

# Le téléchargement illicite d'œuvres protégées par le droit d'auteur

Rapport à Monsieur le Ministre de la Culture et de la Communication

Jean Cédras

- avril 2007 -

Le 12 avril 2007

Monsieur le Ministre de la Culture et de la  
Communication

*Monsieur le Ministre,*

*Par lettre de mission du 16 janvier 2007, vous m'avez chargé de rechercher des solutions au problème du téléchargement illicite, complémentaires de la répression de la contrefaçon, « adaptées au traitement d'une grande masse d'infractions qui, prises isolément, occasionnent un trouble limité ».*

*Vous m'avez suggéré « d'imaginer un dispositif combinant des actions d'information et de sensibilisation des internautes, notamment par l'envoi de courriels individualisés, et des sanctions pécuniaires adaptées et proportionnées ». Le dispositif à vous proposer devait « être articulé avec le dispositif actuel et impliquer les fournisseurs d'accès à Internet ». En particulier, avez-vous précisé, « il pourrait être utile d'envisager dans quelle mesure l'abonné pourrait en tant que tel être responsabilisé, en s'appuyant notamment sur les dispositions de l'article L. 335-12 du Code de la propriété intellectuelle ».*

*Ma mission consistait donc à explorer ces possibilités et à « formuler des propositions, en analysant leur compatibilité avec les principes juridiques fondamentaux, notamment les droits de l'homme et la protection de la vie privée, ou avec les engagements internationaux de la France ».*

*J'ai pu rencontrer au ministère de nombreux représentants des acteurs économiques et institutionnels concernés et m'entretenir longuement avec certains d'entre eux par téléphone ou par courriel. Je tiens à saluer ici l'apport inestimable de M. l'Ingénieur général Jean Berbinau. En revanche, malgré mes demandes, il ne m'a pas été donné de rencontrer les représentants des consommateurs, ce que je regrette.*

*Je vous prie de bien vouloir trouver ci-joint la synthèse de mes recherches.*

*Croyez, Monsieur le Ministre, à l'expression de ma respectueuse considération.*

Jean  
CEDRAS

## Le téléchargement illicite d'œuvres protégées par le droit d'auteur

### Sommaire

1. Les logiciels d'échanges de pair à pair
2. Un équilibre social et économique
3. Le domaine public au sens large
4. La licence globale
5. Le droit exclusif
6. Le volume des téléchargements illicites
7. Des réalités criminologiques différentes
8. La « réponse graduée »
9. Une sanction encourue disproportionnée
10. Le droit positif
11. L'exception de copie privée
12. La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
13. Le Groupe de travail « Article 29 »
14. Les décisions de la CNIL
15. En matière de jeux vidéos
16. En matière musicale
17. En matière audiovisuelle
18. La doctrine de la CNIL
19. Une épée de Damoclès juridictionnelle ?
20. Le constat d'un téléchargement illicite à l'heure actuelle
21. Le but à atteindre
22. La responsabilité de l'abonné pour contrefaçon au regard de petits téléchargements illicites par le pair à pair ne peut plus être retenue
23. La responsabilisation du fournisseur d'accès pour défaut de fourniture de filtrage et celle de l'abonné pour défaut de surveillance de sa machine
24. La proposition de créer une contravention visant le fournisseur d'accès
25. La proposition de créer une contravention visant l'abonné
26. La pertinence et la fiabilité du filtrage des œuvres protégées sur le poste de l'abonné
27. Le filtrage des œuvres protégées installé chez le fournisseur d'accès
28. Une esquisse de solution
29. D'autres réponses

Annexe : Personnalités consultées

## Le téléchargement illicite d'œuvres protégées par le droit d'auteur \*

1. Techniquement possible, l'accès libre, gratuit et sans limite aux œuvres protégées est inadmissible éthiquement, économiquement et juridiquement. S'agissant des jeux, du son et de l'image, on pense aux commodités offertes par le téléchargement illicite sur Internet, dont la facilité installe une culture de la gratuité dans les esprits, spécialement chez les jeunes gens. Il en va ainsi des **logiciels d'échange de pair à pair** (peer to peer, P2P, c'est-à-dire d'ordinateur à ordinateur). Le mécanisme est le suivant : un internaute installe sur son ordinateur un logiciel de partage de fichiers. Il peut ainsi communiquer avec tous les ordinateurs semblablement connectés. Il énonce les fichiers d'œuvres recherchées. Le logiciel les télécharge automatiquement sur son disque dur (téléchargement descendant). Simultanément (selon les versions), il met à la disposition des autres internautes l'œuvre qu'il est en train de télécharger et toutes celles du dossier partagé sur son propre disque dur (téléchargement ascendant). Une première génération de logiciel d'échanges impliquait un serveur centralisé pour mettre en relation les internautes connectés au service. Aujourd'hui, les échanges sont décentralisés et les fichiers mutualisés. Les logiciels Bittorrent et eDonkey sont les plus connus. L'installation et l'utilisation en sont simples et rapides, le coût dérisoire, la qualité des copies parfaite.

Pour obvier à ce phénomène, l'on dispose soit du droit d'auteur (droit exclusif) soit de la licence globale. La solution de la licence globale a été écartée par le législateur français. Reste le droit d'auteur, lequel implique le contrôle de l'utilisation des œuvres, avec des risques sérieux pour la vie privée des internautes. Or, si certains d'entre eux sont indéliçables, d'autres sont irréprochables. Autant que l'accès gratuit aux œuvres protégées, il serait inadmissible que ceux qui opèrent des téléchargements licites soient l'objet de suspicion, voire puissent être enregistrés dans des fichiers de délinquants potentiels.

2. Le système du droit d'auteur et des droits voisins repose sur un **équilibre social et économique** entre domaine payant et domaine public. D'une part les créateurs et leurs ayants droit ont certaines prérogatives sur les œuvres de l'esprit : c'est la propriété littéraire et artistique, qui confère droit moral et rémunération, c'est le domaine payant. D'autre part les amateurs de ces œuvres (le public) peuvent dans

certaines conditions y accéder ou les utiliser librement : on parle alors de domaine public au sens large, notion qui participe de la diffusion de la culture dans son innovation et dans sa diversité. Non seulement ce souci d'équilibre est-il universel mais encore il innervé tous les droits de la propriété intellectuelle et industrielle, tels ceux des brevets ou des marques.

### 3. Quel est le contenu du **domaine public au sens large** ?

Au sens strict, tout d'abord, le domaine public se compose d'une part des œuvres qui, par leur nature, ne peuvent donner prise à un droit d'auteur (actes officiels, etc.) et d'autre part de celles qui sont « tombées » dans le domaine public, sous leur aspect patrimonial, par écoulement du temps.

Du domaine public stricto sensu on peut rapprocher, mais rapprocher seulement, les œuvres que leurs créateurs ont déclarées libres de certains droits. Il s'agit de certains aspects du phénomène du Web2.0 (Web deuxième génération) appelés copyleft (antonyme de copyright) ou encore « sites communautaires ». Les internautes qui utilisent les logiciels libres ont par exemple l'obligation de redistribuer les logiciels reçus et modifiés par eux avec leurs codes sources. Les licences « copyleft » de type GPL (General Public Licence) ou « art libre » utilisent pleinement le régime du copyright pour concéder des droits et des devoirs aux usagers, et ces licences ressortissent au droit des contrats. Ce n'est que lorsque le logiciel sera tombé dans le domaine public, qu'il soit libre ou propriétaire, qu'il n'y aura plus de restrictions à ce que les usagers pourront en faire.

Parmi d'autres exemples, l'éditeur public scientifique américain PLoS (Public Library of Science) publie les résultats de la recherche. Leur consultation est libre et gratuite. Des formules interactives existent : la propriété des données n'est revendiquée par personne et ce sont les utilisateurs qui les enrichissent en les faisant circuler par le truchement des blogs (bloc notes personnels) et des sites de partage. Ainsi, sur Wikipedia (350 millions de visiteurs par mois), les internautes écrivent eux-mêmes les articles de cette encyclopédie en ligne et peuvent améliorer les articles existants. Fondée sur le bénévolat et le partage des connaissances, l'oeuvre peut être librement et gratuitement copiée ou encore mise en ligne sur un autre site. Ainsi encore, sur le français DailyMotion, les internautes peuvent-ils poster leurs propres vidéos et regarder librement celles des autres internautes. Certains, tels MySpace, favorisent un

lien direct et permanent entre artistes et public. Les droit d'auteurs s'appliquent ici encore, mais de façon variable. Le droit de visualisation n'implique pas le droit d'usage commercial, par exemple. Certaines licences de type libre, comme les Creative commons, disposent de plusieurs types de licences pour distinguer facilement ce qui est permis ou interdit : modification, redistribution, usage commercial, etc. Certains de ces sites permettent même l'achat légal de musique en ligne mais le danger est naturellement que ces sites ne soient utilisés pour les téléchargements illicites d'œuvres protégées.

A côté du domaine public lato sensu décrit ci-dessus, existent encore des œuvres qui sont normalement protégées mais pour lesquelles la loi a prévu une exception au droit d'auteur en faveur de chaque membre du public. Il s'agit notamment de la copie privée (pour laquelle une redevance forfaitaire est néanmoins acquittée sur les supports d'enregistrement vierges : CD, DVD, lecteurs de MP3, etc. par leurs fabricants ou importateurs, le coût s'en répercutant au moins partiellement sur le prix de vente au public) ou encore représentation dans un « cercle de famille », tel que défini par la jurisprudence : le cercle constitué par la réunion de parents, d'alliés ou de personnes ayant des relations habituelles. Lorsqu'elles sont invoquées, ces exceptions doivent subir avec succès, au cas par cas, le test en trois étapes imposé par l'art. L. 122-5 al. 4 CPI « Les exceptions énumérées par le présent article ne peuvent porter atteinte à l'exploitation normale de l'œuvre ni causer un préjudice injustifié aux intérêts légitimes de l'auteur ». Toujours est-il que la copie privée et la représentation dans un cercle de famille, exceptions au droit d'auteur, doivent être soigneusement distinguées du téléchargement illicite, violation du droit d'auteur.

**4. La licence globale**, qui recueille les faveurs des organisations de consommateurs et des sociétés d'artistes interprètes, a été considérée puis écartée par le législateur après de sérieuses hésitations. L'une des architectures proposées était la suivante : les reproductions d'œuvres effectuées à usage privé, réalisées par téléchargement descendant, auraient bénéficié de l'exception de copie privée ; quant aux actes de mise à disposition par téléchargement ascendant, ils auraient fait l'objet d'un régime de gestion collective obligatoire. La finalité de la licence globale se rapproche de celle de la licence légale.

Les arguments invoqués contre la licence globale se résument ainsi : 1) optionnelle, elle n'aurait été payée que par les internautes qui téléchargent honnêtement ; obligatoire, elle aurait été payée par tous les internautes pour financer les téléchargements de certains d'entre eux ; 2) le montant de la redevance, par hypothèse faible, serait fixé selon un processus bureaucratique incluant les pouvoirs publics et les consommateurs ; 3) cette modicité sacrifierait substantiellement la rémunération des ayants droit par rapport à celle qu'ils peuvent escompter du droit exclusif ; 4) il s'ensuivrait le tarissement progressif de la création faute de ressources suffisantes car les auteurs n'auraient plus intérêt à créer, les artistes à interpréter ni les producteurs à produire ; 5) sa répartition entre ayants droit serait nécessairement injuste en raison de l'impossibilité de savoir précisément quelles œuvres ont été téléchargées et il faudrait procéder à des sondages, au sens de repérage de ce qui est chargé en balayant Internet; 6) enfin ces sondages avantageraient mécaniquement les titres les plus diffusés et lèseraient corrélativement les auteurs et les artistes peu connus.

Les arguments invoqués en faveur de la licence globale sont les suivants : 1) une rémunération légale, même modique et forfaitaire, est préférable à l'absence de rémunération de la situation actuelle du piratage ; 2) la licence globale est le seul système pratique et efficace applicable, permettant de prendre en compte, dans les calculs de redistribution des redevances, l'ensemble des œuvres circulant au sein du public et non uniquement celles vendues au sein des circuits de distribution ; 3) il est encore avancé la relative facilité de concilier la licence globale avec le principe de chronologie des médias des œuvres audiovisuelles, ce qui peut sembler discutable.

**5. Le droit exclusif** implique que l'utilisateur ait obtenu, hors l'hypothèse d'une exception au droit d'auteur, l'autorisation préalable de l'auteur et des titulaires de droits voisins (représentés normalement par des sociétés civiles) de la représenter ou de la reproduire. Le montant de la redevance est arrêté librement et individuellement entre les parties en fonction de l'utilisation qui sera faite de l'œuvre.

**6. Le volume des téléchargements illicites** menacerait l'industrie culturelle, notamment les producteurs de phonogrammes et de vidéogrammes.

Selon la Direction générale du Trésor et de la Politique économique, la France comptait en 2005 huit millions d'utilisateurs occasionnels et 750 000 utilisateurs



réguliers des réseaux de pair à pair. Il n'y a que quelques dizaines de plaintes par an et un nombre infime de condamnations. Les statistiques policières ne rendent compte que d'une partie minime de la criminalité réelle, le chiffre noir est astronomique.

« L'effet global du piratage sur les ventes de contenu légal est ambigu. D'une part, deux mécanismes pèsent à la baisse sur les ventes d'albums : le téléchargement peut être vu comme un substitut à l'achat d'originaux ou même de copies légales et son coût marginal minime réduit le consentement à payer des utilisateurs. D'autre part, d'autres mécanismes tendent à stimuler les ventes : le piratage peut être considéré comme un moyen de diffusion et d'exposition des œuvres culturelles ; ... la concurrence qu'il exerce sur le marché de la musique conduit à moyen terme à une baisse du prix qui permet à des consommateurs dont le consentement à payer était trop faible de l'acheter et donc à une augmentation de la demande. D'un point de vue qualitatif, on peut toutefois s'attendre à ce que l'effet de substitution l'emporte sur l'effet positif d'apprentissage ».

**En ce qui concerne la musique**, les études disponibles sur le lien entre piratage et baisse des ventes d'œuvres musicales sont peu nombreuses, empiriques et souvent contradictoires. Une étude américaine de mars 2004 fait apparaître que le pair à pair aurait un impact limité sur les ventes de disques. Une autre étude, européenne, de janvier 2004 conclut que sur les 9% de réduction des ventes de cédéroms constatés en 2002, seulement 2 % pourraient être dus aux échanges de fichiers, le reste étant lié à l'écoute de radios sur Internet. Pour sa part, l'IFPI (International Federation of the Phonographic Industry), qui représente les industries musicales, indique que les ventes mondiales de musique ont diminué de 7% en 2003, baisse qui selon elle trouve son origine dans les effets combinés du piratage sur Internet, des contrefaçons physiques de cédéroms et de la concurrence des autres produits de divertissement. De son côté, la SACEM indique dans ses rapports annuels d'activité que le montant des droits encaissés dans les dernières années est en augmentation régulière de 5 à 6% par an (en 2002 de 672,4 millions d'euros, et, pour l'année 2005, 757,4 millions d'euros). Il n'en reste pas moins que la bonne santé globale du secteur ne peut masquer une baisse considérable des revenus phonographiques, les perceptions de la SDRM ayant baissé en 2004 de 24,5 % en ce domaine, baisse compensée en partie seulement par l'augmentation des perceptions vidéographiques dues à l'augmentation de ventes de DVD.

Les échanges illicites de fichiers musicaux peuvent sans doute expliquer pour partie la baisse des ventes d'œuvres mais n'en sont certainement pas le facteur unique. D'autres éléments doivent être mis en cause. Ils sont évoqués par M. le Député Ch. Vanneste dans un rapport effectué au nom de la Commission des lois de l'Assemblée nationale dans le cadre de l'examen du projet de loi DADVSI. Ainsi, notamment, sont souvent cités la politique éditoriale des éditeurs « parfois accusés de privilégier la rentabilité à court terme plutôt que l'installation d'artistes dans la durée », « un appui excessif sur les réseaux de la grande distribution » (la taille limitée des rayons favorise les produits les plus vendus), « la concurrence accrue d'autres produits de loisirs » (déjà citée par l'IFPI : DVD, jeux vidéo, Internet, téléphonie mobile, etc. dont le coût s'impute sur le budget, souvent limité, de consommateurs, souvent jeunes), « une certaine obsolescence du support que constitue le CD », « la gestion des prix unitaires »... « Pour autant, conclut le rapporteur, il est certain que les téléchargements ont connu une simultanéité manifeste avec la diminution des ventes ».

Par ailleurs, le développement des plate formes de téléchargement, concurrence légale des lieux de téléchargements illicites (aucune en France jusqu'en 2004, 20 en 2005) semble devoir apporter un effet positif puisqu'une étude faite pour l'IFPI montre que le nombre de personnes achetant légalement de la musique en ligne s'accroît rapidement et tend à rejoindre celui des internautes utilisant le pair à pair. A ce sujet, il semble que les très jeunes gens seraient les plus réticents à s'orienter vers le téléchargement légal du fait des contraintes liées au paiement en ligne et de la nécessité de disposer d'une carte bancaire.

Il n'en reste pas moins que, quelle que soit l'ampleur de la contrefaçon musicale commise à l'aide de réseaux de pair à pair, elle est inadmissible et doit être combattue.

**Quant à l'audiovisuel**, le téléchargement illicite, d'apparition plus récente et lié à la généralisation du haut débit, menace à l'évidence la production et la distribution, la fréquentation des salles et les recettes des ventes et des locations de vidéos. Le Centre national de la cinématographie, dans une étude, estimait en 2005 à un million par jour le nombre de téléchargements illicites, nombre environ deux fois plus élevé que celui des spectateurs dans les salles (185 millions d'entrées en 2006, en progression de 6%

par rapport à 2005). Quoiqu'il en soit de son volume réel, la contrefaçon d'œuvres audiovisuelles par téléchargement illicite sur des logiciels d'échange de pair à pair doit naturellement elle aussi être affrontée.

7. Le téléchargement illicite recouvre des **réalités criminologiques** différentes. En matière de cinéma, de jeux et de musique, on peut constater une délinquance organisée, par exemple lorsque des copies de films sont mises à disposition (uploading) avant la sortie en salle ou même avant l'établissement de la version définitive (première copie standard). L'on doit néanmoins distinguer les contrefacteurs occasionnels des habituels ou encore distinguer ceux qui téléchargent en vue d'une utilisation commerciale des autres. Toujours est-il que l'on assiste à une migration de ces comportements, de la criminalité artificielle (réprobation sociale faible ou inexistante) vers la criminalité naturelle (conscience généralisée de violation d'un interdit) dans la mesure où aujourd'hui, pratiquement tous les internautes ont connaissance du caractère illicite du téléchargement d'œuvres protégées sans autorisation. Comment pourrait-il en être autrement ? Non seulement les médias, mais encore et surtout la loi le leur rappelle. Ainsi, la loi du 21 juin 2004 pour la confiance dans l'économie numérique, en son article 7, oblige t-elle les fournisseurs d'accès qui invoquent à des fins publicitaires la possibilité qu'ils offrent de télécharger des fichiers dont ils ne sont pas les fournisseurs à faire « figurer dans cette publicité une mention facilement identifiable et lisible rappelant que le piratage nuit à la création artistique ». La loi du 1<sup>er</sup> août 2006, de manière analogue, impose aux fournisseurs d'accès d'adresser à leurs frais « aux utilisateurs de cet accès des messages de sensibilisation aux dangers du téléchargement et de la mise à disposition illicites pour la création artistique ». Toujours est-il que notre propos ne concerne que les « petits » téléchargements illicites, réalisés sans visée lucrative, en d'autres termes « une grande masse d'infractions qui, prises isolément, occasionnent un trouble limité ».

8. Prenant acte de cette réalité criminologique, le gouvernement a tenté d'introduire une répression dérogatoire et mesurée, dite « **réponse graduée** », pour défaire l'innombrable armée des petits contrevenants occasionnels en les sanctionnant d'une peine de police, et non plus délictuelle. Tel était le but de l'art. 24 du projet de la loi du 1<sup>er</sup> août 2006 créant l'art. L. 355-11 CPI : après avertissement à l'internaute indélicat, étaient incriminées spécialement la reproduction non autorisée à des fins

personnelles et la communication au public à des fins non commerciales grâce au pair à pair lorsque cette communication résultait automatiquement de la reproduction. Il s'agissait dans les deux cas de petites contraventions de police. Mais la loi DADVSI, promulguée le 1<sup>er</sup> août 2006, a été amputée de ce dispositif de « réponse graduée » le 27 juillet précédent par le Conseil constitutionnel comme contraire à l'égalité devant la loi pénale : il n'y a aucune raison, a dit le Conseil, de distinguer entre vecteurs analogique et numérique de la contrefaçon ni entre vecteur pair à pair ou autre vecteur. Certes, la position du Conseil constitutionnel pouvait être critiquée: l'égalité des citoyens devant la loi pénale, motif de la censure, suppose une criminalité de même nature ; or peut-on assimiler l'internaute ludique, qui agit pour son propre usage et celui de proches à celui qui reproduit en nombre pour vendre ? De plus, le principe de proportionnalité est constitutionnellement aussi important que celui d'égalité. On ne doit punir qu'avec des peines proportionnées à la gravité du comportement. Il ne faut pas oublier que le délit de contrefaçon, par extensions successives, a englobé des attitudes antisociales très différentes, certaines étant moins graves que d'autres.

En l'état du droit positif, le contrefacteur par téléchargement illicite, quelle que soit la gravité de son comportement, reste donc coupable d'un délit de contrefaçon, punissable au maximum de trois ans d'emprisonnement et de 300 000 euros d'amende. Les peines encourues sont aggravées à 5 ans et à 500 000 euros en cas d'infraction commise en bande organisée et l'on peut se demander si cette circonstance n'est pas systématiquement présente dès lors qu'il y a utilisation d'un réseau d'échanges de pair à pair.

**9. La sanction encourue paraît disproportionnée** à tous les observateurs et au gouvernement : le ministre de la Culture et de la Communication a adressé une lettre ouverte aux internautes le lendemain de la décision du Conseil constitutionnel, dans laquelle il annonce qu'il demandera aux garde des Sceaux de réserver les poursuites aux cas les plus graves. Les maxima prévus par les textes sont loin d'être appliqués par les juges (aucun emprisonnement ferme n'a jamais été prononcé et les amendes sont faibles, parfois assorties du sursis). La réponse sociale à cette petite délinquance de masse doit être repensée et adaptée dans le respect de la décision du Conseil constitutionnel, des principes du droit pénal et de ceux qui protègent la vie privée. En

première approche, on peut aussi imaginer une réponse autre que pénale ou encore des accords contractuels préventifs, à imaginer eux aussi, notamment entre producteurs des œuvres protégées et intermédiaires techniques tels que fournisseurs d'accès à Internet, ou encore des accords contractuels entre fournisseurs d'accès et internautes.

La contrefaçon d'œuvres musicales et celle d'œuvres audiovisuelles ne posent sans doute pas les mêmes problèmes. Le volume des investissements est sans commune mesure ; il en va de même corrélativement du préjudice subi par les victimes. Et si certaines solutions techniques, telle la réduction de la bande passante, montante ou descendante, sont de nature à entraver le téléchargement illicite des œuvres audiovisuelles, elles sont sans efficacité sérieuse sur celui des œuvres musicales.

Toujours est-il qu'il semble préférable d'aboutir à des solutions qui soient communes aux secteurs concernés et qui ne soient pas rendues obsolètes par l'évolution vertigineuse de la technique.

**10.** Il convient au préalable de donner un aperçu commenté du **droit positif**, en ce qu'il concerne les téléchargements illicites au moyen des réseaux de pair à pair.

Outre la protection pénale de l'intégrité des mesures techniques de protection (DRM, Digital Rights Management), le législateur du 1<sup>er</sup> août 2006 a organisé spécifiquement la répression de

En matière civile, l'art. L. 336-1 CPI dispose que le juge des référés peut ordonner toute mesure nécessaire à la protection des droits d'auteur et des droits voisins lorsque le logiciel est « principalement utilisé pour la mise à disposition illicite d'œuvres ou d'objets protégés ».

Les mesures en question sont probablement les mesures techniques de protection. Le texte impose-t-il leur utilisation aux éditeurs de logiciels d'échange de pair à pair, ce qui ne serait guère compatible avec l'existence même de logiciels libres ? L'absence de ces mesures fournit-elle la preuve que l'éditeur avait l'intention de proposer un logiciel permettant l'échange illicite d'œuvres protégées ?

Un autre problème se pose : comment dire qu'un logiciel est « manifestement » ou « principalement » destiné à l'échange illicite ? Des éléments de réponse sont donnés par la Cour suprême des Etats-Unis : « celui qui distribue un objet avec pour but de promouvoir son utilisation afin de contrefaire le copyright, tel que démontré par des manifestations claires... pour encourager la contrefaçon, est responsable des agissements consécutifs contrefaisants des tiers » et par la Cour fédérale d'Australie à propos du logiciel d'échange de pair à pair Kazaa : est tenu responsable l'éditeur qui a « autorisé » les contrefaçons en n'utilisant pas les mesures techniques de protection et en incitant directement les internautes à réaliser des contrefaçons. Le jugement énonce que les éditeurs pourront continuer leurs activités s'ils mettent en place un filtrage agréé par les demandeurs ou accepté par la cour. L'abstention suffirait-elle à caractériser l'élément moral de la complicité de contrefaçon, à supposer que l'on soit bien en présence d'une telle complicité ?

Mais ne s'agit-il que d'une loi déjà dépassée ? Les logiciels les plus utilisés sont désormais des logiciels libres (open source) créés non plus par un éditeur identifiable mais par une communauté anonyme d'internautes. Ces logiciels tels Kaméléon, Mute ou Share sont équipés d'un système de cryptage très élaboré, rendant en outre le filtrage et l'identification des utilisateurs pratiquement impossible. Certes, même si la communication est cryptée, on peut toujours savoir quelles sont les adresses IP de l'émetteur et du destinataire. Mais pour matérialiser l'infraction, en revanche, il faut pouvoir analyser le flux, et donc « casser » le cryptage, ce qui est ardu. Mieux vaut donc aller directement perquisitionner le disque dur de l'internaute et cela même avant

d'avoir atteint une présomption forte d'un comportement délictueux, ce qui est problématique au regard des libertés individuelles. Il existe aussi des systèmes d'anonymisation de connexion, comme TOR (The Onion Ring) qui brouille les pistes en faisant « rebondir » la connexion cryptée entre de multiples serveurs.

En tout état de cause, la répression de ces actes (édition de logiciels voués au piratage et publicité) par le droit commun au titre de la complicité de contrefaçon par provocation ou par fourniture de moyens semblait discutable : d'une part, la résolution d'un concours idéal d'infractions se fait par le choix de l'infraction spéciale et d'autre part, la complicité s'entend de l'aide apportée en contemplation de la commission d'une infraction déterminée. C'est sans doute cette fragilité du droit commun, outre la mise en conformité du droit français avec la directive du 22 mai 2001, qui a suscité ces dispositions spécifiques. Il n'en reste pas moins qu'à notre connaissance, sept mois après la promulgation de la loi DADVSI, aucune poursuite n'a été exercée sur le fondement de ce texte.

Quant à l'internaute, téléchargeur occasionnel, son sort n'a pas changé à la suite de la censure par le Conseil constitutionnel de la partie du projet de loi qui prévoyait pour lui une répression adoucie.

La répression de la **mise à disposition** (téléchargement ascendant, uploading) sans le consentement des titulaires de droits obéit au droit commun : c'est une contrefaçon par représentation, puisque les internautes qui ont accès au disque dur de celui qui met à disposition ne forment pas un cercle de famille. Cette mise à disposition est particulièrement dommageable lorsqu'elle se situe en amont de la chaîne de diffusion, voire avant la divulgation, permettant ainsi en aval un grand nombre de téléchargements descendants illicites avant que l'œuvre n'ait pu être normalement exploitée. En revanche, le comportement de l'internaute utilisateur final, qui télécharge occasionnellement une œuvre protégée tout en mettant à disposition les œuvres figurant sur son disque dur (mise en partage automatique des fichiers téléchargés, optionnelle ou obligatoire selon le logiciel d'échange de pair à pair utilisé) réalise le comportement le moins grave au sein de cette première famille de contrefaçons.

Il en va de même de la répression du **téléchargement descendant** (downloading) sans le consentement des titulaires de droits et sans mise en partage : selon l'opinion

dominante, c'est une contrefaçon par reproduction. Le comportement de l'internaute indélicat, s'il profite d'un système interdit d'échanges, ne s'en trouve néanmoins pas à l'origine et là encore ce comportement peut être considéré comme le moins grave au sein de cette deuxième famille de contrefaçons. Dans ce cas de téléchargement descendant illicite comme dans le précédent, le recours à l'incrimination de droit commun de recel de contrefaçon (tirer profit de la contrefaçon réalisée par autrui) a pu être envisagée mais cette dernière n'a pas encore été appliquée par le juge.

**11. L'exception de copie privée**, fait justificatif de la contrefaçon, peut-elle profiter à celui qui télécharge sur une plate forme pair à pair ?

Les textes compétents sont les alinéas 2 et 4 de l'art. L. 122-5 CPI, cet article traitant des exceptions aux droits d'auteur. L'alinéa 2 donne la liste des exceptions au droit exclusif. L'alinéa 4 soumet les exceptions au test en trois étapes. La mise en œuvre des exceptions suppose que l'œuvre ait été divulguée.

En substance, l'art. L 122-5 al. 2, 2° CPI excepte du droit d'auteur les copies strictement réservées à l'usage personnel du copiste et non destinées à une utilisation collective. Celui qui opère un téléchargement descendant pour son seul usage semble donc, en première approche, justifié. Reste cependant à savoir si, pour profiter de l'exception de copie privée, la **source** (l'œuvre représentée par autrui en téléchargement ascendant) à partir de laquelle il copie doit être **licite**.

Le ministre de la justice pense que oui. Donc, dans la mesure où les œuvres ont été proposées illégalement sur Internet, l'exception de copie privée ne pourrait pas être invoquée avec succès. S'agissant d'une circulaire, elle s'impose au parquet lorsqu'il exerce l'action publique mais ne lie pas le juge.

La Cour de cassation n'a pas encore pris parti. Un internaute était poursuivi pour contrefaçon pour avoir effectué des copies de films sur des cédéroms (CD-Roms). La cassation pour manque de base légale de l'arrêt de relaxe déféré est motivée par le fait que la cour d'appel n'avait pas déterminé comment l'internaute avait eu accès aux œuvres et n'avait pas répondu aux conclusions des parties civiles faisant valoir que l'exception de copie privée ne pouvait s'appliquer que si la source était licite. Une cassation n'aurait pas été prononcée sur ce moyen si la recherche refusée par la cour d'appel avait été inutile. Doit-on en déduire une condition de licéité de la source ? Il faut attendre la décision de la cour de renvoi.

La doctrine est partagée. Certains auteurs estiment que l'internaute qui télécharge n'a



pas le devoir de vérifier la licéité de la première divulgation de l'œuvre copiée. Ils invoquent à l'appui de leur thèse le silence de la directive du 22 mai 2001 et de la loi du 1<sup>er</sup> août 2006 (alors qu'il eût été facile et opportun pour le législateur de s'exprimer sur ce point important) ainsi que la compensation venant de la rémunération pour copie privée. Pour sa part, le Conseil économique et social a proposé de qualifier de copies privées les téléchargements d'œuvres protégées. Au contraire, pour d'autres auteurs, il serait peu compréhensible qu'une copie privée soit licite si elle a pour origine directe une copie illicite, l'illégalité de la source corrompant toutes les utilisations ultérieures. Un acte illégal ne peut être la source d'un acte légal et la copie privée ne peut « blanchir » la contrefaçon. A cela ils ajoutent le principe général d'interprétation stricte des exceptions.

Autre obstacle à la qualification de copie privée ou de représentation dans un cercle de famille, l'art. L. 122-5 al. 4 CPI (loi du 1<sup>er</sup> août 2006) dispose que « les exceptions énumérées par le présent article ne peuvent porter atteinte à l'exploitation normale de l'œuvre ni causer un préjudice injustifié aux intérêts légitimes de l'auteur ». Il s'agit là du **test en trois étapes** prévu la directive du 22 mai 2001, elle-même issue d'autres engagements internationaux de la France. Ce test a été mis en œuvre par le juge avant même la promulgation de la loi du 1<sup>er</sup> août 2006 : la Cour de cassation, en février 2006, a validé l'insertion de mesures techniques de protection dans le support numérique par application du test, même si ces mesures entravent le jeu de l'exception de copie privée. Cette jurisprudence sera-t-elle confirmée par d'autres arrêts ? En toute hypothèse, le nouvel alinéa 4 de l'art. L. 122-5 exige d'interpréter toutes les exceptions au droit d'auteur à la lumière du test en trois étapes. Or, on a soutenu qu'en premier lieu, si la copie privée devait exister indépendamment du caractère licite ou non de sa source, elle serait généralisée et ne constituerait donc plus une « exception ». En deuxième lieu, a-t-on écrit, l'« exploitation normale » de l'œuvre en serait nécessairement perturbée. En troisième lieu, on peut penser que les titulaires des droits subiraient un « préjudice injustifié » puisqu'ils devraient subir non seulement les contrefaçons mais aussi les copies contrefaisantes réalisées à la suite (les exemplaires de l'œuvre n'étant achetés ni par le contrefacteur d'origine ni par le copiste et les agissement entravant l'essor de la vidéo sur demande et du téléchargement légal). On peut observer que ce test en trois étapes rend singulièrement aléatoire le jeu de l'exception de copie privée dans la mesure où il

implique une appréciation économique par l'internaute (avant de copier) et par le juge (saisi d'une poursuite en contrefaçon) et que de ces appréciations, éventuellement divinatoires, dépend la qualification de contrefaçon. Tout au plus, tant l'internaute que le juge doivent-ils pouvoir se faire une idée de l'impact économique de la copie en fonction du moment où elle a été réalisée dans l'exploitation commerciale de l'oeuvre. Mais l'insécurité juridique qui en découle est-elle compatible avec le principe de la légalité des incriminations ?

**12.** S'agissant de constater des faits qui prennent place sur des réseaux, on délaissera provisoirement la constatation directe des faits par l'intelligence humaine pour se tourner vers la recherche automatisée. La loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements et données à caractère personnel a ajouté, à la demande des ayants droit, un article 9-4° à la **loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**. Le texte permet aux sociétés de perception et de répartition des droits d'auteurs et des droits voisins ainsi qu'aux organismes de défense professionnelle de demander à la CNIL (Commission nationale de l'informatique et des libertés, une autorité administrative indépendante) l'autorisation de procéder à des traitements informatisés ou manuels de données personnelles relatives aux infractions et aux sanctions en vue d'assurer la défense des droits de leurs adhérents. L'intervention du législateur était nécessaire, les données concernées telles les adresses IP (Internet Protocol) étant indirectement nominatives. Lors des débats parlementaires, les rapporteurs du texte à l'Assemblée nationale et au Sénat avaient tous deux précisé la pensée de la loi : il s'agissait de « recenser les délits d'habitude », le « piratage organisé » et non la masse des petits contrevenants occasionnels, objets de notre étude.

**13.** Pour sa part, le 7 mars 2005, le **Groupe de travail « Article 29 »** (dit encore G29) sur la protection des données de la vie privée a suggéré les limites de cette recherche d'infractions confiée à des organismes privés représentant des intérêts particuliers : il désapprouve « la recherche systématique à grande échelle comme le balayage d'Internet ou la demande de communication de données personnelles détenues par d'autres acteurs tels que les fournisseurs d'accès ou les contrôleurs des annuaires Whois ; de telles enquêtes sont de la compétence de l'autorité judiciaire ». Ce Groupe de travail, établi par l'article 29 de la directive 95/46 CE du 24 octobre

1995, est un organe européen consultatif indépendant regroupant les représentants des organes de protection de la vie privée des pays de l'Union européenne (pour la France, la CNIL).

**14. La CNIL s'est prononcée** à ce jour (février 2007) à trois reprises sur des demandes d'autorisation de création de fichiers de données personnelles présentées par des sociétés d'ayants droit. La première concernait les jeux vidéo (environ 25% des téléchargements, autorisation du 11 avril 2005), la deuxième la musique (environ 39%, refus d'autorisation du 24 octobre 2005) et la troisième l'audiovisuel (environ 34%, autorisation du 21 décembre 2006). Dans le cas des jeux vidéo et de la musique, les demandes d'autorisation prévoyaient l'envoi de messages de prévention et d'avertissement puis des poursuites judiciaires réservées aux comportements le plus graves. S'agissant de l'audiovisuel, il n'est pas prévu l'envoi de messages d'avertissement. L'examen de délibérations de la CNIL permet de dire ce qui est possible et ce qui ne l'est pas.

**15. En matière de jeux vidéo**, le 11 avril 2005, la CNIL (séance du 24 mars) a autorisé le Syndicat des éditeurs des logiciels de loisirs (SELL) à mettre en œuvre deux traitements automatisés de détection des contrefaçons de logiciels de jeux vidéo sur Internet, spécialement en matière de pair à pair. La demande tendait à deux objets. D'une part, il s'agissait d'adresser des messages de prévention aux internautes téléchargeant et mettant à disposition des logiciels copiés illégalement sur les réseaux pair à pair. En général, ces logiciels comprennent une fonction de messagerie et le SELL devait utiliser cette fonction lorsque l'internaute recherchait, mettait à disposition ou opérait un téléchargement descendant pour envoyer le message de prévention. En d'autres termes, le fournisseur d'accès n'avait pas à faire de conversion entre l'adresse de courrier électronique et l'adresse IP de l'internaute. D'autre part, il s'agissait de relever, dans des cas limités, l'adresse IP d'internautes mettant à disposition des logiciels de loisirs copiés illégalement sur ces réseaux. La Commission a examiné si la demande assurait un équilibre entre le respect de la vie privée et les droits des auteurs.

A - L'envoi de messages de prévention

La demande portait que les messages adressés aux internautes téléchargeant et

mettant à disposition des logiciels de loisirs devaient indiquer que ces logiciels sont des œuvres de l'esprit protégées par le droit d'auteur et que la violation du droit d'auteur d'un logiciel, telle la mise à disposition sur Internet sans autorisation, constitue un acte de contrefaçon. Le message ne devait entraîner aucune poursuite ni sanction, mais simplement sensibiliser les internautes au caractère illégal de leur comportement et aux sanctions qu'ils pourraient encourir.

Ces messages ne devaient être envoyés qu'aux internautes téléchargeant ou mettant à disposition des logiciels de loisirs appartenant aux éditeurs membres du SELL.

Le logiciel mis en œuvre par le SELL, selon la demande, devait identifier automatiquement les machines offrant illicitement des logiciels de jeu et, se faisant passer pour un amateur, devait collecter leurs adresses IP. Ces adresses, collectées mais non conservées, devaient être les cibles immédiates du message de prévention.

La Commission s'est assurée que l'envoi de ces messages ne donnera lieu à aucune conservation d'informations de la part du SELL. Ainsi, l'adresse IP des internautes à qui le message est adressé ne pourra pas être conservée ni utilisée pour dresser un procès-verbal d'infraction. L'on doit remarquer ici que l'adresse IP ne sert pas à identifier un internaute, mais un ordinateur sur le réseau. Un même ordinateur peut héberger des milliers d'utilisateurs différents. Si ce dispositif a été utilisé dans le cas présent, c'est que d'autres données ont été collectées, comme l'adresse courriel du joueur.

B - La collecte de l'adresse IP de certains internautes en vue de dresser un procès-verbal d'infraction.

La Commission s'est attachée à contrôler l'adéquation des traitements présentés par le SELL aux stricts besoins de la lutte contre la contrefaçon sur internet.

Les adresses IP des internautes mettant à disposition des logiciels de loisirs propriétés de membres du SELL devaient être collectées et cette fois-ci conservées, mais seulement dans des cas limités, caractérisés par la gravité de l'infraction (critères qualitatifs de la première mise à disposition ou de la mise à disposition d'une œuvre non encore commercialisée) et soumis à la CNIL. Les poursuites seraient donc limitées aux internautes responsables de la première mise à disposition sur le réseau, à supposer qu'on puisse les déterminer dans un système de pair à pair (rapport E de Givry sur la délibération SACEM et autres). Les procès-verbaux permettant au SELL de lancer des poursuites ne pouvaient être dressés que par un agent assermenté, agréé

par le ministère de la culture et désigné par le SELL.

La CNIL s'est assurée que les adresses IP des internautes ne seraient recueillies que dans le seul but de permettre la mise d'informations à disposition de l'autorité judiciaire et ne pourront acquérir un caractère nominatif que dans le cadre d'une procédure judiciaire. La durée de conservation des données à caractère personnel était proportionnée à la finalité poursuivie et les mesures prises afin d'en assurer la sécurité satisfaisantes.

En conclusion, la CNIL a considéré que les garanties accompagnant la mise en œuvre des traitements présentés par le SELL étaient de nature à préserver l'équilibre entre la protection des droits reconnus aux personnes dont les données sont traitées et la protection des droits dont bénéficient les auteurs et leurs ayants droits. Elle a donc autorisé le traitement. A notre connaissance, le SELL ne l'utilise plus depuis quelques mois.

**16. En matière musicale**, le 24 octobre 2005, la CNIL (séance du 18 octobre) a refusé d'autoriser les traitements demandés par la Société des auteurs, compositeurs et éditeurs de musique (SACEM) ; la Société pour l'administration du droit de reproduction mécanique (SDRM) ; la Société civile des producteurs phonographiques (SCPP) et la Société civile des producteurs de phonogrammes en France (SPPF). Un recours contre ce refus est pendant devant le Conseil d'Etat.

La CNIL a donc rejeté les demandes identiques de ces quatre sociétés d'auteurs et de producteurs de musique de mettre en œuvre des dispositifs permettant la détection automatisée de mises à disposition illégales d'œuvres musicales sur les réseaux de pair à pair et l'envoi de messages de sensibilisation aux internautes. Pour quelles raisons ? « Si les finalités poursuivies par les traitements présentés par [les sociétés] sont similaires à celles figurant dans la demande d'autorisation du SELL, les fonctionnalités de ces dispositifs ainsi que l'échelle de leur mise en œuvre ne sont en revanche pas comparables ». Quant à la différence d'échelle, le dispositif envisagé par les sociétés devait permettre de surveiller la quasi-totalité des réseaux de pair à pair existants, alors que les traitements autorisés pour le SELL ne portaient que sur les quatre principaux réseaux. Alors que le SELL prévoyait d'envoyer environ 300 messages de prévention par jour, les sociétés envisageaient de 50 000 à 100 000 envois par jour. Quant aux différences de fonctionnalités, le raisonnement est le

suivant :

#### A - L'envoi de messages de prévention

Le dispositif prévoyait le repérage, par les sociétés d'ayants droit, d'internautes mettant à disposition illégalement des œuvres musicales puis l'élaboration d'un message personnalisé d'avertissement à l'attention de ceux mettant à disposition moins de 50 fichiers et la transmission de ce message et de l'adresse IP concernée au fournisseur d'accès dont cette adresse relève. Le fournisseur d'accès devait faire le lien entre l'adresse IP et un abonné à qui il devait envoyer le message par courrier électronique.

La Commission a considéré que les sociétés d'auteurs ne pouvaient avoir recours aux fournisseurs d'accès à Internet pour qu'ils identifient les internautes et relayent les messages de prévention. D'une part, l'envoi de messages pédagogiques pour le compte de tiers ne fait pas partie des cas de figure où les fournisseurs d'accès à Internet sont autorisés à conserver les données de connexions des internautes. D'autre part, dans sa décision du 29 juillet 2004, le Conseil constitutionnel a rappelé, sur la base de l'art. L. 34-1 du Code des postes et communications électroniques, que les données collectées à l'occasion des traitements portant sur des infractions aux droits d'auteur ne pourront acquérir un caractère nominatif que sous le contrôle de l'autorité judiciaire. « Le non respect de ce qui représente l'une des garanties essentielles de nature à préserver l'équilibre entre protection des droits d'auteur et protection des données à caractère personnel apparaît, en première analyse, constituer un obstacle à la mise en œuvre de tout dispositif d'envoi de messages nécessitant l'identification des internautes par les fournisseurs d'accès à Internet ».

#### B - La recherche et la constatation de mise à disposition illicite d'œuvres musicales

La Commission a estimé que les dispositifs présentés n'étaient pas proportionnés à la finalité poursuivie. En premier lieu ils n'avaient pas pour objet la réalisation d'actions ponctuelles strictement limitées au besoin de la lutte contre la contrefaçon. En deuxième lieu ils pouvaient aboutir à une collecte massive de données à caractère personnel. En troisième lieu, ils permettaient la surveillance exhaustive et continue des réseaux d'échanges de fichiers de pair à pair. En quatrième lieu enfin, la sélection des internautes susceptibles de faire l'objet de poursuites pénales ou civiles devait s'effectuer sur la base de seuils relatifs au nombre de fichiers mis à disposition (respectivement 1000 et 500 œuvres), seuils qui devaient être déterminés uniquement

par les sociétés d'auteurs et que celles-ci se réservaient la possibilité de réviser unilatéralement à tout moment. A ce critère de sélection quantitatif, on peut opposer le critère qualitatif retenu par le SELL et validé par la CNIL, celui de la première mise à disposition d'une œuvre, commercialisée ou non.

La CNIL a donc rejeté les demandes des sociétés.

**17. En matière audiovisuelle** : par une délibération du 21 décembre 2006, la CNIL a autorisé la mise en œuvre par l'Association de lutte contre la piraterie audiovisuelle (ALPA) de traitements de données à caractère personnel ayant pour finalité principale la recherche des auteurs de contrefaçons audiovisuelles.

A – La demande d'autorisations

a) Recherche et constatation des actes de contrefaçons sur Internet.

Le traitement demandé avait pour seul objet de permettre aux agents assermentés de dresser procès-verbal de constatation des faits aux fins de permettre l'engagement des poursuites.

Pour les réseaux de pair à pair, les agents devaient saisir manuellement l'œuvre dont ils faisaient la requête (contrairement aux demandes d'autorisation présentées par les sociétés musicales, qui tendaient à automatiser de bout en bout la chaîne des recherches et des constatations). Le logiciel de pair à pair affichait en réponse la liste des fichiers correspondants. Les données collectées devaient être notamment l'adresse IP des internautes, le nom du fournisseur d'accès, le pseudonyme, le réseau pair à pair concerné et la date et l'heure de mise à disposition.

b) Recherche sur Internet d'œuvres faisant l'objet d'un marquage.

Le marquage, explique la CNIL (watermarking, tatouage numérique, apposition d'un filigrane) consiste à intégrer à l'œuvre, lors de sa réalisation et avant sa mise en ligne, un identifiant associé à la personne à qui elle est licitement remise. Cela permet, lors de la surveillance des œuvres circulant sur les réseaux, de détecter et d'identifier à qui l'œuvre illicitement mise à disposition a été régulièrement remise. Ce n'est pas nécessairement cette personne qui est l'auteur de la contrefaçon : une enquête peut ensuite déterminer qui en est l'auteur réel. Le marquage est invisible et ne peut donc être décelé par l'utilisateur final ; il ne dégrade pas la qualité de l'image. Il est possible de retrouver cette marque quel que soit le format vidéo (analogique ou

numérique) ou de compression utilisé. L'efficacité de cette technique sera discutée plus loin. La mise en œuvre de ce dispositif, dit la CNIL, implique en amont la gestion de bases de données dans lesquelles figurent des données personnelles de la personne associée à l'identifiant unique de l'œuvre. Il ne peut s'agir que d'un professionnel du secteur audiovisuel. Pour surveiller le réseau d'échanges, l'ALPA doit faire une requête en téléchargement d'une œuvre marquée et déterminera si le fichier reçu en réponse est celui d'un exemplaire marqué. Il n'y aura ni collecte ni enregistrement des données de l'internaute mettant à disposition les œuvres ou en permettant l'accès.

Les agents assermentés de l'ALPA constatent alors la mise à disposition d'une œuvre marquée dans un fichier téléchargé et font la mise en relation entre l'identifiant figurant dans ce fichier et la base de données nominatives qu'ils sont seuls à détenir et à pouvoir consulter.

Ces traitements ont pour unique objet de permettre aux agents assermentés de dresser un procès-verbal de constat des faits, non la mise en cause directe d'une personne. C'est à la seule autorité judiciaire qu'il appartiendra de déterminer l'imputabilité de ces faits lors d'une procédure mettant en cause le professionnel destinataire du support marqué ou celui qui est à l'origine de la contrefaçon.

L'ALPA informe les personnes concernées, au plus tard lors de la remise de l'œuvre marquée, qu'un lien est effectué entre leur identité et l'identifiant enregistré sur l'œuvre qui leur est remise et que des contrôles seront réalisés sur Internet dans la perspective d'actions en justice.

c) Traitements relatifs à la gestion des procès-verbaux et rapports.

Ces documents portent sur la contrefaçon commise tant sur Internet que dans le monde physique (par exemple vidéoclubs et marchés). Ils sont d'abord établis au format numérique puis édités sur format papier, classés et archivés le temps de la procédure judiciaire. La version numérique est supprimée dès la réalisation de l'édition au format papier.

B – La décision de la CNIL

La Commission prend acte de ce que le traitement proposé est de nature à préserver l'équilibre entre la protection des droits reconnus aux personnes dont les données sont traitées et celle des droits des auteurs et de leurs ayants droits. En effet, les



adresses IP objets de ces traitements ne sont recueillies que pour le besoin de la recherche, de la constatation et des poursuites et dans le seul but de permettre leur mise à la disposition de l'autorité judiciaire. Ce n'est que dans le cadre d'une procédure judiciaire que ces données acquièrent un caractère nominatif.

La Commission considère ensuite que les traitements demandés sont proportionnels à la finalité poursuivie puisqu'ils ne visent pas à un fichage systématique et exhaustif des personnes qui mettent à disposition ou échangent des fichiers grâce au pair à pair mais à des actions ponctuelles et ciblées strictement limitées aux besoins de la lutte contre la contrefaçon. Il n'y a pas utilisation d'un procédé permettant d'automatiser l'ensemble de la chaîne de recherche et de constatation des contrefaçons.

Enfin, la CNIL prend acte de ce que les traitements sont initiés sur le fondement de critères qualitatifs et ont pour objet principal de lutter contre ceux qui sont à l'origine même des préjudices subis par la filière audiovisuelle (ceux qui procèdent à la première divulgation non autorisée).

**18.** Il semble que la **doctrine de la CNIL** s'établisse alors ainsi : elle ne délivre son autorisation que lorsque certaines conditions sont réunies, qui préservent l'équilibre primordial entre le droit au respect de la vie privée des personnes dont les données sont traitées et les droits dont bénéficient les auteurs et leurs ayants droit.

Tout d'abord, les données personnelles ne peuvent être collectées que pour une finalité explicite et légitime, qui est la lutte contre la contrefaçon de grande ampleur (téléchargements en très grand nombre) ou de grande conséquence (téléchargements en amont de la chaîne de reproduction) sur les réseaux de pair à pair. C'est là le respect de l'intention du législateur telle qu'indiquée dans les travaux préparatoires de la loi du 6 août 2004. Ensuite, les traitements ne doivent porter atteinte ni à la vie privée des internautes (il s'agit en réalité d'un équilibre entre le respect de la vie privée des internautes et le droit de propriété des ayants droit), ni aux libertés (garanties par la loi du 6 janvier 1978, article 1<sup>er</sup>, et comprenant la liberté de communication). Puis les données personnelles et leur collecte doivent être proportionnées à cette finalité (loi de 1978, art. 6-2<sup>o</sup> et 3<sup>o</sup>). Seules des actions ponctuelles et ciblées sur un critère qualitatif sont permises et non la surveillance exhaustive et continue des réseaux de pair à pair sur un critère quantitatif (le balayage continu et automatique des réseaux serait peut-être légalement possible, à fins de statistiques, pour déterminer quelles sont les œuvres le plus souvent copiées, mais à

condition que les données soient rendues anonymes avant de rentrer dans les statistiques). C'est cette absence de proportion au regard des risques pour la vie privée et les libertés et le pouvoir de modifier unilatéralement les critères de seuil qui ont été relevés dans le refus opposé aux sociétés musicales. Ces données personnelles peuvent être collectées à l'insu des internautes grâce à l'exception apportée par l'article 32-VI de la loi de 1978 à l'obligation d'informer les personnes dont les données sont recueillies. Enfin, l'acquisition du caractère nominatif d'une adresse IP ne peut intervenir que dans le cadre d'une procédure judiciaire (décision du Conseil constitutionnel validant la loi de 1994), hormis naturellement les possibilités ouvertes par la loi du 10 juillet 1991 en matière d'interception des correspondances émises par la voie des télécommunications (interceptions judiciaires et administratives), par la loi du 9 mars 2004 en matière de criminalité organisée et la loi du 23 janvier 2006 relative à la lutte contre le terrorisme. C'est, entre autres, l'identification nominative par le fournisseur d'accès à Internet qui a été censurée dans le refus aux sociétés musicales.

A suivre la position de la CNIL, les possibilités de surveillance du réseau par recherche automatique impliquant le traitement de données personnelles semblent donc bien limitées. Elles sont même exclues pour ce qui concerne les « petits » téléchargements occasionnels. Certes, la surveillance « manuelle » reste possible. Pour être efficace cependant, elle doit viser à tarir à la source les contrefaçons le plus dommageables, celles qui concernent les premières mises à disposition illicites des œuvres protégées, ce qui nécessite une surveillance du réseau en continu (matériellement impossible) et une action dans les minutes qui suivent (également impossible).

### **19. Une épée de Damoclès juridictionnelle ?**

Le dispositif bâti par la CNIL au fil de ses trois décisions résisterait-il à une appréciation judiciaire ? Telle est la question posée un spécialiste. A supposer qu'un contrefacteur fût poursuivi, ne pourrait-il exciper de l'illégalité de la preuve des faits obtenue à l'aide d'un traitement pourtant autorisé ? En effet, l'article 9 de la loi de 1978 évoque « les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté » et non pas les traitements de données relatives aux suspicions d'infractions. Dans les deux autorisations accordées

en vue de poursuivre les contrefacteurs, il s'agissait d'infractions suspectées mais non judiciairement établies, donc n'ayant encore aucune existence, en vertu du principe de la présomption d'innocence, jusqu'à ce que le juge pénal ait prononcé une condamnation définitive. Comment un traitement pourrait-il être relatif à ce qui n'existe pas ? Pis encore : pour les autorisations accordées en vue d'envoyer de simples messages de prévention, l'interprétation faite par la CNIL de l'expression « traitements de données...relatives aux infractions... » pourrait-elle paraître d'autant plus extensive qu'aucune poursuite n'est même envisagée. On est donc encore plus loin des « infractions » exigées par la loi.

Or, la liberté de la preuve n'est pas sans limites. On ne peut prouver la matérialité des faits d'une infraction, de contrefaçon par exemple, par n'importe quel moyen. La Cour de cassation condamne traditionnellement l'emploi de procédés d'obtention illicites et écarte des débats les preuves ainsi obtenues, encore que sa position se soit assouplie récemment dans certains domaines. C'est ainsi que la Chambre criminelle admet aujourd'hui la régularité des provocations qui, sans inciter à perpétrer l'infraction, en permettent la constatation. L'hypothèse d'un agent assermenté se rendant sur le réseau pour y constater des téléchargements mais sans opérer lui-même de téléchargement ascendant semble donc irréprochable. Autre assouplissement de la doctrine de la Chambre criminelle : cette dernière accepte de ne pas écarter des débats les preuves déloyales offertes par la partie civile mais non par les autorités judiciaires. Or n'est-ce pas la police judiciaire qui fait acquérir un caractère nominatif à l'adresse IP ? Quelle serait la position de Cour de cassation ? Il faut pour le moment se contenter de rappeler un arrêt rendu en 2006 par la Chambre criminelle, en matière d'envoi de pourriels (spams) : violation de l'art. 226-18 du Code pénal alors en vigueur en ce que, d'une part, constitue une collecte de données nominatives le fait d'identifier des adresses électroniques et de les utiliser, même sans les enregistrer dans un fichier, pour adresser à leurs titulaires des messages électroniques ; d'autre part, est déloyal le fait de recueillir, à leur insu, des adresses électroniques personnelles de personnes physiques sur l'espace public d'Internet, ce procédé faisant obstacle à leur droit d'opposition.

Par ailleurs, il ne faut pas oublier le recours en annulation pour excès de pouvoir dirigé par les sociétés musicales contre la décision de refus d'autorisation qui leur a

été opposée par la CNIL. Si le Conseil d'Etat annulait ce refus d'autorisation, en résulterait-il que les traitements demandés mais refusés sont autorisés ? Probablement pas, une annulation éventuelle remettant la situation au statu quo ante. Mais la motivation de l'arrêt du Conseil d'Etat sera indubitablement source d'enseignements.

**20. À l'heure actuelle, le constat d'un téléchargement illicite** par de petits contrevenants occasionnels ne peut donc pas s'effectuer sur les réseaux au moyen de traitement de données de caractère personnel, sous réserve que la CNIL assouplisse sa position.

La collecte de la preuve pourrait alors être mise en oeuvre de la manière suivante, déclarée régulière par le Tribunal de grande instance de Paris le 8 décembre 2005.

Un agent assermenté d'une société civile de producteurs se connecte à Internet et télécharge un logiciel d'échange de pair à pair. Il constate, en l'occurrence, que un milliard et 290 millions de fichiers musicaux sont mis à disposition et que deux millions d'internautes utilisent ce système. Parmi ces derniers, un internaute sous pseudonyme a téléchargé 1663 fichiers dont 1212 correspondent à des enregistrements d'artistes dont les producteurs sont membres de la société civile qui l'a désigné.

L'agent assermenté, après avoir repéré le pseudonyme en question, utilise un logiciel pour connaître son adresse IP et saisit un officier de police judiciaire, lequel identifie nominativement l'internaute en interrogeant son fournisseur d'accès. Une analyse du disque dur de l'internaute est effectuée et laisse apparaître 1875 fichiers musicaux téléchargés.

Mais ce système est-il encore pertinent lorsque, dans une entreprise ou une administration, la même adresse IP couvre des centaines, voire des milliers de machines et d'utilisateurs potentiels ?

A l'inverse, une décision du Tribunal de grande instance de Bobigny décide que les preuves obtenues par traitements automatisés et transmises par les sociétés de protection des droits d'auteurs tel que la SACEM sont irrecevables lorsque la CNIL n'a pas donné son autorisation. En effet, le Tribunal considère que ces éléments de preuve (les adresses IP) sont des données personnelles et que, de ce fait, une autorisation de la CNIL est obligatoire pour leur consultation, leur extraction ou leur

conservation.

Il faut donc attendre que la jurisprudence judiciaire soit fixée sur la procédure de constitution de la preuve.

**21. Le but à atteindre**, tel qu'assigné par M. le ministre de la Culture et de la Communication dans sa lettre de mission, reste de prévenir la grande masse des petits téléchargements occasionnels, faits sans but lucratif autre que le non paiement du bien et, le cas échéant, de les sanctionner par un traitement généralisé, mesuré et automatique, tout en respectant leur vie privée, en ne contrôlant pas la circulation des fichiers libres de droits et en se souvenant que les logiciels d'échange de pair à pair ne sont pas illicites en eux-mêmes

**22. La responsabilité pénale, de type contraventionnel, ou civile, de l'abonné pour contrefaçon au regard des petits téléchargements illicites via le pair à pair ne peut plus être retenue.**

En premier lieu, en matière pénale, le Conseil constitutionnel a refusé l'idée d'une dualité de contrefaçons, l'une, grave, constituant classiquement un délit et l'autre, commise par le pair à pair, vénielle, constituant une contravention (supra, n° 9).

En second lieu, et la question est commune à toutes les contrefaçons par téléchargement, quelles qu'en soient l'ampleur ou la gravité, l'imputabilité des actes à un internaute particulier, condition essentielle de sa responsabilité pénale ou civile, est impossible à établir sans la visite de son disque dur. L'idée d'une réponse graduée automatique, aussi séduisante qu'elle ait pu apparaître, doit donc être abandonnée.

S'agissant de l'imputabilité, l'abonné ne peut empêcher que son adresse IP ne soit utilisée par autrui. Certes il y a bien vraisemblance de l'imputabilité des faits à l'abonné, certes ce dernier pourrait faire valoir ses moyens de défense devant le juge, mais sa possibilité d'apporter une justification utile en prouvant qu'il n'a pas commis l'infraction semble techniquement impossible. Un tiers, un voisin, dans un rayon d'une trentaine de mètres, peut utiliser l'adresse IP de l'abonné à son insu grâce à la connexion Wifi (soi-disant Wireless Fidelity) de ce dernier. Il suffit pour cela que le boîtier de raccordement soit demeuré ouvert, ce qui est pratiquement toujours le cas

chez tous les internautes, même les plus diligents. Aucune trace ne pourrait être conservée de cette usurpation temporaire, que l'abonné honnête serait donc incapable de prouver. Certes, il existe bien des clés de protection Wep (Wired Equivalent Privacy) ou, plus efficaces, Wpa (Wifi Protocol Access) mais, à supposer que l'abonné ait songé à les activer, les clés Wep seraient « cassables » en quelques minutes par un bon technicien. Pour les clés Wpa, les avis scientifiques recueillis divergent, ce qui n'est guère rassurant : pour certains, elles n'ont pas encore été subverties mais pour d'autres, quelques dizaines de minutes suffiraient à les neutraliser par un technicien hautement compétent. Ensuite, rien n'empêche l'intrus de publier sur les réseaux les solutions de cassage auxquelles il est parvenu, permettant dans l'heure à des centaines d'internautes d'utiliser eux aussi cette même adresse IP. De plus, le voisin indélicat peut agir de manière occulte grâce, par exemple, au réseau suédois Relakks, qui permet de circuler anonymement sur Internet, y compris pour fréquenter les réseaux de pair à pair. L'argentin Fon propose un service analogue. Le spoofing est également possible, c'est la possibilité d'usurper l'adresse IP d'une machine. En réalité, on peut donner n'importe quelle adresse IP à une machine donnée. Ainsi, un salarié indélicat pourrait-il, s'il sait que la machine d'un autre est éteinte, reconfigurer la sienne de manière à lui donner la même adresse MAC (adresse de carte réseau) que celle de son collègue et donc obtenir du routeur de réseau l'attribution temporaire de l'adresse IP de son collègue au vu de cette adresse MAC frauduleuse.

Problème d'autant plus délicat que de grandes entreprises ou de grandes administrations n'ont qu'une seule adresse IP extérieure, pouvant desservir des dizaines voire des centaines de postes et d'utilisateurs différents, solution paradoxalement conçue à l'origine pour des raisons de sécurité. En outre, en matière de téléphonie mobile, on sait que tous les abonnés d'un même réseau (Bouygues, Orange, SFR) accédant à l'Internet partagent la même adresse IP, soit en tout trois adresses.

Ces facilités techniques constituent le talon d'Achille de la responsabilisation de l'abonné pour le téléchargement, quel que soit le degré de la réponse à apporter aux téléchargements illicites. Dans l'hypothèse d'un accord contractuel entre fournisseur d'accès à Internet (FAI) et abonné, à supposer qu'une clause menace l'internaute qui télécharge illicitement d'une réduction de bande ou de suspension de l'abonnement :

non seulement la réduction ou la suspension seraient injustifiées (impossibilité pour le FAI de prouver la faute et le lien de causalité avec la contrefaçon, impossibilité pour l'internaute de résister à une présomption de téléchargement illicite) mais en outre, l'abonné serait fondé à engager la responsabilité contractuelle du FAI pour défaut de fourniture du service. Même chose dans l'hypothèse de l'envoi de messages de prévention : ils arriveraient à la mauvaise adresse et l'abonné honnête pourrait alors se plaindre d'avoir été injustement suspecté. Dans l'hypothèse de poursuites engagées par les ayants droit, tant pénales que civiles, on peut conjecturer sans risque que le juge refuserait de condamner pour contrefaçon un abonné pour défaut de surveillance de sa machine ou de son boîtier de raccordement Wifi sur la seule constatation que sa machine, identifiée par son IP, a servi aux téléchargements illicites. Il faut donc renoncer à l'idée d'une responsabilité pénale ou civile de l'internaute pour contrefaçon par téléchargement illicite.

Cette responsabilité aurait été fondée, faute de preuve de l'imputabilité, sur une présomption d'imputabilité. L'on a pu penser s'inspirer de solutions retenues notamment par le Code de la route : l'imputabilité ne pouvant être établie, peut-on du moins se contenter d'une présomption simple d'imputabilité, à l'image par exemple de celle qui existe pour la circulation routière ? C'est là une fausse bonne idée.

Les articles L. 121-2 et L. 121-3 du Code de la route disposent en effet que le titulaire du certificat d'immatriculation est redevable pécuniairement de l'amende encourue pour certaines contraventions (stationnement, péage, vitesse maximale, distances de sécurité entre véhicules, usage de voies et chaussées réservées, signalisations imposant l'arrêt), « à moins qu'il n'établisse l'existence d'un vol ou de tout autre événement de force majeure ou qu'il n'apporte tous éléments permettant d'établir qu'il n'est pas l'auteur véritable de l'infraction ». Le titulaire du certificat d'immatriculation, n'est pas pénalement responsable, il est seulement « redevable pécuniairement » de l'amende.

Le Conseil constitutionnel a validé ces dispositions le 16 juin 1999, raisonnant sur une présomption de culpabilité et considérant « qu'en principe le législateur ne saurait instituer de présomption de culpabilité en matière répressive ; que, toutefois, à titre exceptionnel, de telles présomptions peuvent être établies, notamment en matière contraventionnelle, dès lors qu'elles ne revêtent pas de caractère irréfragable, qu'est

assuré le respect des droits de la défense et que les faits induisent raisonnablement la vraisemblance de l'imputabilité » ; « qu'en outre, le titulaire du certificat d'immatriculation ne peut être déclaré redevable pécuniairement de l'amende que par une décision juridictionnelle prenant en considération les faits de l'espèce et les facultés contributives de la personne intéressée ; que, sous réserve que le titulaire du certificat d'immatriculation puisse utilement faire valoir ses moyens de défense à tout stade de la procédure, est dès lors assuré le respect des droits de la défense » ; enfin « le refus du titulaire du certificat d'immatriculation d'admettre sa responsabilité personnelle dans la commission des faits, s'il en est l'auteur, ou, dans le cas contraire, son refus ou son incapacité d'apporter tous éléments justificatifs utiles seraient constitutifs d'une faute personnelle ; que celle-ci s'analyserait, en particulier, en un refus de contribuer à la manifestation de la vérité ou en un défaut de vigilance dans la garde du véhicule ; qu'est ainsi respecté le principe, résultant des articles 8 et 9 de la Déclaration des droits de l'homme et du citoyen, selon lequel nul n'est punissable que de son propre fait ».

Pourquoi ne pas s'inspirer de ces textes en matière de contrefaçon par téléchargement ?

Parce que les choses s'y présentent d'une manière fondamentalement différente : alors que le propriétaire du véhicule peut empêcher que l'infraction ne soit commise ou, si elle a été commise, s'en disculper, l'abonné ne peut non seulement pas empêcher que son adresse IP soit utilisée par autrui mais encore il ne peut techniquement pas prouver qu'il a été victime d'une usurpation. Dans un cas, l'identification du coupable est aisée, dans l'autre elle est pratiquement impossible.

**23.** L'idée d'une **responsabilisation du fournisseur d'accès** pour **défaut de fourniture de logiciel de filtrage** ainsi que celle d'une **responsabilisation de l'abonné**, de type contraventionnel, pour **défaut de surveillance** de sa machine, ont été également examinées. En effet, l'article 6 de la loi du 21 juin 2004 édicte : « I.-1. Les personnes dont l'activité est d'offrir un accès à des services de communication au



CPI dispose que « Le titulaire d'un accès à des services de communication au public en ligne doit veiller à ce que cet accès ne soit pas utilisé à des fins de reproduction ou de représentation d'œuvres de l'esprit sans l'autorisation des titulaires des droits... en mettant en œuvre les moyens de sécurisation qui lui sont proposés par le fournisseur de cet accès en application du premier alinéa du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ». Cette obligation de l'abonné n'est pas non plus pénalement sanctionnée. Des incriminations contraventionnelles à créer pourraient-elles compléter ces textes et constituer des infractions obstacles, distinctes de la contrefaçon mais placées sur son chemin ?

**24.** Une première proposition tend à la création d'une **contravention**, visant le **fournisseur d'accès**, consistant pour ce dernier, à ne pas proposer de filtrage des oeuvres à l'abonné. A l'heure actuelle, tous les fournisseurs d'accès disent en proposer. Reste à savoir quel type de logiciel de filtrage est proposé, qui doit être de qualité suffisante pour ne pas risquer de voir les fournisseurs d'accès s'exposer au reproche de remplir leurs obligations à bon compte. Un projet de décret du ministre de l'Intérieur était à l'étude il y a encore quelques jours (mars 2007), fixant sur ce point des critères minimaux de qualité. Il a été abandonné. L'idée devrait être reprise. La majorité des fournisseurs d'accès, groupés au sein de l'AFA, est favorable à une solution unique et obligatoire, le cas échéant règlementaire, pour tous les fournisseurs. Ils craignent la distorsion de concurrence au bénéfice de celui qui ne proposerait pas de filtrage, attirant ainsi vers lui la masse des internautes qui téléchargent illicitement. Il semble cependant que ce fournisseur non volontaire se verrait pénalisé à brève échéance par cette même loi du marché. En effet, s'il concentre effectivement les téléchargements, il devra fournir à ses abonnés une quantité importante de bande passante, ce qui lui sera très onéreux, alors que les autres fournisseurs garderont une clientèle équilibrée entre internautes qui téléchargent (légalement) et ceux qui ne le font jamais. Au final, il n'est pas du tout certain qu'il ait intérêt à se différencier de ses homologues en s'abstenant de proposer un filtrage à ses abonnés. En attendant de voir si ce raisonnement commercial se vérifie durablement, il n'est nul besoin d'un texte rendant une position commune obligatoire, du moins dans l'immédiat.

**25.** Une seconde proposition tend à la création d'une **contravention**, visant l'**abonné**,

cette fois-ci, consistant pour ce dernier à ne pas installer ou mettre en œuvre un ou plusieurs logiciels de filtrage paramétrés et proposés par les fournisseurs d'accès. La responsabilité serait établie également si l'abonné ne sécurisait pas son installation Wifi. La responsabilisation de l'abonné au regard de l'obligation de filtrage ou de sécurisation éviterait dans certains cas d'engager des procédures, nécessairement lourdes, de contrefaçon, avec des enquêtes parfois attentatoires au respect dû à la vie privée des internautes pour identifier l'utilisateur responsable (il faut redire que l'abonné peut bien évidemment ne pas être le contrefacteur). Détachée de la contrefaçon, cette contravention ne ferait cependant pas obstacle à une éventuelle poursuite en contrefaçon s'il apparaissait que des téléchargements illicites étaient opérés. La contravention pourrait être établie par le constat d'un téléchargement illicite, ascendant ou descendant. L'abonné pourrait exciper d'un fait exonératoire tiré de la preuve qu'il a mis en œuvre le filtrage et la sécurisation. La contravention serait commodément et automatiquement sanctionnée par une amende forfaitaire.

Cette seconde proposition se heurte à certaines difficultés. La constatation de la non sécurisation poserait-elle les mêmes problèmes qu'en matière de contrefaçon ? Etablir que tel abonné n'a pas installé le logiciel de filtrage proposé sur la machine dont on connaît l'adresse IP ne nécessite-t-il pas de recourir à un traitement informatisé de donnée personnelles ? S'agissant de contrôles de masse, la CNIL accepterait-elle ici ce qu'elle a refusé aux sociétés musicales ? Le logiciel de filtrage pourrait-il être désactivé par le truchement du Wifi, ce qu'il serait intéressant de savoir puisque sa neutralisation sera naturellement le premier souci d'un intrus ? L'abonné pourrait-t-il garder la preuve de la neutralisation par un tiers (et non par lui-même) ? Par ailleurs, le fait d'instaurer une amende automatique pour défaut de surveillance se heurte au fait que, dans le cas de piratage par Wifi, l'accès illicite se fait depuis un équipement (la "box") qui dans la grande majorité des cas n'appartient pas à l'internaute, mais au fournisseur d'accès. L'internaute n'a donc pas les moyens de mettre en œuvre une politique de sécurité adaptée. Un fournisseur d'accès qui ne permettrait pas de mettre en œuvre un cryptage WPA sur sa box, mais seulement une protection Wep, serait-il, par défaut, coupable de négligence ? Faut-il en ce cas obliger les internautes qui pratiquent le téléchargement à s'équiper de box équipées de WPA (alors que ni les « vieilles » box, ni la version initiale de Windows XP, ni certains pilotes de cartes réseau, ni certains équipements WiFi usuels tels que la Nintendo DS ne supportent le

WPA) ?

Outre les probables réserves de la CNIL et la fragilité des protections du Wifi, on doit signaler que les ordinateurs connectés à Internet peuvent être infectés par un virus donnant à des tiers la possibilité de les piloter à distance à l'insu de leur utilisateur. Ce sont des PC zombies, ou botnet. Ces tiers utilisent une insuffisance de protection ou une faille dans la protection appropriée qui a été installée pour instiller un programme, lequel ordonnera à l'ordinateur d'exécuter telle tâche. Ce peut être la mise à disposition du public d'une partie de l'espace disque dur de l'abonné, à l'insu de ce dernier. L'ordinateur de l'abonné se transforme ainsi en serveur et son adresse IP sera mise à disposition du public. Les tiers pourront alors télécharger une œuvre mise illégalement à disposition sur l'ordinateur de l'abonné, sans que ce dernier en soit conscient. Ces faiblesses ne sont pas les seuls obstacles à la création d'une contravention de non sécurisation de son poste par l'abonné qui s'adonne au téléchargement.

**26.** Plus généralement, c'est la question de **la pertinence et de la fiabilité du filtrage des œuvres protégées** qui est posée, lorsque le filtrage est installé **sur le poste de l'abonné**. Ce filtrage n'est pertinent que s'il permet de discriminer automatiquement ce qui est permis de ce qui est interdit.

On peut concevoir un filtrage par œuvres, mais il est possible de supprimer les tatouages par filtrage et ré-encodage du signal afin d'éliminer les informations de très haute ou très basse fréquence contenant l'information du tatouage. Le système est donc contournable mais en toute hypothèse, il suffit d'utiliser les œuvres non tatouées sur les cédéroms existants. On peut encore concevoir le filtrage par port de communication car les logiciels d'échange utilisent des ports déterminés pour attendre les requêtes venant d'autres machines. Mais là encore le contournement est facile puisque l'abonné peut décider que le système d'échange, de pair à pair ou autre, utilisera un port classique (par exemple 109-110 pour la récupération des courriels). On peut imaginer aussi un filtrage par logiciel ou par site, ce qui serait sans objet puisque nombre de sites de pair à pair sont multi usages (YouTube permet l'enregistrement des programmes télévisés et les créations audiovisuelles personnelles). L'interdiction d'un site uniquement voué au pair à pair illicite entraînerait incontinent la masse des internautes vers ces sites multi usages. De plus bel, il est impossible de distinguer entre échanges licites et illicites lors de

l'utilisation de chacune des applications disponibles. Imposer à un utilisateur de mettre en œuvre un outil permettant d'empêcher l'émission ou la réception de contenus illégaux aurait techniquement pour conséquence de l'empêcher d'utiliser Internet. En effet, chacune des applications permet les échanges aussi bien illicites que licites. Ainsi le Web permet-il le téléchargement de logiciels gratuits, le commerce en ligne, etc. mais aussi la mise à disposition illicite d'une œuvre protégée. La messagerie électronique permet des échanges licites (correspondance ; on peut aussi s'envoyer à soi-même, sur une autre adresse de messagerie et donc dans une boîte de réception personnelle, la copie licite d'une œuvre protégée afin, par exemple, d'y accéder de son lieu de vacances) mais aussi la transmission illicite, publique ou privée, d'œuvres protégées. Il en va de même pour les newsgroups ou pour les échanges de pair à pair : les échanges illicites y sont aussi possibles que les échanges licites. Au niveau de l'ordinateur de l'abonné à Internet, chaque application ou logiciel n'a aucun moyen de détecter si l'information entrante ou sortante est illicite. Même si un logiciel pouvait vérifier qu'un fichier joint à un e-mail ou un fichier téléchargé correspond à une œuvre protégée, ce fichier pourrait être licite. Il pourrait s'agir d'un envoi à soi-même, comme évoqué précédemment, ou d'une copie licite d'une œuvre achetée, ou encore du téléchargement d'une œuvre achetée sur une plateforme d'offres légales.

De plus, il faut rappeler que toute information peut être chiffrée, ce qui empêche l'analyse du contenu de la communication. Il est possible de réencoder un fichier sous un autre format, de l'altérer de façon à en changer la signature, etc. Les internautes utilisent d'autres systèmes encore : sites warez, réseaux cryptés, listes de diffusion... Sans doute tout cela n'est-il pas à la portée du petit contrevenant occasionnel mais les solutions évoquées peuvent se communiquer sur le réseau à la vitesse des kilobits. Au surplus, le déploiement de la prochaine génération du protocole IP, IPv6, en incluant le cryptage de bout en bout (IPsec), va empêcher toute analyse intermédiaire et donc toute possibilité de filtrage.

Par ailleurs, à supposer levées les objections qui viennent d'être formulées, on sait que des logiciels de filtrage existent déjà, en matière de pornographie infantile ou de racisme et de xénophobie, ou encore de contrôle parental au sens large. Ces logiciels de contrôle parental fonctionnent par systèmes de listes noires pour les adolescents (liste des sites interdits, tous les autres étant autorisés) ou de listes blanches pour les enfants (liste des sites autorisés, tous les autres étant interdits). L'on sait aussi qu'ils

sont d'une efficacité variable, certains étant reconnus comme excellents mais d'autres aussi de qualité « très mauvaise », voire « catastrophique ». Pourquoi en irait-il autrement des logiciels de filtrage des œuvres protégées ? Qui supporterait le coût final de l'harmonisation par le haut de la qualité de ces logiciels ? Est-ce nécessairement aux internautes de payer la protection des ayants droit par un surcoût de leur abonnement, notamment aux internautes qui n'ont jamais téléchargé quoi que ce fût, même licitement ?

En outre, l'on constate que ces logiciels de contrôle parental ne sont pas obligatoires là où des enfants ont accès à Internet et que par suite aucune amende ne sanctionne leur non installation. Ne serait-il pas surprenant que la société considère comme plus grave de copier une œuvre protégée que laisser les enfants avoir accès par inadvertance aux sites pédophiles, violents, haineux ou racistes ?

Enfin, on sait encore que certains logiciels, pour travailler, désactivent automatiquement les mécanismes de protection et qu'ils ne les rebranchent pas toujours ensuite (par exemple le logiciel de jeu World of Warcraft, ou encore le logiciel de téléphonie Skype, ou encore les logiciels Triple Play : offres de télévision, de téléphonie fixe et d'Internet). Peut-on imposer aux internautes des manipulations constantes de ces outils de protection ?

Pour toutes ces raisons, la création d'une contravention de non sécurisation de son installation par l'abonné qui télécharge ne peut être recommandée. Une efficacité minimale, une preuve délicate à rapporter, une désactivation du système, volontaire ou non, facile et parfois inévitable, l'impossibilité de filtrer efficacement, une peine encourue trop faible pour être dissuasive... Une telle incrimination ressortirait à un effet d'annonce sans contribuer sérieusement à la résolution du problème des téléchargements illicites de masse. « Il ne faut point de lois inutiles, elles affaiblissent les lois nécessaires ».

**27.** En second lieu, un **filtrage installé chez le fournisseur d'accès** (ou chez le fournisseur d'hébergement) ou sur un site est-il envisageable ?

Sur le plan du fond, en tout état de cause, il ne doit pas entraver la circulation des logiciels et œuvres libres de droits, en tout ou en partie. Un filtrage empêchant l'abonné d'avoir accès aux plates formes de téléchargement de pair à pair, en les plaçant sur une liste noire, au motif qu'elles servent parfois, ou souvent, ou même la plupart du temps à des téléchargements illicites, ne serait pas admissible. Un tel

filtrage serait également sans efficacité, tant sont nombreuses les possibilités de communication (messageries, newsgroups, forum, etc.). Deux hypothèses semblent à première vue envisageables. La première serait de prévoir que le filtrage n'empêche pas la libre circulation de ces logiciels et œuvres sur les plates formes d'échange notamment (mais nous avons vu qu'un logiciel de filtrage ne peut reconnaître les œuvres protégées, intactes ou maquillées). La seconde serait d'imposer à l'internaute, sous la menace d'une autre contravention de police, de désactiver son système de filtrage lorsqu'il opère un chargement licite (les données de cette désactivation étant alors conservées par les fournisseurs d'accès). Cette seconde hypothèse risque d'être peu réaliste. En tout état de cause, un filtrage chez les fournisseurs d'accès serait redoutablement onéreux : qui paierait ?

**28. Une esquisse de solution** pourrait alors être cherchée dans des accords collectifs entre les ayants droit et les opérateurs de télécommunications, fournisseurs d'accès ou d'hébergement, ou les sites. Seuls ces opérateurs ou ces sites pourraient bloquer la circulation illicite d'œuvres protégées. Un filtrage par protocole ou par port est exclu (voir plus haut). Un filtrage par contenu supposerait une technique de reconnaissance audio et vidéo. Les sites de partage DailyMotion, Snow Reaper, YouTube, par exemple, ont accepté de se doter de certains logiciels de filtrage. L'intérêt des fournisseurs d'accès, qui ont objectivement profité du téléchargement illicite, serait peut-être aujourd'hui de s'équiper eux-mêmes de filtres et de libérer ainsi de la bande passante descendante au profit de leurs propres contenus, tels les offres Triple Play, la Video on Demand ou les bouquets, gros consommateurs de cette bande ?

**28. D'autres réponses** peuvent probablement être apportées aux petits téléchargements en masse d'œuvres protégées. Sans doute ne tariraient-elles pas le flot des contrefaçons, du moins seraient-elles susceptibles de le réduire progressivement.

Ainsi de l'encouragement au développement du téléchargement légal. Pour que le légal concurrence sérieusement l'illicite, il faut que l'internaute y trouve sensiblement les mêmes agréments, le prix mis à part. En téléchargeant licitement, l'internaute paye pour jouir d'une œuvre, choisie au sein d'un catalogue encore limité et dont l'utilisation est bridée par les MTP, ou DRM (le nombre de copies réalisables et les supports sont limités). En revanche, l'internaute qui télécharge illicitement ne paye

pas le bien et dispose d'un choix infini et d'une copie de l'œuvre non bridée par les MTP. Il peut donc en faire un usage illimité. Les MTP (DRM) ont été justifiés par le souci de protéger les prérogatives des ayants droit contre le téléchargement illicite. Or les œuvres se trouvent déjà sur ces réseaux illicites.

Pendant longtemps, l'offre légale a été faible en quantité. Cela s'expliquait, selon les producteurs, par le fait « qu'un certain nombre d'artistes s'opposent au téléchargement car ils ne veulent pas qu'un seul titre soit vendu, d'autres sont attachés à la vente du support avec jaquette, livret de paroles, etc. ». Les choses se sont très largement améliorées depuis quelques mois. Avec 1,2 million de titres proposés, les objectifs de la Charte d'engagements pour le développement de l'offre légale de musique en ligne, le respect de la propriété intellectuelle et la lutte contre le piratage numérique signée le 28 juillet 2006 ont été doublés. L'« atonie » du marché légal que l'on constate ne résulte donc pas d'une offre insuffisamment diversifiée. Le prix dit « psychologique » (psychologiquement acceptable) de 0,99 euro par titre musical (s'inspirant du prix américain de 0,99 dollar) serait versé par souscription d'abonnements et non par carte bancaire, à la pièce.

La question du maintien des mesures techniques de protection (DRM) se poserait avec une plus grande acuité. Les producteurs indépendants de musique semblent sur la voie de les abandonner en permettant l'accès à leurs œuvres sur les plates formes de téléchargement légal au format MP3, donc sans DRM. C'est déjà le cas de VirginMega et de Fnac Music. Il est possible que les majors suivent un jour ce mouvement, à l'instar de l'anglais EMI (mais le prix est majoré).

Pour le cinéma, le maintien des DRM se justifierait pour que les producteurs puissent contrôler la chronologie des médias. Autre protection pour le cinéma contre le piratage des œuvres audiovisuelles récentes : l'apposition d'un filigrane relativement indélébile (watermarking).

Outre l'extension de l'offre et le débridage, il faut continuer de faire confiance à la prévention générale, par exemple au moyen d'annonces télévisées (« la contrefaçon tue la création et voici pourquoi... »), de messages de sensibilisation sur les dangers du téléchargement illicite pour la création artistique imposés aux fournisseurs d'accès par l'art. L. 336-2 CPI. Mais tous ces messages doivent être séduisants, ni rébarbatifs ni solennels, munis d'un texte adapté au langage des jeunes gens d'aujourd'hui (du type « Hey mec ! non mais tu sais ske tu fais là ? arrête !! » mettant en scène des acteurs connus et sympathiques), facilement compréhensibles par ceux qui

formeraient les gros bataillons du téléchargement illicite. Certes, les campagnes de sensibilisation du public n'ont pas remporté dans le passé les effets escomptés. Mais chacun sait que la prévention est un travail de longue haleine et que le progrès d'une idée dans l'opinion publique est lent et non linéaire. Une prévention spéciale par un message d'avertissement personnalisé pourrait-elle être envisagée si la CNIL admettait la conservation temporaire de données personnelles cryptées automatiquement, la clé étant détenue par un tiers de confiance ; seule l'autorité judiciaire pouvant y avoir accès ?



## Annexe : Personnalités consultées

- 13 M. Jean Berbinau, Ingénieur général des Télécommunications, Conseil général des technologies de l'information, ministère de l'Economie, des Finances et de l'Industrie
- 14 M. Sébastien Canevet, maître de conférences à l'Université de Poitiers, membre fondateur, Le Forum des droits sur Internet
- 15 Mme Karine Colin, directrice juridique, Société civile des producteurs de phonogrammes en France
- 16 M. Frédéric Delacroix, délégué général, Association de lutte contre la piraterie audiovisuelle
- 17 Mlle Estelle De Marco, responsable affaires publiques, Association des Fournisseurs d'accès et de services Internet
- 18 M. Giuseppe De Martino, président, Association des Fournisseurs d'accès et de services Internet
- 19 M. Jean Frayssinet, professeur à l'Université Aix-Marseille III Paul Cézanne
- 20 Mme Florence Galeazzi, juriste, Société des auteurs et compositeurs dramatiques
- 21 M. Eric Garandeau, directeur juridique et financier, Centre national de la Cinématographie
- 22 M. Frédéric Goldsmith, directeur des affaires juridiques et sociales, directeur des nouvelles technologies, Syndicat national de l'édition phonographique
- 23 M. Michel Gomez, délégué général, Société civile des auteurs réalisateurs producteurs
- 24 M. Stéphane Grégoire, chargé de mission, Le Forum des droits sur Internet
- 25 M. Gilles Guglielmi, professeur à l'Université Paris II Panthéon-Assas
- 26 M. Marc Hérubel, conseiller du ministre de la Culture et de la Communication pour les nouvelles technologies, le multimédia, le droit d'auteur et les industries culturelles
- 27 Mlle Aurélie Jimenez, chargée de mission, Chambre syndicale de l'édition musicale
- 28 M. Mathias Moulin, juriste, Commission nationale de l'Informatique et des Libertés

- 29 M. François Pellegrini, maître de conférences, Ecole nationale supérieure d'Electronique, Informatique et Radiocommunications de Bordeaux
- 30 Mme Queyrol, Chambre syndicale de l'édition musicale
- 31 M. Pascal Rogard, directeur général, Société des auteurs et compositeurs dramatiques
- 32 M. Jérôme Roger, directeur général, Union des producteurs phonographiques français indépendants
- 33 M. Hervé Rony, directeur général, Syndicat national de l'édition phonographique
- 34 M. Pierre Sirinelli, professeur à l'Université Paris I Panthéon-Sorbonne, membre du Conseil supérieur de la Propriété littéraire et artistique
- 35 Me Christian Soulié, avocat au Barreau de Paris
- 36 M. Hubert Tillet, directeur juridique, Société des auteurs, compositeurs et éditeurs de musique
- 37 M. Christophe Tilmont, vice-président Marketing & Business Development, Société Advestigo
- 38 M. Idzard Van Den Puyl, secrétaire général, Société civile pour la perception et la répartition des droits de représentation publique des films cinématographiques ; directeur général, Agence française International Standard Audiovisual Number

