y avoir des difficultés d'identification, il est aussi à craindre des détournements. Pour y pallier, la LOPPSI 2 peut certainement jouer d'une certaine complémentarité avec les lois HADOPI, mais la bonne application de ces dernières reste confuse.

<http://www.cio-online.com/contributions/lire-la-captation-des-donnees-informatiques%C2%A0-enjeux-et-consequences-pour-les-entreprises-de-la-loppsi-2-408-page-1.html>

Chapitre II - Des lois à l'efficience incertaine

Les nombreuses difficultés rencontrées par ces nouvelles dispositions législatives mettent leur expérimentation en péril. Il est cependant possible d'imaginer un moyen permettant aux lois HADOPI de combler l'une de ses lacunes par l'intermédiaire d'une autre disposition de la LOPPSI 2 pour lui permettre une meilleure effectivité (section I). De plus, ces lois souffrent d'une légitimité contestée car elles créent un climat de surveillance généralisée très dérangeant. Il faut donc s'attendre à une réaction plus ou moins aléatoire des utilisateurs (section II).

Section I - La LOPPSI 2 : support de la HADOPI ?

A la première lecture du nouveau délit d'usurpation d'identité, il semble qu'il n'y ait aucun rapport avec les dispositions des lois HADOPI (I). Cependant, cette vision s'avère quelque erronée si l'on s'attarde sur la rédaction du texte très certainement apte à combattre le détournement de l'adresse IP pour ainsi servir de support aux lois HADOPI (II).

I. Un cadre général du délit d'usurpation d'identité a priori en dehors des considérations liées à la connexion Internet

Cette nouvelle infraction pénale est initialement venue palier une insuffisance de fondement en matière d'usurpation d'identité (A). Cependant, sa rédaction semble englober la notion d'identité numérique qui peut s'avérer bénéfique pour les lois HADOPI (B).

A. Définition d'une infraction palliative au délit d'usurpation d'identité en ligne

La LOPPSI 2, outre la création de la procédure de captation des données informatiques, a permis de faire naître une nouvelle disposition relative à la protection de l'identité. Désormais, l'article 226-4-1[169] du code pénal dispose que « *le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende* ». Afin de couvrir également les faits d'usurpation commis sur Internet, ce même article ajoute que « *cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne* ».

En effet, avec l'avènement du « *web 2.0* »[170], on a pu assister ces dernières années à une multiplication des moyens de communication sur le réseau Internet (blogs, forums, réseaux sociaux, etc.) impliquant pour les utilisateurs de nombreuses inscriptions révélant souvent leur identité. Dans le même temps, on a pu constater que de nombreuses personnalités notoires se sont fait usurper leur identité, en particulier sur les réseaux sociaux. Ainsi, l'utilisateur lambda pouvait légitimement penser pouvoir entrer en relation avec la personnalité en question alors qu'il n'en était rien. Plus grave encore, certains « *faux profils* » étaient utilisés pour commettre des infractions au préjudice de l'identité réelle tels que proférer des propos injurieux, ou diffamatoires. Plusieurs décisions de justice ont donc été prises afin de contrer ce phénomène[171]. Cependant, aucune disposition législative ne s'accordait parfaitement à ces usurpations effectuées sur Internet. Il était par

[169] Article 226-4-1 du Code pénal créé par LOI n°2011-267 du 14 mars 2011 - art. 2 <http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=7175E19A9E290A0B00B973C66DDC265F.tpdjo07v_3?idArticle=LEGIARTI000023709201&cidTexte=LEGITEXT000006070719&dateTexte=20110825&categorieLien=id>

[170] On appelle « *web 2.0* » l'évolution d'Internet qui a permis une plus grande simplicité ne nécessitant pas de connaissances techniques pour pouvoir participer. Par conséquent, Internet est devenu un lieu bien plus attractif, participatif et interactif puisque tout internaute a la possibilité d'agir sur la diffusion des contenus proposés, d'en permettre l'échange et d'être ainsi à la fois l'émetteur et le récepteur de l'information

[171] Par exemple, une ordonnance de référé du 24 novembre 2010 du TGI de Paris avait sanctionné l'internaute qui avait crée le faux profil de l'humoriste Omar Sy

exemple invoqué l'article 434-23 du Code pénal qui dispose que « *le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende* », mais cet article ne couvrait pas l'ensemble des usurpations pouvant s'effectuer par voie numérique. L'article 9 du Code civil protégeant la vie privée ou les articles 8 et 10 de la CEDH posant le droit au respect de la vie privée et familiale et le droit à la liberté d'expression pouvaient également servir de fondement.

C'est cette insuffisance qui a permis de faire voir le jour à une nouvelle disposition pénale réprimant explicitement et de manière adaptée tout délit d'usurpation d'identité. Cependant, cette infraction fait référence à la notion d'identité, or sur Internet, on va parler d'identité numérique. Ce concept nouveau mérite une circonscription afin d'en déterminer la portée.

B. Les difficultés de la délimitation de l'identité numérique

Une difficulté se pose cependant dans la définition de l'identité numérique. En effet, les éléments de ce nouveau concept ne sont absolument pas définis par la loi. Lucien Castex détermine l'identité comme « *la conscience qu'une personne a d'elle-même, la qualité qui fait qu'une chose est la même qu'une autre, c'est l'ensemble des données de fait et de droit permettant d'individualiser quelqu'un* »[172]. Ainsi, elle peut recouvrir différentes formes et se multiplier par le biais de différents moyens puisqu'il est tout à fait possible de créer des comptes à son identité sur les multiples espaces proposés par le réseau Internet.

Plus précisément, Lucien Castex pose que l'identité numérique peut être divisée en trois types d'identités principales :

- L'identité numérique au sens strict qui regroupe l'ensemble des données techniques permettant de recomposer le parcours d'un individu sur Internet comme les données de connexion et l'adresse IP ;
- L'identité numérisée composée des données relatives à la personne physique en tant qu'elle est transposée sur Internet comme les photographies, les textes publiés, les identifiants de connexion ;
- L'identité immatérielle qui fait plutôt référence aux avatars sensés représenter les utilisateurs sur Internet, notamment dans les jeux vidéo.

Dans le cadre de notre étude, c'est l'identité numérique au sens strict qui va nous intéresser puisqu'elle va concerner l'adresse IP. Comme nous l'avons observé dans le cadre des risques techniques auxquels se trouve confronté la loi HADOPI, cette adresse IP peut-être usurpée afin de se cacher derrière elle pour commettre l'infraction de contrefaçon et provoquer la négligence caractérisée.

Dans la lettre de l'article 226-4-1 du code pénal, il est fait référence à l'usurpation « *d'une ou plusieurs données de toute nature* » permettant d'identifier. Cette rédaction large a été pensée pour s'appliquer au plus grand nombre de possibilités. Ainsi, il est tout à fait possible d'imaginer qu'elle puisse recouvrir l'adresse IP.

Il reste à savoir si l'adresse IP peut-être considérée comme une donnée à caractère personnel pour ainsi entrer dans le champ d'application de l'infraction d'usurpation d'identité.

[172] Lucien Castex, ATER en droit privé et sciences criminelles et Conseil en technologies de l'information, « Le nouveau délit d'usurpation d'identité en ligne », lors de la Conférence du 17 mars 2011 organisé par le Master 2 Droit du Multimédia et de l'Informatique Université Panthéon-Assas Paris 2 en partenariat avec l'association française des juristes d'entreprise et juriscom.net

II. Un moyen de répression de l'usurpation de l'adresse IP au service de la Loi HADOPI

Si l'adresse IP est considérée comme une donnée personnelle entrant dès lors dans le champ de l'identité numérique (A), il est permis de penser que cette nouvelle infraction permettra de réprimer les comportements visant à détourner la ligne d'un utilisateur (B).

A. L'adresse IP : une donnée à caractère personnel ?

L'adresse IP relève des données dites de connexion. Ce sont des données de communication engendrées automatiquement par les communications effectuées via Internet ou la téléphonie et donnant des informations sur les messages échangées, comme le nom, le prénom, ou encore l'adresse IP.

La Loi du 6 janvier 1978 modifiée par la Loi du 6 août 2004 définit, dans son article 2, une donnée à caractère personnel comme « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres [via] l'ensemble des moyens dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne* ».

La jurisprudence est divisée sur le point de savoir si l'adresse IP relève des données à caractère personnel et donc potentiellement de l'identité numérique. Deux arrêts de la cour d'appel de Paris se sont penchés sur cette question les 27 avril 15 mai 2007[173]. Dans chacun des cas d'espèce, il s'agissait d'internautes poursuivis pour avoir mis à disposition des fichiers musicaux sur réseau de « *peer to peer* » sans autorisation des ayants droits. En l'occurrence, en première instance, les procès verbaux constatant les infractions par les agents de la Société civile des producteurs phonographiques avaient été écartés car ils avaient été établis sans l'autorisation préalable de la CNIL. Cependant en appel, les juges ont décidé que le simple procès-verbal probatoire d'un agent assermenté de la Société civile de producteurs de phonogrammes ne constitue pas un traitement de données personnelles.

A l'opposé, une divergence d'appréciation a été constatée dans deux décisions de la Cour d'appel de Rennes en date du 22 mai 2008 et du 23 juin 2008, les juges ayant qualifié à deux reprises l'adresse IP de donnée à caractère personnel. Ils considèrent ainsi que *« l'adresse IP de l'internaute constitue une donnée indirectement nominative car, si elle ne permet pas par elle même, d'identifier le propriétaire du poste informatique, ni l'internaute ayant utilisé le poste et mis les fichiers à disposition, elle acquiert ce caractère nominatif par le simple rapprochement de la base des abonnés, détenue par le fournisseur d'accès internet* ».

Cependant, par une décision du 13 janvier 2009[174], la Chambre criminelle de la Cour de Cassation casse l'arrêt de la Cour d'appel de Rennes du 22 mai 2008 estimant que l'agent assermenté, dans son opération de constat de l'infraction, « *se contente de relever l'adresse IP pour pouvoir localiser son fournisseur d'accès en vue de la découverte ultérieure de l'auteur des contrefaçons* ». Dès lors, le procès verbal ne revêtant pas la qualification de traitement de données à caractère personnel, l'autorisation préalable de la CNIL n'est pas nécessaire.

A l'opposé, le G29[175] et la CNIL[176] considèrent l'adresse IP comme une donnée à caractère personnel. Une proposition de loi du Sénat visant à mieux garantir le droit à la vie privée à l'heure du numérique adoptée le 23 mars 2010 et transmise à l'Assemblée nationale propose justement d'intégrer tout numéro identifiant le titulaire d'un accès des services de communication au public dans le champ des données à caractère personnel puisque visé par la Loi « *informatique et Libertés* »[177]. Comme le suggère Christiane Féral-Schuhl, cette loi permettrait enfin de « *clarifier le statut de l'adresse IP* »[178].

---

[173] CA Paris, 13e ch. A, 15 mai 2007, RG n°06/01954 – CA Paris, 13e ch. B, 27 avril 2007, RG n°06/02334, Gaz. Pal. 2008, 13-15 janvier, n°13 à 15, p. 9
[174] Crim. 13 janvier 2009, n°08-84.088, Bull. crim., n°13, RLDI 2009, n°49
[175] Avis du 20 juin 2007 - <http://ec.europa.eu/justice/data-protection/index_en.htm>
[176] Par 3 décisions rendues le 18 octobre 2005
[177] Proposition de loi, article 2
[178] Christiane Féral-Schuhl – *Cyberdroit – Le droit à l'épreuve de l'Internet* – 6e édition Dalloz – p159 à 160

Dernièrement, la CJUE a eu l'occasion d'apporter son éclairage dans le cadre de son arrêt relatif au filtrage du web[179]. Elle expose en effet que « *l'injonction de mettre en place le système de filtrage litigieux impliquerait une analyse systématique de tous les contenus ainsi que la collecte et l'identification des adresses IP des utilisateurs qui sont à l'origine de l'envoi des contenus illicites sur le réseau, ces adresses étant des données protégées à caractère personnel, car elles permettent l'identification précise desdits utilisateurs* ». La question semble donc désormais tranchée, l'adresse IP constitue bien aux yeux de la CJUE une donnée à caractère personnel.

B. Une infraction finalement définie de manière suffisamment large pour ramener l'utilisateur sous le coup de la HADOPI

A la vue des différents éléments observés, il est très probable que la LOPPSI 2 puisse servir de véritable support à la HADOPI. En effet, l'identité numérique est une notion insuffisamment circonscrite à l'heure actuelle permettant d'y incorporer le cas de l'adresse IP à la condition que cette dernière satisfasse à l'exigence de relever des données personnelles. Au delà de cet aspect, il est également fait référence au fait de « *troubler (la) tranquillité ou celle d'autrui* ». Il s'agit une nouvelle fois d'un concept trouble dont le caractère « *fourre-tout* » peut permettre son application à de nombreuses infractions et notamment l'usurpation de l'adresse IP.

L'ensemble de ces éléments permettrait de restreindre la difficulté relative au détournement de l'adresse IP rencontrée par la loi HADOPI. La parfaite sécurisation de la connexion étant impossible, le fait de réprimer la possibilité pour un internaute d'usurper une adresse IP peut être un élément fortement dissuasif, voir le cas échéant, répressif. Certains spécialistes comme Myriam Quéméner posent d'ailleurs d'ores et déjà que « *ce texte vise donc non seulement l'identité mais toutes les données liées à un individu et ainsi devrait permettre de réprimer l'usurpation de l'adresse IP* ».

Cette rédaction semble ainsi bienvenue. Pour autant, on pourrait tout de même soulever l'idée que les pratiques d'usurpations d'identité étaient déjà réprimées sur le fondement du délit d'escroquerie, du délit d'atteinte à la vie privée d'autrui, de la diffamation[180]. Cette critique semble malvenue dans la mesure où ces fondements étaient réducteurs puisqu'ils ne permettaient qu'une défense des atteintes faites à l'individu lui même et non pas aux données qui s'intègrent dans la notion d'identité numérique. En ce sens, il est possible de croire que la Loi LOPPSI 2 puisse venir au secours de l'une des carences de la Loi HADOPI.

Il faudra attendre les réponses de la jurisprudence pour donner forme et délimiter les notions d'identité numérique et de trouble de la tranquillité. La loi devra par ailleurs enfin déterminer le statut de l'adresse IP. Ce n'est qu'à l'issue de ces différentes étapes que nous serons fixés sur la possibilité de protéger le contrôle de l'accès par l'utilisateur via ce fondement.

[179] CJUE, 24 nov.2011 affaire C-70/10 – Scarlet Extended SA contre SABAM <http://curia.europa.eu/jurisp/cgibin/gettext.pl?where=&lang=fr&num=79888875C19100070&doc=T&ouvert=T&seance=ARRET>

[180] Claudine Guerrier, « La LOPPSI 2 en 2011 », Revue Lamy droit de l'immatériel, n°70, pages 92-101, janvier 2011

Section II - Vers une responsabilisation de l'utilisateur ?

L'effectivité des lois dépend de la bonne réaction de l'utilisateur, surtout pour la loi HADOPI qui comporte clairement un volet qui se veut pédagogique (I). En revanche, il n'est pas certain que tous les utilisateurs voient d'un œil confiant ces nouvelles dispositions visant à les espionner, voir leur faire perdre leur connexion à Internet (II).

I. La valeur pédagogique de ces extensions pour un meilleur contrôle de sa connexion Internet

Si la Loi LOPPSI 2 ne paraît pas avoir de vertus clairement pédagogiques (A), les lois HADOPI s'inscrit tout à fait dans cet objectif, bien qu'il ne soit pas certain que les utilisateurs en soient absolument convaincus (B).

A. La loi LOPPSI 2 a priori en dehors de considérations pédagogiques

Les extensions des atteintes opérées par le législateur au contrôle de la connexion Internet par l'utilisateur posent la question de leur valeur pédagogique. Pour le cas de la Loi LOPPSI 2, à priori, elle est inexistante. En effet, cette Loi a pour objectif de renforcer la sécurité intérieure du pays par différents moyens déployés. La partie relative à la procédure de captation de données informatiques n'aura aucune incidence sur la pédagogie de l'utilisateur puisque l'on ne fait que donner de nouveaux moyens d'investigation aux autorités judiciaires. Concernant l'usurpation d'identité numérique, nous l'avons vu, les contours sont encore trop flous pour que l'utilisateur soit conscient du risque qu'il prend s'il vient à détourner une adresse IP. En revanche, si la Loi et la jurisprudence tendent à réprimer clairement ce comportement, il est possible que cela puisse jouer un rôle de prévention. Averti de l'épée de Damoclès, le « *pirate* » sera peut-être moins tenté de commettre une infraction.

B. La loi HADOPI au cœur de considérations éducatives controversées

Concernant les lois HADOPI en revanche, la ligne directrice se veut pédagogique[181], comme le montre la modification du Titre III du Livre III du code de propriété intellectuelle qui s'intitule désormais « Prévention, procédure, sanctions ».

L'objectif initial est de rappeler à l'ordre l'utilisateur afin que sa connexion ne soit pas un vecteur de contrefaçon si un constat de manquement à l'obligation de vigilance est fait. En l'avertissant par deux fois avant de le poursuivre en justice, on cherche à le responsabiliser, le faire réagir pour le faire revenir dans le droit chemin. Selon Julien Couard[182], « *en visant directement les titulaires d'abonnement Internet, c'est-à-dire les personnes ayant une autorité au sein des entités telles qu'une famille ou une entreprise, le législateur espère responsabiliser ces personnes et leur donner un rôle beaucoup plus actif dans la surveillance des individus qu'elles ont sous leur garde ». Certains vont même plus loin comme Jean-Sébastien Mariez[183] qui précise que la réponse graduée trouve sa crédibilité dissuasive dans la sanction finale. Selon lui « que serait une Hadopi limitée au statut de boîte aux lettres, sinon un épouvantail dont les messages d'avertissement auraient tôt fait de se transformer en feux de paille* » ? On donne ainsi un « *code de conduite* » à l'utilisateur, comme la nétiquette, mais avec un véritable pouvoir contraignant.

La Loi a même prévu de sensibiliser les futurs utilisateurs. A ce titre, l'article L312-6 du Code de la propriété intellectuelle dispose que « les élèves reçoivent une formation sur les dangers du téléchargement et de la

---

[181] Christophe Caron, *Droit d'auteur et Droits voisins*, Litec, 2e éd., pages 470 à 475, 2010
[182] Julien Couard, « Interview d'un praticien », dans Revue Lamy Droit de l'Immatériel, numéro 67, pages 67 et suivantes, janvier 2011
[183] Jean-Sébastien Mariez, « Hadopi… trois petits points de suspension », dans Revue Lamy droit de l'Immatériel, n°65, Actualités créations immatérielles, éclairage, pages 11 à 17, novembre 2010

mise à disposition illicites d'œuvres ou objets protégés par un droit d'auteur ou un droit voisin pour la création artistique » dans le cadre des enseignements artistiques obligatoires ».

L'article L312-9 du code de la propriété intellectuelle indique quant à lui que les élèves « *reçoivent de la part d'enseignants préalablement sensibilisés sur le sujet une information sur les risques liés aux usages des services de communication au public en ligne, sur les dangers du téléchargement et de la mise à disposition illicites d'œuvres ou d'objets protégés par un droit d'auteur ou un droit voisin pour la création artistique* ».

Le site Internet zdnet.fr révélait en juillet 2011 le bilan chiffré de l'activité de la Haute autorité. Il révèle que « *sur les 18 millions de saisines des ayants droit, la Hadopi a averti par courriel 470.878 abonnés. Un peu plus de 20.000 lettres recommandées ont été envoyées. Pour la haute autorité, l'écart entre les abonnés avertis lors de la première et deuxième phase de la réponse graduée souligne l'efficacité et la pédagogie du dispositif* ».

A priori donc, selon la HADOPI, il semble que la Loi fasse son œuvre. Cependant, rien n'indique que les utilisateurs avertis n'ont tout simplement pas changé de méthode pour télécharger les œuvres sans se faire prendre[184]

Il est aussi possible d'adopter une autre lecture de ces résultats. Ce mécanisme a été mis en œuvre pour appréhender un phénomène massif et diffus par une réponse plus simple et plus souple. Or, d'après les données chiffrées, il aurait été effectué près de 18 millions de constats. Difficile de croire alors que cette procédure n'encombrera pas les prétoires, d'où un tri nécessaire. Il existe bien le moyen de l'ordonnance pénale, mais comme nous l'évoquions, il y a fort à parier que les utilisateurs s'opposeront de manière quasi systématique afin de procéder à un débat contradictoire devant un juge. Cela pose la question du respect du principe de l'égalité devant la Loi. Si la sanction n'est pas systématique, les utilisateurs ne sont donc pas sur un pied d'égalité et rien ne nous permet de savoir pourquoi tel individu sera sanctionné et non un autre.

Enfin, les difficultés juridiques et techniques évoquées plus hauts sont un frein à la bonne réception par l'utilisateur des dispositions législatives. Le système de sécurisation par exemple a parfois été qualifié de « *permis de surfer* »[185] puisque par ce moyen, l'utilisateur est sensé pouvoir contrôler l'usage fait de sa connexion et se défendre devant le juge le cas échéant. Malheureusement, la sécurisation ne garantit rien, l'utilisateur n'étant jamais à l'abri d'un détournement de sa ligne. Cette procédure complexe et confuse pour l'utilisateur lambda ne le place pas dans une situation confortable puisqu'il semble bien difficile pour lui de respecter la Loi[186]. Il n'est alors pas certain qu'il changera son comportement.

[184] Le site ReadWriteWeb a, à ce sujet, publié le 4 janvier 2010 quelques moyens de contournement du dispositif HADOPI <http://fr.readwriteweb.com/2010/01/04/usages/comment-contourner-hadopi-solutions-anti-hadopi/>

[185] Vincent Gautrais , Dossier spécial « Hadopi : regards du dehors », Perspectives, 1° Analyse coûts/bénéfices, dans Revue Lamy Droit de l'Immatériel, n°67, pages 87 à 94, janvier 2011

[186] Bien que le Conseil Constitutionnel ait considéré dans sa décision du 10 juin 2009 au considérant 7 qu'il a été satisfait à « *l'objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi* »

II. La méfiance de l'utilisateur à l'égard des intentions règlementaires

Le législateur affiche une volonté et des objectifs clairs lors de l'élaboration de ses lois. Cependant, leur mise en œuvre fragile (A) et les germes inquiétantes qu'elles portent en elles (B) n'ont pas pour effet de rassurer l'utilisateur.

A. Une méfiance au regard de la législation, fruit d'une transparence et d'une lisibilité insuffisante

Les deux Lois que sont la HADOPI et la LOPPSI 2 tendent à rehausser la méfiance de l'utilisateur à l'égard de ces dispositions parfois obscures. Dans un cas comme dans l'autre, la crainte d'une surveillance généralisée d'Internet est grandissante et peut conduire les utilisateurs à se détourner de la loi. La vertu pédagogique de la loi HADOPI est incertaine et l'immixtion qu'elle produit, comme la LOPPSI 2, par l'intermédiaire de logiciels espions, peut tout à fait inspirer la crainte.

Ce manque de visibilité peut-être le nid d'effets pervers et inattendus. Alors que le législateur cherche à combattre les téléchargements illicites et la cybercriminalité, la connexion Internet est au cœur de tous les maux. La peur suscitée par cet « *espionnage* », bien qu'entouré de garanties, peut pousser l'utilisateur vers de nouveaux moyens afin de se protéger des intrusions faites par le législateur. Par exemple, l'usage de la cryptologie pourrait tout à fait être utilisé à plus haute fréquence pour rendre l'identification d'un ordinateur extrêmement difficile sur le réseau. Ce climat de suspicion n'est guère salvateur pour la protection des intérêts en cause. L'utilisateur est au cœur d'une tourmente qu'il serait souhaitable d'éclaircir en offrant des garanties certaines et des dispositions législatives à l'abri de toute critique afin de bénéficier d'une plus grande légitimité et du regard bienveillant de l'ensemble des internautes.

En somme, bien que la LOPPSI 2 puisse permettre de réprimer un comportement qui pose des difficultés au processus HADOPI, il n'est pas certain que l'utilisateur soit réceptif aux objectifs posés. Les doutes persistent, et il est à craindre que l'utilisateur se retourne contre la Loi.

B. Une méfiance justifiée par la crainte du filtrage d'Internet

Les lois HADOPI semblent être la source de nouvelles craintes et difficultés qu'il convient de mettre succinctement en lumière. Cela concerne le filtrage du web. A titre de rappel, le principe du filtrage consiste à équiper les ordinateurs ou les réseaux d'outils permettant de filtrer les sites web indésirables en fonction de leur URL (liste noire), de leur contenu (analyse de mots clés) ou de leur type de contenu (téléchargement). Il va à l'encontre des principes fondamentaux régissant la neutralité d'Internet qui exige une transmission des données par les opérateurs sans en examiner le contenu, sans prise en compte de la source ou de la destination des données, sans privilégier un protocole de communication et sans en altérer le contenu[187].

En effet, l'architecture du réseau Internet a été conçue selon le principe de bout-à-bout[188]. Il établit que *« plutôt que d'installer l'intelligence au cœur du réseau, il faut la situer aux extrémités : les ordinateurs au sein du réseau n'ont à exécuter que les fonctions très simples qui sont nécessaires pour les applications les plus diverses, alors que les fonctions qui sont requises par certaines applications spécifiques seulement doivent être exécutées en bordure de réseau. Ainsi, la complexité et l'intelligence du réseau sont repoussées vers ses lisières. Des réseaux simples pour des applications intelligentes[189].* » Lawrence Lessig expose à ce sujet[190] : « *que les auteurs du réseau [Internet] aient eu conscience ou non de ce qui naîtrait de leur création, ils l'ont bâtie en fonction d'une certaine philosophie : en un mot, l'idée selon laquelle le réseau lui-même ne serait pas en mesure de réguler son mode de croissance. Ce sont les applications qui le feraient. Tel était l'enjeu d'une*

[187] D'après les propos de Benjamin Bayart lors des Rencontres mondiales du logiciel libre de 2009
[188] Aussi connu sous le nom de *end to end*
[189] Lawrence Lessig, *L'Avenir des idées*, 2005, Presses universitaires de Lyon, 1re partie, paragraphe 75 dans l'édition numérique des Presses universitaires de Lyon
[190] Lawrence Lessig, *L'Avenir des idées*, 2005, Presses universitaires de Lyon, 1re partie, Chapitre 2 « Les fils, câbles et biens communs » dans l'édition numérique des Presses universitaires de Lyon

structure end-to-end[191]». En somme, il s'agit de laisser le contrôle du réseau aux utilisateurs, et ainsi « *favoriser un modèle acentré, dans lequel l'intelligence est poussée en périphérie* »[192].

Or, en obligeant l'utilisateur à sécuriser sa ligne *via* le logiciel espion labellisé par la HADOPI, c'est bien le principe du *end-to-end* qui est remis en cause, on pousse la responsabilité et l'usage de cette responsabilité vers les extrémités, à savoir l'utilisateur lui-même[193]. En effet, la surveillance des contenus aux périphéries du réseau permet la mise en place d'une forme de filtrage qui remet en cause la neutralité du net par le biais de ses propres fondements. La « *corruption* » de l'accès à Internet de l'utilisateur empêche ainsi toute neutralité.

En outre, l'article L331-23 du Code de la propriété intellectuelle[194] dispose que « *(la HADOPI) évalue, en outre, les expérimentations conduites dans le domaine des technologies de reconnaissance des contenus et de filtrage par les concepteurs de ces technologies, les titulaires de droits sur les œuvres et objets protégés et les personnes dont l'activité est d'offrir un service de communication au public en ligne. Elle rend compte des principales évolutions constatées en la matière, notamment pour ce qui regarde l'efficacité de telles technologies, dans son rapport annuel prévu à l'article L. 331-14* ».

Il faut ajouter à cela l'article L336-2 du Code de la propriété intellectuelle[195] qui dispose qu' « *en présence d'une atteinte à un droit d'auteur ou à un droit voisin occasionnée par le contenu d'un service de communication au public en ligne, le tribunal de grande instance[…] peut ordonner à la demande des titulaires de droits sur les œuvres et objets protégés, de leurs ayants droit, des sociétés de perception et de répartition des droits visées à l'article L. 321-1 ou des organismes de défense professionnelle visés à l'article L. 331-1, toutes mesures propres à prévenir ou à faire cesser une telle atteinte à un droit d'auteur ou un droit voisin, à l'encontre de toute personne susceptible de contribuer à y remédier* ».

En somme, le législateur semble bien apporter aux ayants-droit les moyens de demander au juge d'imposer une mesure assimilable à la technique du filtrage, et ce à titre d'expérimentation.

N'oublions pas non plus que la loi LOPPSI 2 consacre également une partie de ses dispositions au filtrage[196]. L'article 4 de la loi octroie à une autorité administrative le droit, sans arbitrage par un juge, d'imposer aux FAI le filtrage de contenus de nature pédopornographique[197].

Enfin il faut souligner l'influence du potentiel traité[198] ACTA[199]. Il a été négocié entre l'Union Européenne et ses États membres, les États-Unis, l'Australie, le Canada, le Japon, le Mexique, le Maroc, la Nouvelle Zélande, Singapour, la Corée du Sud, et la Suisse. L'objectif de l'ACTA est de lutter contre les atteintes aux droits de propriété intellectuelle, à savoir la contrefaçon et le piratage, en encourageant la coopération et la surveillance à l'échelle internationale.

---

[191] En français, le principe du bout à bout
[192] « Les caractéristiques techniques d'Internet et ses potentialités politiques »
[193] Pascal Adam, *Numériques, Internet, perspectives… arsenic et vieilles dentelles (la suite)*, publié le 21/12/2001 <http://blogs.orange-business.com/live-france/2011/12/numerique-internet-prospectives-part2-hadopi.html>
[194] Article L331-23 CPI - Créé par LOI n°2009-669 du 12 juin 2009 - art. 5 <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000020740330&cidTexte=LEGITEXT000006069414>
[195] Article L336-2 CPI - Modifié par LOI n°2009-669 du 12 juin 2009 - art.10 <http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006069414&idArticle=LEGIARTI000020740350&dateTexte=20111118>
[196] Sur ce thème, pour aller plus loin, voir le dossier sur le filtrage du net mis en place par la Quadrature du Net, <http://www.laquadrature.net/fr/filtrage-du-net>
[197] LOI n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, Article 4 : « *Lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du code pénal le justifient, l'autorité administrative notifie aux personnes mentionnées au 1 du présent I les adresses électroniques des services de communication au public en ligne contrevenant aux dispositions de cet article, auxquelles ces personnes doivent empêcher l'accès sans délai.* »
< http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&categorieLien=id>
[198] <http://trade.ec.europa.eu/doclib/docs/2011/may/tradoc_147938.pdf>
[199] Anti-Counterfeiting Trade Agreement

Certaines dispositions laissent craindre un risque d'une forme de filtrage. L'article 27 dispose notamment qu'un Etat partie à l'accord pourra « *ordonner à un fournisseur de services en ligne de divulguer rapidement au détenteur du droit des renseignements suffisants pour lui permettre d'identifier un abonné dont il est allégué que le compte aurait été utilisé en vue de porter atteinte à des droits, lorsque le détenteur du droit a présenté des allégations suffisantes sur le plan juridique, relativement à une atteinte à une marque de fabrique ou de commerce ou au droit d'auteur ou à des droits connexes, et lorsque ces renseignements sont demandés aux fins de la protection ou du respect de ces droit ».* Ce même article prévoit également qu'*«une Partie peut prévoir que ses autorités compétentes seront habilitées […] à ordonner à un fournisseur de services en ligne de divulguer rapidement au détenteur du droit des renseignements suffisants pour lui permettre d'identifier un abonné dont il est allégué que le compte aurait été utilisé en vue de porter atteinte à des droits ».*

Les opposants[200] au texte dénoncent le fait que les fournisseurs d'accès à Internet auraient ainsi l'obligation de censurer tout contenu et d'interdire tout accès à un site ou plate-forme portant atteinte au droit d'auteur. En outre, c'est la possibilité de confier, à des acteurs privés, sans passer par le juge, le soin d'exercer des missions de police (surveillance et collection de preuves) et de justice (sanctions)[201].

L'article 27 prévoie comme garde-fou que ces procédures devront être «*mises en œuvre d'une manière qui [...] préserve les principes fondamentaux comme la liberté d'expression, les procédures équitables et le respect de la vie privée*».

Le Conseil fédéral de Suisse a exprimé[202] à propos du risque de filtrage que « *le verrouillage d'Internet par un fournisseur d'accès suscite des réserves comparables à celles formulées à l'égard de la réponse graduée. Ces mesures ne sont guère compatibles avec le droit à la liberté d'expression, et le fait que ce verrouillage ne soit pas ordonné par un tribunal, mais qu'il émane d'une entreprise privée le rend encore plus problématique* ».
« *On évoque l'emploi de technologies de filtres en guise d'alternative, mais elles se heurtent également à des réticences liées à la protection des données. On craint, de surcroît, qu'elles ralentissent sérieusement la vitesse de connexion à Internet. Pour l'heure, cette approche ne semble donc pas non plus très prometteuse d'un point de vue pratique* ».

Nous noterons cependant que la CJUE vient de porter un coup d'arrêt au développement du filtrage dans le cadre d'un renvoi préjudiciel[203]. En effet, dans son arrêt du 24 novembre 2011, elle établit clairement que « *le droit de l'Union s'oppose à une injonction, prise par une juridiction nationale, d'imposer à un fournisseur d'accès à Internet la mise en place d'un système de filtrage afin de prévenir les téléchargements illégaux de fichiers* ». La Cour a jugé que le droit de l'UE (notamment les directives 2000/31, 2001/29, 2004/48, 95/46 et 2002/58) s'oppose à une telle injonction, qui menacerait un certain nombre de droits et libertés (liberté d'entreprendre, liberté d'information, protection des données à caractère personnel...)[204]. Elle a par ailleurs confirmé cette position dans une autre décision rendue le 16 février 2012[205] estimant que « *l'exploitant d'un réseau social en ligne ne peut être contraint de mettre en place un système de filtrage général, visant tous ses utilisateurs, pour prévenir l'usage illicite des œuvres musicales et audiovisuelles* ». Elle estime qu' « *une telle obligation ne respecterait pas l'interdiction d'imposer à un tel prestataire une obligation générale de surveillance ni l'exigence d'assurer le juste équilibre entre, d'une part, la protection du droit d'auteur et, d'autre part, la liberté d'entreprise, le droit à la protection des données à caractère personnel et la liberté de recevoir ou de communiquer des informations* ».

---

[200] Et notamment la quadrature du net <http://www.laquadrature.net/fr/ACTA>
[201] http://www.depresdeloin.eu/
[202] http://www.ejpd.admin.ch/content/dam/data/pressemitteilung/2011/2011-11-30/ber-br-f.pdf
[203] CJUE, 24 nov.2011 affaire C-70/10
<http://curia.europa.eu/jurisp/cgibin/gettext.pl?where=&lang=fr&num=79888875C19100070&doc=T&ouvert=T&seance=ARRET>
[204] Pour plus d'informations : <http://www.pcinpact.com/news/67217-sabam-scarlet-filtrage-blocage-hadopi.htm>
[205] CJUE, 16 fév.2012 affaire C-360/10 Sabam
< http://curia.europa.eu/jcms/upload/docs/application/pdf/2012-02/cp120011fr.pdf>

En somme, dans un contexte où le filtrage est envisagé comme une solution au niveau national comme au niveau international, il faudra composer avec la jurisprudence de la CJUE qui ne manquera pas de contrôler et mettre en balance les intérêts en cause au regard des droits et libertés fondamentaux.

Conclusion finale

Nous l'avons constaté à travers ce mémoire, les lois *HADOPI* et *LOPPSI 2*, qui pourtant on des objectifs louables, souffrent d'une crise de légitimité. Est-ce à dire qu'elles n'auront aucun impact positif ? Certainement pas. La connexion Internet de l'utilisateur est devenue une véritable passerelle pour combattre certaines infractions accentuées dans l'univers spécifique du monde numérique. Si le contrôle qu'il a de sa connexion est remis en cause, c'est parce qu'il a manqué à son obligation de vigilance ou parce que l'autorité judiciaire a eu besoin, à un moment donné, de la détourner parce qu'il est suspecté d'avoir commis une infraction liée à la criminalité organisée. Nécessairement, la *LOPPSI 2* aidera les enquêteurs à mieux combattre le crime sur Internet. Les lois *HADOPI*, même si elles ne connaissent pas le succès et le résultat fulgurant défendu et escompté par ses instigateurs, auront le mérite d'avoir fait changer le comportement de quelques uns et d'ouvrir le débat sur de nouvelles alternatives pour « *consommer* » autrement la musique.

Les difficultés juridiques et techniques rencontrées peuvent mettre en exergue des points quelque peu oubliés des objectifs du législateur. Comme le souligne très bien Vincent Gautrais[206], « *le moyen de concilier « droit » et « réalité » passera sans doute par une meilleure reconnaissance des nouvelles prérogatives des utilisateurs ; ce que le droit d'auteur ne fait que très peu. En effet, une prise en compte des « intérêts » des premiers est loin d'être consacrée dans un domaine qui s'intéresse surtout aux « droits » des seconds »*. Ainsi, pour le cas des lois *HADOPI*, nous sommes face à un droit spécial qui ne s'intéresse non pas à développer de meilleures prérogatives pour l'utilisateur pris au sens large du terme, mais qui vient alourdir considérablement sa responsabilité au bénéfice d'intérêts privés. Il n'est ici nullement question de critiquer le droit d'auteur ou le besoin de le protéger, mais plutôt de faire le constat qu'à une époque où Internet fait désormais parti des incontournables de la vie courante, aussi bien pour les particuliers que pour les professionnels, la construction des prérogatives de l'utilisateur par le droit ne se construit que de façon épidermique, réactionnaire voir allergique à de nouvelles pratiques. Il est ainsi dommage que celui-ci soit d'abord vu comme un vecteur de contrefaçon, plutôt qu'un vecteur de liberté d'expression.

Par ailleurs, si la légitimité peine à s'imposer, c'est tout d'abord parce que les deux lois s'attaquent à des droits et libertés fondamentaux. Certes, la liberté d'expression et le droit à la vie privée ne sont pas absolus et peuvent être limités pour des cas bien précis. Mais il est bien difficile d'apporter des garanties stables en retour à l'utilisateur concerné.

La CNIL a eu un apport essentiel concernant ces deux lois puisqu'elle a permis, et continue de mettre en lumière de nombreux risques. Le législateur a d'ailleurs répondu de manière positive à la plupart de ces inquiétudes (différencier les points d'accès publics, protéger le secret professionnel, etc.)

Le Conseil constitutionnel est lui aussi bien présent pour toujours veiller à ce que les dispositions législatives soient conformes aux normes les plus hautes de notre droit. La première d'entre elles, la Constitution, est là pour rappeler les principes et droits fondamentaux de la République française.

Le juge est également une importante garantie pour éviter les dérives. Sa liberté d'appréciation et son indépendance sont autant de marques de confiance pour l'utilisateur. Mais elles supposent d'être intangibles et très solides.

Mais malgré ces assurances, le droit se heurte à la technique. A-t-il trouvé ses limites ? Le législateur, lorsqu'il s'empare de ce monde nouveau ne fait-il pas que mettre en avant les difficultés qu'il a à s'y adapter ? Il est très probable que la technique aura certainement toujours une longueur d'avance, non pas parce que le droit est incapable de s'y accommoder, mais du fait que la technologie évolue à une vitesse déconcertante. La technique est difficile à appréhender par sa nature mouvante et instable. Par exemple, pour le cas des logiciels espions, Franck Macrez et Julien Gossa[207] expliquent que s'ils viennent à se répandre, le risque de piratage est accru. En effet, « *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*

[206] Vincent Gautrais , Dossier spécial « Hadopi : regards du dehors », Perspectives, 1° Analyse coûts/bénéfices, dans Revue Lamy Droit de l'Immatériel, n°67, pages 87 à 94, janvier 2011

[207] Franck Macrez et Julien Gossa, « surveillance et sécurisation : ce que l'HADOPI rate », *point n°55 «* Un moyen de désécurisation *»* dans Revue Lamy Droit de l'Immatériel, n°50, pages 79 à 91, juin 2009

trous de sécurité qui sera découvert dans ces logiciels, aura à sa disposition des millions de cibles potentielles ». Cela démontre clairement que si la technique peut servir la loi, il est tout à fait possible de la retourner contre elle.

Enfin et surtout, il faut rappeler comme le disait Montesquieu, qu'"*une chose n'est pas juste parce qu'elle est loi ; mais elle doit être loi parce qu'elle est juste*."[208]

[208] Montesquieu – cahiers, I, Paris, Grasset, p393

Annexe I – Tableau récapitulatif à l'attention de l'utilisateur

HADOPI	
Titulaires d'accès soumis à l'obligation de vigilance	• **Particuliers** : le titulaire de l'accès est soumis à l'obligation de vigilance • **Entreprise, collectivité territoriale, Université, Bibliothèque, Bar et autres points d'accès publics** : le titulaire de la connexion est soumis à l'obligation de vigilance mais pourra vraisemblablement bénéficier d'aménagements de la sanction • **« Hotspot » (neuf wifi, Free wifi, etc.)** : l'utilisateur doit s'authentifier pour bénéficier de l'accès à Internet et navigue par le biais de sa propre adresse IP, distincte de celle du titulaire de l'accès à Internet, il est donc identifiable et passible de la sanction
Conditions de mise en œuvre	• **Conditions préalables :** - En tant que titulaire de la ligne, s'être vu recommandé par la CPD de mettre en œuvre un moyen de sécurisation après constat d'une première infraction - Dans les 6 mois suivant cette recommandation, s'être vu notifié le constat d'une nouvelle infraction relative à l'obligation de vigilance - Dans l'année suivant cette recommandation, s'être vu notifié le constat d'une nouvelle infraction relative à l'obligation de vigilance • **Faits constitutifs :** - Ne pas avoir mis en œuvre un moyen de sécurisation - Avoir manqué de diligence dans la mise en œuvre du moyen de sécurisation
Sanctions	• Contravention de cinquième classe d'un montant maximum de 1.500 euros portée à 7.500 euros pour les personnes morales • Peine complémentaire de suspension de la connexion Internet pendant un mois (selon l'appréciation du juge, à priori cette sanction s'adresse aux particuliers)
Moyens de prévention	• **Pour les particuliers :** (concernant la marche à suivre, rapprochez vous de votre FAI) - utiliser une clé WPA ou WPA-2 plutôt qu'une clé WEP généralement configurée par défaut - Préférez une adresse IP statique pour faciliter la preuve d'usurpation si vous en êtes victime - utiliser un logiciel antivirus, un logiciel antispyware, un pare-feu de manière à empêcher l'accès aux serveurs de P2P ou de téléchargement direct (Megaupload, Rapidshare…), etc. • **Pour les entreprises :** - Mise en place d'une solution de sécurité unifiée des postes de travail regroupant un antivirus classique et divers services permettant de réguler l'accès aux sites de téléchargement et filtrer les contenus qui transitent par le réseau d'entreprise - Mise en place d'un système de filtrage bloquant les extensions en .mp3, .avi, .wma - Bloquer les applications de P2P comme Emule, Kazaa Lite, Bit Torrent, Vuze ou encore Limewire - Se doter d'une Charte d'utilisation d'Internet et des systèmes d'informatique en général. Celle-ci doit être annexée au règlement intérieur et permettra de circonscrire les usages faits d'Internet au sein de l'entreprise - Mise en place après consultation des représentants du personnel d'un système de surveillance préalablement porté à la connaissance des salariés, traduisant l'intérêt légitime de l'employeur, proportionné et limité à la lutte contre les téléchargements illicites, et déclaré à la CNIL
Moyens d'exonération	• Démontrer la sécurisation effective de son accès : toute sécurisation est recevable mais l'utilisation d'un moyen labellisé est un élément positif dans le cadre de l'appréciation des faits par la CPD (*liste des moyens à venir : à ce jour, l'opérateur Orange a édité un logiciel « Contrôle de téléchargement » et la société H2DS a lancé quand à elle son logiciel « ISIS », mais aucun de ces deux logiciels n'est à ce jour labellisé*) • Démonstration d'un motif légitime : voir les causes d'irresponsabilité pénale posées à l'article 122-1 et s. du Code pénal, le titulaire d'un accès wifi hotspot pourra faire une demande auprès de son FAI pour identifier la personne qui a utilisé son accès pour commettre l'infraction, besoin impérieux de se connecter à Internet, etc. • La preuve se fait par tout moyen (courriel reçu de la part du fournisseur d'accès, relevé d'état du système, attestation du gestionnaire de pare-feu, etc.)

LOPPSI 2	
Utilisateurs susceptibles d'être surveillés	- Les entreprises et les particuliers entrent dans le champ d'application de la Loi - Exclusion des systèmes automatisés de traitement des données se trouvant dans les lieux visés aux articles 56-1, 56-2 et 56-3 du Code de procédure pénale - Exclusion du véhicule, du bureau et du domicile des avocats, des magistrats, des députés et des sénateurs - Exclusion des points d'accès publics
Conditions de mise en œuvre requises à peine de nullité	- Les infractions spécifiquement visées à l'article 706-73 du Code de procédure pénale (principalement celles relevant de la criminalité organisée) - Localisation exacte ou description détaillée des systèmes de traitement automatisé de données ainsi que la durée des opérations - Durée des opérations (4 mois maximum, renouvellement exceptionnel de 4 mois possible)
Elements susceptibles de surveillance	- Tous lieux (véhicule ou lieu privé) - Données informatiques utiles à la manifestation de la vérité telles qu'elles s'affichent sur un écran pour l'utilisateur - Les opérations révélant des infractions autres que celles visées dans les décisions ne constituent pas une cause de nullité des procédures incidentes - Exclusion des données relatives à la vie privée étrangère aux infractions visées dans les décisions
Destruction des données	- Les enregistrements des données informatiques sont détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique.

Bibliographie

Manuels :

- Gérard Cornu, Association Henri Capitant, « Vocabulaire Juridique », 7e éd. PUF
- J. Larrieu, « *Droit de l'Internet* », 2ème édition Ellipses
- Emmanuel Derieux et Agnès Granchet – « *Lutte contre le téléchargement illégal - Loi Dadvsi et Hadopi* »
- Christiane Féral-Schuhl – Cyberdroit – Le droit à l'épreuve de l'Internet – 6e édition Dalloz
- Christophe Caron, Droit d'auteur et Droits voisins, Litec, 2e éd., 2010

Revues :

- Dussolier Séverine, « L'utilisation légitime de l'œuvre : un nouveau sésame pour le bénéfice des exceptions en droit d'auteur », Communication Commerce électronique, n°11, novembre 2005, étude 38. A propos de la décision Cass. Crim., 30 mai 2006, n°05-83.335, F-D, SEV et al. c/ Aurélien D, Juris-Data n°2006-033837
- Christophe CARON – « La source de la copie privée doit-elle être licite ? », dans Communication Commerce électronique n°9, Septembre 2006, comm.118, et à propos de la décision CA Versailles, çe ch. Corr., 16 mars 2007, O. : Juris-Data n°2007-331563 « Source licite et usage privé du copiste », dans Communication Commerce électronique n°7, juillet 2007, comm.91
- Julia Heinich, « La nouvelle obligation de surveillance de sa ligne : nouvelle responsabilité civile ? », dans Revue Lamy Droit de l'Immatériel, 67, 2011
- Vincent Gautrais, « *Hadopi : regards du dehors* », dans Revue Lamy Droit de l'Immatériel, Perspectives, Dossier spécial, 2011
- Florence Gaullier, Elise Pasacal-Heuze, Gilles Vercken, « *Les derniers décrets d'application des lois HADOPI* », dans Revue Lamy Droit de l'Immatériel, 2010
- Nicolas Catelan, « *La protection du droit d'auteur : une négligence caractérisée ?* », Revue Lamy Droit de l'Immatériel, 2011
- Julien Couard, « *Interview d'un praticien* », dans Revue Lamy Droit de l'Immatériel, 2011
- Philippe Belloir, « *LOPPSI : un projet pour la captation de données informatiques* », dans Revue Lamy Droit de l'Immatériel, 2009
- Hubert Bitan, Dossier spécial Loi « CREATION ET INTERNET » - Réflexions sur la loi *Création et Internet* et sur le projet de loi « *HADOPI 2* », dans Revue Lamy Droit de l'Immatériel, 2009
- Myriam Quéméner, « *Projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2) : les réponses en matière de cybercriminalité* », dans Communication Commerce électronique n°11, Novembre 2010
- Article collectif : DADVSI 2, HADOPI, *Création et internet... De bonnes questions? De mauvaises réponses*, dans Recueil Dalloz 2008, p. 2290
- Derieux, E. et Granchet, A., « *Jurisprudence de la Cour européenne des droits de l'Homme* », Droits des médias. Droit français, européen et international, LGDJ, 5e éd., 2008, p.945-962
- Gautrons – « *"La riposte graduée" (à nouveau) épinglée par le Conseil Constitutionnel. Ou la délicate adéquation des moyens aux fins* », RLDI/51, juillet 2009 p.66).
- Marcel Moritz – Revue Lamy Droit de l'Immatériel – 2008 – « *Les perquisitions en ligne et la surveillance d'internet* »
- Franck Macrez et Julien Gossa, « *surveillance et sécurisation : ce que l'HADOPI rate »,* dans Revue Lamy Droit de l'Immatériel, 2009
- Jean-Sébastien Mariez, « *Hadopi… trois petits points de suspension* », dans Revue Lamy droit de l'Immatériel, 65, Actualités créations immatérielles, éclairage, 2010
- Laurent Saenko, « *Le nouveau délit d'usurpation d'identité numérique* », dans Revue Lamy Droit de l'Immatériel, 72, 2011
- Diane de Bellescize, « *Hadopi 1 et Hadopi 2, en attendant Hadopi 3 ?* », dans Rec. Dalloz 2010, p293

Publications diverses :

- Claudine Guerrier, « *Captation de données et vie privée en 2011* », <www.juriscom.net/documents/donneesperso20110318.pdf>
- Vocabulaire de l'informatique et de l'Internet – Journal Officiel du 16 mars 1999
- 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, voir « *Barrières de sécurité* », p. 1946.
- Etienne Papin – « *La captation des données informatiques : enjeux et conséquences pour les entreprises de la LOPPSI 2* », <http://www.cio-online.com/contributions/lire-la-captation-des-donnees-informatiques%C2%A0-enjeux-et-consequences-pour-les-entreprises-de-la-loppsi-2-408-page-1.html>

Liens :

- ***Institutionnels***

HADOPI : <www.hadopi.fr>
CJUE : <http://curia.europa.eu>
Conseil Constitutionnel : <www.conseil-constitutionnel.fr>
Le Sénat : <www.senat.fr>
Légifrance : <http://www.legifrance.gouv.fr/>
Cour européenne des droits de l'homme : <http://www.echr.coe.int/echr/>
Cour de cassation : <www.courdecassation.fr>
ARCEP: <www.arcerp.fr>

- ***Journalistiques***

Juriscom : <www.juriscom.net>
Numerama : <www.numerama.com>
Association des fournisseurs d'accès et de services Internet : <http://www.afa-france.com>
Vie publique : <www.vie-publique.fr>
Rue89 :<www.rue89.com>
Zdnet : <www.zdnet.fr>
PCinpact : <http://www.pcinpact.com/>
Le Monde : <www.lemonde.fr>
Le Figaro : <www.actualite.lefigaro.fr/>

- ***Divers***

Le monde du droit : <www.lemondedudroit.fr>
e-juristes : <www.e-juristes.org/>
Comment ça marche : <www.commentcamarche.net/>
Lexatic : <http://www.lexatic.com/>
CIO Online : <www.cio-online.com>
Readwriteweb : <www.readwriteweb.com/>

Conférences :

- Conférence du 17 mars 2011, « LOPPSI 2 : Un nouvel arsenal contre la cybercriminalité » organisé par le Master 2 Droit du Multimédia et de l'Informatique Université Panthéon-Assas Paris 2 en partenariat avec l'association française des juristes d'entreprise et juriscom.net »

Vidéos :

- Alain Bensoussan, Avocat, lors d'une interview par mydsitv.accenture.fr « *Le média qui analyse et qui décrypte l'actualité des DSI* »
  < http://www.youtube.com/watch?v=SbLjtXy5FIY>

Textes de lois :

- Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&categorieLien=id>

- Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020735432&categorieLien=id>

- Loi relative à la protection pénale de la propriété littéraire et artistique sur internet

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021208046&categorieLien=id>