CONSEIL SUPÉRIEUR DE LA PROPRIÉTÉ LITTÉRAIRE ET ARTISTIQUE

Commission sur la propriété littéraire et artistique et les libertés individuelles

♦ ♦ ♦

PROPRIETE LITTERAIRE ET ARTISTIQUE ET LIBERTES INDIVIDUELLES DANS L'ENVIRONNEMENT NUMERIQUE

♦ ♦ ♦

SOMMAIRE

♦ ♦ ♦

Par lettre de mission en date du 16 octobre 2002, le président du Conseil supérieur de la propriété littéraire et artistique a demandé à une commission présidée par M. Maurice Viennois, conseiller doyen honoraire à la Cour de cassation et vice-président du Conseil supérieur, de réfléchir aux nouveaux déséquilibres apparus entre les droits de propriété littéraire et artistique et les libertés individuelles et de proposer des solutions pour que leur conciliation soit assurée au mieux dans l'environnement numérique. Le présent rapport, qui se substitue au document d'étape présenté lors de la séance du Conseil supérieur du 26 juin 2003, récapitule les conclusions définitives auxquelles elle est parvenue.

♦ ♦ ♦

Corollaires de la liberté d'expression et de création, les droits de propriété littéraire et artistique favorisent le dynamisme de la pensée et la créativité et contribuent ainsi à créer un environnement favorable pour les libertés en général. Dans le même temps, s'agissant de droits de propriété sur des objets ayant vocation à la publicité, les œuvres d'art, ils entrent en tension avec les libertés que revendiquent les personnes qui souhaitent utiliser ces objets ou y avoir accès dans un but de plaisir esthétique et d'élévation de l'esprit.

Cette tension est résolue, dans les sociétés occidentales, par la recherche de compromis juridiques. Ainsi, pendant la durée des droits, les prérogatives des ayants droit limitent la liberté d'accès aux œuvres, leur utilisation et leur exploitation étant normalement subordonnées à l'obtention d'une autorisation, en général accordée en contrepartie d'une rémunération. Mais la protection ainsi instituée n'est pas absolue et souffre, au nom de l'accès du public aux œuvres, des dérogations : d'une part, la durée des droits est limitée et leur extinction se traduit par l'entrée des œuvres dans le domaine public ; d'autre part, même pendant la durée de ces droits, des dérogations y sont apportées en vue de satisfaire les exigences les plus fortes de la société, qu'il s'agisse du *fair use* aux Etats-Unis ou des exceptions aux droits exclusifs prévues par le droit français, comme l'exception pour copie privée.

L'équilibre ainsi atteint apparaît cependant menacé par le développement simultané, au cours des dernières années, des technologies numériques et du réseau Internet, avec les possibilités de reproduction parfaite et de diffusion massive et décentralisée qui y sont associées. Ce nouveau contexte, s'il offre des opportunités nouvelles d'exploitation et d'utilisation licites des œuvres, notamment par le biais de ce qu'il est convenu d'appeler les systèmes de gestion numérique des droits (*digital rights management systems* ou DRMS), favorise en effet la multiplication des actes de contrefaçon, au point de remettre en cause l'effectivité des prérogatives reconnues aux titulaires de droits de propriété littéraire et artistique. Loin d'être neutre, la technique

aboutit ainsi à déplacer la frontière entre liberté de communication et droits de propriété littéraire et artistique, au détriment de ces derniers.

La préoccupation légitime des ayants droit de rétablir l'effectivité de leurs prérogatives dans l'environnement numérique ne saurait toutefois se traduire, en retour, par des atteintes injustifiées à la liberté des utilisateurs : c'est un nouvel équilibre que, dans l'intérêt commun des différentes parties prenantes, il s'agit de rechercher. A cet égard, la commission a identifié deux points de tension principaux entre droits de propriété littéraire et artistique et libertés individuelles.

D'une part, le développement des DRMS, dont l'objet est d'adapter les modes de gestion traditionnels des droits de propriété littéraire et artistique à l'environnement numérique, est susceptible de comporter des risques au regard du droit des utilisateurs au respect de leur vie privée, qui est, selon la jurisprudence constitutionnelle, une composante à part entière de la liberté individuelle[1]. Il convient de prendre la mesure de ces risques potentiels et des moyens de les minimiser, dans le cadre notamment du droit européen et national de la protection des données personnelles. La commission entend toutefois souligner, dès ce stade, que ces risques, par définition, ne constituent qu'un sous-ensemble des risques liés, de manière générale, aux nouvelles technologies de l'information et de la communication, et plus particulièrement à l'Internet. Dans ces conditions, les travaux de la commission, qui ne peuvent, sur ce point, qu'être partiels, doivent être regardés comme une contribution à la réflexion plus générale sur la « vie privée en ligne » qui a lieu dans d'autres enceintes, notamment le Forum des droits sur l'Internet[2].

D'autre part, les instruments traditionnels de prévention et de répression des infractions aux droits de propriété littéraire et artistiques (regroupées sous le terme générique de contrefaçon[3]), dont l'objet est d'assurer l'effectivité des prérogatives reconnues aux ayants droit, doivent être adaptés à l'environnement numérique. La disproportion croissante entre le nombre d'infractions commises, notamment par le biais de l'Internet, et les moyens matériels et juridiques dont dispose l'Etat pour lutter contre la contrefaçon, est en effet patente, ce qui pose la question de la complémentarité entre l'action des pouvoirs publics et celle des ayants droit et de leurs représentants. Ce souci d'efficacité doit cependant, tout particulièrement lorsqu'est en cause la matière pénale, prendre en compte l'exigence de respect des libertés individuelles.

Il importe de souligner, en tout état de cause, que, compte tenu notamment de la dimension transnationale des réseaux ouverts comme l'Internet, les nouveaux instruments techniques et juridiques qu'appelle le contexte de l'économie numérique, en vue de la protection tant des libertés individuelles que des droits de propriété littéraire et artistique, ne pourront être réellement efficaces que s'ils sont relayés aux niveaux européen et international. Ceci milite notamment pour que les questions relatives à la protection de la vie privée examinées dans le présent rapport soient également portées à l'ordre du jour du groupe de travail dit de l'article 29, mis en place par la directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[4]. Au-delà des frontières de l'Union européenne, il est possible d'imaginer des mécanismes du type de celui mis en place par le chapitre IV de cette même directive, qui consiste à assurer un niveau de protection harmonisé à l'échelle européenne pour, ensuite, limiter la possibilité d'échanges de données aux pays assurant un niveau de protection équivalent, et qui, en donnant notamment naissance à l'accord dit « *Safe Harbour* », a permis de tirer vers le haut la coopération internationale en matière de protection des données personnelles.

♦ ♦ ♦

[1] Voir Cons. const., 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, n° 94-352 DC, *Rec.*, p. 170 ; 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*, n° 99-416 DC, *Rec.*, p. 100.

[2] Site Internet: www.foruminternet.org.

[3] V. not., s'agissant du droit d'auteur, l'art. L. 335-2 du code de la propriété intellectuelle : « *Toute édition d'écrits, de composition musicale, de dessin, de peinture ou tout autre production, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon ; et toute contrefaçon est un délit* ».

[4] Directive 95/46/CE du Parlement européen et du Conseil, *J.O.C.E.*, L 281, 23 novembre 1995, p. 31.

Pour clore ces considérations liminaires, il convient de noter, pour mémoire, que la commission a pris connaissance, au cours de ses travaux, de deux questions qu'elle n'a pas examinées de façon approfondie, car elles étaient seulement connexes à son champ d'investigation.

La première est relative aux conséquences, dans la perspective du développement des DRMS, de la coexistence d'un secteur de logiciels « *open source* » (c'est-à-dire dont le code source est public) et d'un secteur de logiciels « *propriétaires* » (c'est-à-dire juridiquement protégés). A l'heure actuelle, l'accès à une œuvre encodée, sous forme numérique, dans un certain format nécessite en général le recours à un logiciel propriétaire. Dans ces conditions, la question se pose, pour certains, de savoir si le contournement de la protection de l'œuvre afin de rendre sa lecture possible par un logiciel *open source*, dans les limites de la licence attachée à cette œuvre, pourrait être regardée comme licite au regard de la prohibition de tels actes de contournement par les traités de l'Organisation mondiale de la propriété intellectuelle (OMPI) du 20 décembre 1996 sur le droit d'auteur et sur les interprétations et exécutions et les phonogrammes et la directive européenne du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information[5]. Pour les représentants des ayants droit et des éditeurs de logiciels, la réponse à cette question est nécessairement négative.

La seconde question a trait aux modalités de la nécessaire conciliation entre les droits de propriété littéraire et artistique et la liberté de l'information. Eu égard aux mises en cause croissantes d'organes d'information par des ayants droit, leurs héritiers ou des propriétaires d'œuvres d'art, on peut se demander, en effet, si toute représentation visuelle ou sonore d'une œuvre à des fins d'information doit être soumise à autorisation, sur le fondement du droit de la propriété littéraire et artistique ou du droit de propriété – certains estimant que cette question n'est pas épuisée par l'existence de l'exception pour courte citation prévue aux articles L. 122-5 et L. 211-3 du code de la propriété intellectuelle.

♦ ♦ ♦

1 SYSTÈMES DE GESTION NUMÉRIQUE DES DROITS ET PROTECTION DE LA VIE PRIVEE

Les systèmes de gestion numérique des droits ont pour objet de permettre l'exploitation et l'utilisation d'œuvres sous forme numérique[6] dans des conditions propres à assurer le respect des droits de propriété littéraire et artistique, notamment par l'octroi d'autorisations correspondant aux prérogatives conférées par la loi aux titulaires de tels droits[7]. A cette fin, ils mettent en œuvre un ensemble d'instruments allant des outils de description des droits, permettant l'expression sous forme numérique des utilisations autorisées par le titulaire, à ce qu'il est convenu d'appeler les « mesures techniques de protection »[8] des contenus, tendant à prévenir les utilisations non conformes aux autorisations accordées. Certains de ces instruments sont spécifiques à la gestion numérique des droits, mais la plupart, par exemple ceux qui ont recours aux techniques de chiffrement, ont été développés et sont utilisés dans d'autres contextes, notamment aux fins de sécuriser les échanges et transactions sur les réseaux ouverts.

Ainsi définis, les DRMS peuvent être regardés comme l'un des instruments de la recherche d'un nouvel équilibre, dans l'environnement numérique, entre les intérêts des différents acteurs de ce qu'on peut appeler l'« économie de la culture ». Dans la mesure où ils tendent à assurer l'effectivité des prérogatives reconnues aux

---

[5] Directive 2001/29/CE du Parlement européen et du Conseil, *J.O.C.E.*, L 167, 22 juin 2001, p. 10.

[6] On distingue parfois les « oeuvres numériques » *stricto sensu*, créées directement sous forme numérique, des « œuvres numérisées », copies numériques d'œuvres originellement créées sous une autre forme.

[7] On a restreint, pour les besoins du présent rapport, la définition de la gestion numérique des droits aux droits de propriété littéraire et artistique ; il convient toutefois de garder présent à l'esprit que, comme le soulignent de nombreux auteurs, les DRMS représentent une voie prometteuse aux fins de garantir la sécurité d'autres types d'échanges sur les réseaux ouverts, par ex. en matière médicale ou scientifique. Pour une présentation générale, v. par ex. Q. Liu, R. Safavi-Naini, N. P. Sheppard, *Digital Rights Management for Content Distribution*, Australian Computer Society, 2003 (http://www.itacs.uow.edu.au/research/smicl/publications/aisw2003.pdf).

[8] Sur cette notion, v. par ex. L. Tellier-Loniewski, E. Joly-Passant, « Les mesures techniques de protection des droits d'auteur dans l'environnement numérique », *Gazette du Palais*, Rec. Juillet-août 2002, p. 1125.

titulaires de droits de propriété littéraire et artistique par la législation en vigueur, leur développement répond à une préoccupation légitime de ces derniers, qui a d'ailleurs trouvé une consécration juridique dans la protection accordée aux mesures techniques auxquelles ont recours ces systèmes par les traités de l'OMPI du 20 décembre 1996 sur le droit d'auteur (article 11) et sur les interprétations et exécutions et les phonogrammes (article 18), d'une part, et par la directive européenne du 22 mai 2001 (articles 6 et 7), d'autre part[9]. Au-delà, la technique rend possible de nouveaux modes d'exploitation des œuvres et, par conséquent, de nouveaux usages, cette diversification présentant potentiellement des avantages importants pour les consommateurs (en termes de service rendu, de prix,…).

Il est clair, en tout état de cause, que, si les DRMS sont théoriquement neutres quant à la nature et à l'étendue des droits des différentes parties prenantes, leur développement est de nature à exercer une influence considérable, difficilement mesurable à l'heure actuelle, sur les modes de consommation culturelle. Dès lors, sans perdre de vue que le développement de ces systèmes répond à la nécessité de rétablir un équilibre (notamment économique) que l'avènement du numérique et des réseaux a rompu au détriment des titulaires de droits de propriété littéraire et artistique, il convient de s'assurer que leur mise en œuvre ne favorise pas, par un retour de balancier excessif, des atteintes à d'autres droits et libertés protégés, et en particulier au droit des consommateurs au respect de leur vie privée. Il ne fait aucun doute que les garanties qui pourront être offertes à cet égard par les concepteurs des DRMS et ceux qui les mettent en œuvre, et le climat de confiance qui en résultera, constituent une condition essentielle du développement de ces systèmes et de la viabilité du modèle économique qu'ils sous-tendent.

Les considérations qui suivent n'ont d'autre ambition que d'apporter un premier éclairage sur les conditions de la conciliation, dans la conception et la mise en œuvre des DRMS, entre les droits de propriété littéraire et artistique et la vie privée des consommateurs. En effet, eu égard au caractère encore émergent et extrêmement évolutif des technologies en cause, et en l'absence, à ce stade, d'un recul suffisant sur les utilisations qui peuvent en être faites, il ne peut s'agir que d'un état des lieux provisoire, qui appelle des réflexions plus poussées associant l'ensemble des acteurs, que ce soit au niveau national ou au niveau européen, voire mondial (dans la mesure notamment où, dans leur grande majorité, les concepteurs de DRMS sont des entreprises américaines ou asiatiques).

1.1 LES DRMS DANS L'ÉCONOMIE NUMÉRIQUE, ENTRE RISQUE ET SÉCURITÉ

Les craintes le plus souvent exprimées, s'agissant des conséquences potentielles des DRMS sur les libertés individuelles, concernent les atteintes à la vie privée des utilisateurs que ces systèmes pourraient favoriser, en permettant le rassemblement et, le cas échéant, l'utilisation à des fins non souhaitées de données personnelles sensibles, car liées à la consommation culturelle. Cette dernière, en effet, est susceptible, plus ou moins directement, de révéler des aspects particulièrement protégés de la vie privée, tels que ceux visés à l'article 8 de la directive du 24 octobre 1995, qui prohibe en principe le traitement « *des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politique, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle* ». Dès lors, même si la finalité des DRMS n'est pas la collecte de données personnelles (le fonctionnement de certains systèmes ne nécessitant d'ailleurs en lui-même, comme on le verra, que très peu de données de ce type), leur utilisation possible à cette fin comporte des risques dont il convient de prendre la mesure.

Dans cette perspective, la présentation du mode de fonctionnement d'un système-type de gestion numérique des droits constitue un préalable nécessaire.

1.1.1 Le fonctionnement des DRMS : du risque à la sécurité

Comme cela a déjà été souligné, les DRMS sont des systèmes émergents, dont les caractéristiques sont loin d'être définitivement fixées et qui peuvent revêtir des formes très variées. La plupart des systèmes actuellement utilisés par les distributeurs de contenus numériques[10] fonctionnent toutefois selon un schéma commun qui, de façon simplifiée, peut être décrit de la façon suivante[11].

---

[9] V. aussi les articles 6 à 15 du projet de loi relatif au droit d'auteur et aux droits voisins dans la société de l'information, déposé le 12 novembre 2003 à l'Assemblée nationale (A.N., 2003, n° 1206).

[10] Parmi les principaux concepteurs actuels, on peut citer Microsoft (avec *Windows Media Rights Manager*), IBM (avec *Electronic Media Management System*), InterTrust (avec *Rights|System*), RealNetworks (avec *Helix*

(1) Le principe fondamental de tout DRMS consiste à séparer le contenu de l'œuvre de l'information sur les droits associés à celle-ci, de sorte que seule la réunion de ces deux ensembles de données, le plus souvent après paiement, permette d'exploiter cette œuvre dans les conditions définies par le titulaire des droits. A cette fin, deux opérations doivent être réalisées préalablement à toute distribution.

D'une part, l'œuvre doit subir un « conditionnement » (*packaging*) qui remplit deux fonctions essentielles : rendre son contenu inexploitable pour une personne non autorisée à y accéder et permettre le rapprochement entre ce contenu et les droits qui y sont associés. Pour ce faire, ce contenu est encodé dans un certain format[12], puis chiffré, et des informations complémentaires (*metadata*) y sont adjointes, telles que l'identification de l'œuvre et la localisation des données relatives aux droits (cette dernière information pouvant consister, typiquement, dans l'URL[13] du serveur où les données peuvent être récupérées). Diverses technologies de signature ou de tatouage permettent d'assurer l'intrication de ces informations et du contenu de l'œuvre, de façon à éviter leur séparation[14]. Si ces technologies sont efficaces, l'œuvre peut, sous cette forme, circuler librement, dans la mesure où elle est en principe inexploitable[15].

D'autre part, l'information sur les droits associés à l'œuvre, c'est-à-dire les usages autorisés par le titulaire des droits, conformément aux prérogatives qu'il tire du droit de la propriété littéraire et artistique, est exprimée sous forme numérique, grâce à un langage de gestion des droits (*rights management language*)[16]. Pour une même œuvre, de très nombreuses « licences numériques » sont imaginables : s'agissant par exemple d'un fichier musical, son écoute peut être autorisée à l'exclusion de sa copie, ou cette copie peut être autorisée dans la limite d'un certain nombre d'exemplaires, ou le nombre d'écoutes peut être limité,… A cette information relative aux droits est jointe la clef de déchiffrement permettant d'accéder, conformément à ces droits, au contenu de l'œuvre associée.

(2) Ces opérations étant réalisées, l'œuvre « conditionnée » pourra être distribuée – dans une architecture client-serveur, *via* un serveur de distribution de contenus (*content distribution server*)[17] – tandis que l'information sur les droits, ainsi que la clef de déchiffrement, alimenteront un serveur d'octroi des droits (*rights fulfilment server*)[18]. C'est le rapprochement, simultané ou différé, chez l'utilisateur, des informations contenues dans ces deux serveurs, qui lui permettra d'accéder à l'œuvre. Ceci suppose que deux conditions soient réunies.

D'une part, l'utilisateur devra acquérir les droits correspondants à l'utilisation qu'il entend faire de l'œuvre, ce qui suppose le plus souvent un paiement préalable (auquel cas le DRMS est intégré dans un système classique de commerce électronique). En échange de ce paiement, le serveur de procuration lui retournera une représentation des droits qu'il a acquis, avec la clef permettant d'accéder à l'œuvre. Pour sécuriser cette opération, des techniques d'authentification et de chiffrement sont utilisées. Leur caractéristique commune est d'impliquer la détention, par l'utilisateur, d'un « secret » auquel il n'a pas accès. En effet, un DRMS, à la différence notamment d'un simple échange de correspondances chiffrées, ne peut fonctionner si la protection contre les utilisations non autorisées cesse après que l'utilisateur a reçu les droits : il faut donc éviter qu'il puisse, par exemple, reproduire sa clef privée de façon à transmettre ses droits. Ce « secret » peut prendre, parmi d'autres, la forme d'une carte à puce à insérer dans un décodeur ou d'une clef stockée dans une mémoire informatique ; de la robustesse de sa protection dépend celle du système dans son entier.

Digital Rights Management), Sony (avec *OpenMG*), etc.

[11] Pour une présentation détaillée, v. not. P. Chantepie, M. Herubel, F. Tarrier, *Mesures techniques de protection des œuvres et DRMS*, rapport au ministre de la culture et de la communication, janvier 2003, p. 78 et s. (http://www.culture.gouv.fr/culture/cspla/Mptdrms.pdf) ; J. P. Cunard, K. Hill, C. Barlas, *Tendances récentes dans le domaine de la gestion numérique des droits*, Comité permanent du droit d'auteur et des droits connexes, Organisation mondiale de la propriété intellectuelle, doc. SCCR/10/2, août 2003 (http://www.wipo.int/documents/fr/meetings/2003/sccr/pdf/sccr_10_2.pdf).

[12] Par ex., dans le DRMS de Microsoft, WMA (*Windows Media Audio*) ou WMW (*Windows Media Video*).

[13] *Uniform resource locator*.

[14] Cette intrication est d'ailleurs protégée par l'article 12 du traité de l'OMPI sur le droit d'auteur du 20 décembre 1996 et l'article 7 de la directive européenne du 22 mai 2001.

[15] Le modèle dit de « *super-distribution* » attribue d'ailleurs un rôle central à cette possibilité pour les utilisateurs de diffuser eux-mêmes les œuvres protégées.

[16] Par exemple ODRL (o*pen digital rights language*) ou XrML (*extensible rights markup language*).

[17] L'œuvre peut également être distribuée sur un support physique, comme un disque compact.

[18] L'expression de « serveur de procuration des droits » est parfois utilisée.

D'autre part, l'utilisateur devra disposer d'un « client » adéquat, c'est-à-dire d'un lecteur capable de reconnaître le format dans lequel l'œuvre a été encodée et de procéder à son déchiffrement à l'aide de la clef fournie avec la représentation des droits. Ce lecteur peut être un matériel (décodeur) ou un logiciel[19]. Afin de renforcer la sécurité du système, en évitant que le franchissement d'une protection fasse « tache d'huile », la plupart des DRMS requièrent en outre l'individualisation d'un tel lecteur, c'est-à-dire l'attribution à celui-ci d'un numéro unique.

(3) Enfin, la dernière étape du processus consiste à consolider les données relatives à la consommation des œuvres (*clearing*) de façon à assurer la rémunération des fournisseurs de contenus et, *in fine*, des titulaires de droits – ce que, il convient de le relever, la gestion numérique permet en général de faire de façon beaucoup plus fine que la gestion traditionnelle.

1.1.2 DRMS et vie privée : de la sécurité au risque ?

A partir de l'architecture-type d'un DRMS, il est possible de mettre en évidence un certain nombre de facteurs de risque pour la vie privée des utilisateurs, deux remarques préalables devant toutefois être faites.

D'une part, le risque potentiellement lié aux DRMS dépend de nombreuses variables qui peuvent être combinées de façons extrêmement diverses selon les technologies employées, l'architecture du système, la structure capitalistique du secteur, etc. Le caractère évolutif des DRMS rend malaisé d'apprécier *a priori* quelle combinaison sera, à l'avenir, dominante. Ceci justifie le raisonnement hypothétique en termes de *facteurs de risque* qui a été adopté ici – ces facteurs constituant les leviers sur lesquels il est possible d'influer pour limiter le risque global représenté par un système particulier.

D'autre part, il ressort des travaux de la commission, et notamment des auditions auxquelles elle a procédé, que ces facteurs de risques ne sont pas spécifiques aux DRMS : certains sont communs à toutes les formes de commerce électronique, d'autres à toutes les techniques de sécurisation des échanges en ligne, etc. Les observations qui suivent doivent donc, comme cela a déjà été indiqué, être replacées dans un cadre plus général.

Ces remarques liminaires étant faites, on peut distinguer deux grandes caractéristiques des DRMS qui sont potentiellement porteuses de risques pour la vie privée des utilisateurs[20].

► **L'identification des contenus et la limitation des usages**

La première caractéristique tient à ce que les DRMS supposent une identification des contenus et une limitation technique des usages.

D'une part, comme on l'a vu, l'œuvre « conditionnée », alors même que son contenu est chiffré, est identifiée par les informations contenues dans son en-tête (*header*), un peu à la façon d'un colis qu'on ne pourrait ouvrir mais qui comporterait une étiquette renseignant sur ce qu'il contient. La précision de l'identification dépend de la nature, du caractère explicite et du degré de détail des informations figurant sur

[19] Par exemple *Windows Media Player*, le logiciel de lecture de Microsoft qui, dans ses versions les plus récentes, est partie intégrante d'un DRMS, *Windows Media Rights Management*.

[20] Pour quelques exemples de réflexions sur le sujet accessibles sur l'Internet, v. not. P. Vora, D. Reynolds, I. Dickinson, J. Erickson, D. Banks, *Privacy and Digital Rights Management – A position paper for the W3C workshop on Digital Rights Management*, janvier 2001 (http://www.w3.org/2000/12/drm-ws/pp/hp-poorvi2.html) ; J. Feigenbaum, M. J. Freedman, T. Sander, A. Shostack, « Privacy Engineering for Digital Rights Management Systems », in *Proceedings of the 2001 ACM Workshop on Security and Privacy in Digital Rights Management*, Lecture Notes in Computer Science, vol. 2320, Springer, Berlin, 2002, pp. 76-105 (http://www.cs.yale.edu/homes/jf/FFSS.pdf); J. E. Cohen, « A Right to Read Anonymously : A Closer Look at 'Copyright Management' in Cyberspace », *Connecticut Law Review*, 1996, n° 28, p. 981 (http://www.law.georgetown.edu/faculty/jec/read_anonymously.pdf) ; « Some Reflections on Copyright Management Systems and Laws Designed to Protect Them », *Berkeley Technology Law Journal*, 12, n° 1, printemps 1997 ; « DRM and Privacy », *Berkeley Technology Law Journal*, 18, n° 2, printemps 2003 (http://www.law.berkeley.edu/journals/btlj/articles/vol18/Cohen.stripped.pdf).

cette « étiquette »[21]. Potentiellement, cette carte d'identité peut permettre de repérer aisément de quels types d'œuvres un utilisateur dispose sur son terminal, lesquelles il échange, etc…

D'autre part, l'acte d'achat (voire de distribution à titre gratuit) lui-même permet, comme dans toute situation de commerce électronique, de renseigner le vendeur sur la nature de l'œuvre acquise. A cet égard, la circonstance que le distributeur utilise un DRMS n'introduit, en soi, aucune différence par rapport à la situation d'un site de vente en ligne spécialisé dans les produits culturels sur supports traditionnels (tel qu'Amazon, par exemple). Toutefois, la séparation entre le contenu et les informations relatives aux droits qui caractérise les DRMS, associée à la souplesse des langages de description des droits, permet de dissocier des autorisations qui, lorsque l'œuvre est vendue sur un support physique traditionnel, ne pouvaient l'être (par exemple, les auditions successives d'une même œuvre musicale). Dans ces conditions, il est permis de penser que l'acte d'achat lui-même renseigne sur les habitudes de consommation du client de manière plus fine que dans une situation de commerce électronique classique.

La finesse de ces informations dépend, en réalité, de deux facteurs essentiels.

(1) Le premier est l'étendue de la « licence électronique » accordée à l'utilisateur. Dans l'hypothèse de base, la licence électronique ne diffère pas de ce qu'elle est lorsque l'œuvre est distribuée sur un support traditionnel. C'est le cas, par exemple, lorsqu'un fichier musical est téléchargé avec le droit de l'écouter sans aucune limite (téléchargement permanent) : en principe, le distributeur ne retire de l'acte d'achat aucune information supplémentaire par rapport à celles dont il disposerait sans recourir à un DRMS. En revanche, à mesure que la discrimination entre les usages se fait plus fine – par exemple si le nombre d'utilisations est restreint, soit en nombre d'écoutes, soit en temps (téléchargement temporaire) – et alors même que chaque utilisation, dans le cadre de la licence, peut avoir lieu sans que l'utilisateur ait à s'identifier auprès du distributeur (*off-line*), l'acte d'achat se fait plus significatif. Ceci est d'autant plus vrai que, dans une telle situation, si l'utilisateur souhaite, une fois ses droits épuisés, continuer d'avoir accès à l'œuvre, il devra renouveler sa licence, ce qui impliquera un nouvel acte d'achat. Les informations que le distributeur sera à même de collecter peuvent, dans ces conditions, atteindre une grande finesse – et présenter, par suite, une haute « valeur ajoutée » commerciale.

(2) Le second facteur est le mode d'octroi des droits et de limitation des utilisations. Dans l'hypothèse basse, l'octroi des droits est dissocié de l'utilisation, ce qui revient à dire que le distributeur n'est pas à même de savoir quand et dans quelles conditions cette utilisation a lieu. Le contrôle se fait à distance et de façon « aveugle », par le biais des mesures techniques qui interdisent à l'utilisateur d'outrepasser les droits qui lui ont été octroyés. Dans l'hypothèse haute, en revanche, l'octroi des droits et l'utilisation sont parfaitement concomitants : c'est le cas, par exemple, lorsque sont utilisées des techniques proches du *streaming*, qui permet la lecture des données en cours de téléchargement[22]. Par exemple, dans le système développé par la société Medialive, si les fichiers contenant l'œuvre elle-même peuvent être téléchargés séparément, l'octroi des droits s'effectue en ligne, à l'occasion de la lecture de l'œuvre, et contre paiement[23]. Le prestataire, dans une telle situation – proche de celle de la télévision à péage – est à même de connaître avec précision les dates et heures de consultation des œuvres. Il s'agit d'une caractéristique commune à tous les services que l'on regroupe sous l'expression de « *pay-per-view* ».

► **L'identification et l'authentification des utilisateurs**

La deuxième caractéristique à risque des DRMS tient à ce qu'ils mettent en œuvre des techniques d'identification et d'authentification des utilisateurs – étant noté d'emblée que cette caractéristique est commune à toute transaction sécurisée dans l'environnement numérique.

On peut à cet égard identifier trois facteurs de risque.

---

[21] V. sur ce point not. S. Bechtold, « The Present and Future of Digital Rights Management – Musings on Emerging Legal Problems », *in* E. Becker, W. Buhse, D. Günnewig, N. Rump, *Digital Rights Management – Technological, Economic, Legal and Political Aspects*, Springer, Berlin, 2003, p. 618 (http://www.jura.uni-tuebingen.de/bechtold/pub/2003/Future_DRM.pdf).

[22] V. par ex., sur cette notion, R. Sermier et A. Emrich, « Les enjeux juridiques du streaming », *Les Petites Affiches*, 14 mai 2002, n° 96, p. 6.

[23] V. le site Internet de la société (http://www.media-live.net) ainsi que le rapport précité de P. Chantepie *et al.*, p. 110.

(1) Le premier est lié au caractère plus ou moins directement personnel des informations rassemblées.

On rappellera qu'aux termes du a) de l'article 2 de la directive du 24 octobre 1995, on entend par donnée à caractère personnel « *toute information concernant une personne physique identifiée ou identifiable* », et qu'« *est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* ». Le 26e considérant de la directive précise que, « *pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne* ». Le risque d'utilisation des données personnelles à des fins non souhaitées, et les conséquences d'un tel détournement, sont évidemment d'autant plus grands que ces données permettent plus directement de remonter jusqu'à l'identité réelle de la personne. Par exemple, s'il est admis, tant par la Commission nationale de l'informatique et des libertés (CNIL) que par le groupe de l'article 29, que l'adresse IP (*Internet protocol*) est une donnée personnelle[24], elle ne peut permettre de remonter jusqu'à l'identité réelle de l'internaute qu'une fois rapprochée des données de connexion (*logs*) détenues par le fournisseur d'accès[25]. Plus malaisée encore peut être l'identification lorsque sont en cause des numéros d'identification de matériels ou de logiciels (alors même qu'il n'est guère douteux qu'un identifiant unique directement lié au terminal de l'utilisateur constitue, pour l'application de la directive du 24 octobre 1995, une donnée personnelle[26]).

On peut donc estimer, au bénéfice de ces observations, que le caractère plus ou moins directement personnel des informations collectées au cours du processus de distribution d'une œuvre constitue un facteur de risque pour la vie privée des utilisateurs. Il convient toutefois de noter que le fonctionnement d'un DRMS ne requiert en lui-même la collecte que d'un nombre limité de données directement personnelles, l'utilisation d'un pseudonyme comme identifiant étant le plus souvent possible[27]. En réalité, c'est généralement l'acte de commerce électronique associé à la distribution sécurisée de l'œuvre qui nécessite la collecte de telles données (adresse électronique, numéro de carte bancaire, etc.). D'une certaine façon, à cet égard, la possibilité offerte par les DRMS de sécuriser la distribution de contenus numériques permet même, par rapport à une situation de commerce électronique classique, de réduire le nombre de données nécessaires à la conclusion de la transaction : en particulier, dès lors que la distribution s'effectue uniquement en ligne, aucune correspondance postale n'est nécessaire pour délivrer le produit. Si, au surplus, l'acheteur utilise un moyen de paiement anonyme, comme une carte prépayée, on peut sans difficulté imaginer des situations où aucune donnée directement personnelle ne serait collectée par le distributeur.

---

[24] Ou *nominative*, selon la terminologie propre à la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction actuelle.

[25] V. sur ce point *infra*, 2.1.3.

[26] V. par ex., s'agissant de l'adresse MAC unique de la carte Ethernet, l'avis 2/2002 du groupe de l'article 29 du 30 mai 2002 *relatif à l'utilisation d'identifiants uniques dans les terminaux de télécommunications : l'exemple de l'IPv6*, WP 58, 10750/02/FR/Final.

[27] Des considérations commerciales, liées à la réticence des consommateurs à fournir certaines informations, incitent du reste fortement les distributeurs à limiter spontanément le nombre des données recueillies, lorsqu'elles ne sont pas absolument nécessaires au fonctionnement du système.

(2) Le deuxième facteur de risque est lié à ce qu'on peut appeler la concentration des données collectées. En effet, le fonctionnement d'un DRMS met en jeu plusieurs bases de données, liées entre elles mais pas nécessairement consolidées. Par exemple, il est tout à fait imaginable que les informations relatives à la gestion des droits, qui sont les plus sensibles en terme de suivi des habitudes culturelles, soient séparées de celles relatives à la facturation, qui sont en général, comme on l'a vu, plus directement personnelles. A cet égard, le degré d'intégration du processus, c'est-à-dire le nombre des acteurs intervenant tout au long de la chaîne de distribution, est un facteur déterminant : il n'est pas indifférent, de ce point de vue, que la conception du DRMS, la gestion du catalogue d'œuvres, la commercialisation, la gestion des droits, etc., soient le fait d'une même société ou de plusieurs. Dans la pratique, des situations très diverses se rencontrent, les plus favorables du point de vue de l'utilisateur étant celles où les différents rôles, au sein de l'architecture-type décrite plus haut, sont répartis entre des acteurs indépendants en termes juridiques et capitalistiques.

(3) Le troisième facteur de risque, enfin, est lié à l'utilisation ou non d'identifiants uniques. Le profilage des habitudes d'un consommateur est en effet d'autant plus aisé qu'il est possible de faire le lien, soit entre des transactions successives auprès d'un même prestataire, soit entre des transactions différentes auprès de plusieurs prestataires – et ce lien sera lui-même aisé à établir si l'intéressé, au-delà des pseudonymes qu'il peut être amené à utiliser, est identifié de la même façon, dans le temps et dans l'espace.

Or la sécurisation des opérations, notamment au sein d'un DRMS, requiert de plus en plus souvent le recours à des identifiants uniques, attachés le plus souvent au « client », logiciel ou matériel, de l'utilisateur. Par exemple, dans le DRMS de Microsoft, l'individualisation de *Windows Media Player* repose sur la génération d'un fichier DLL[28] qui utilise l'identifiant matériel unique de l'ordinateur. D'autres systèmes, qui, sans constituer en eux-mêmes des DRMS, pourraient revêtir un intérêt pour la gestion numérique des droits, reposent également sur ce type d'identifiants : c'est le cas notamment du projet *Palladium* (aujourd'hui rebaptisé *Next Generation Secure Computing Base*) de Microsoft, qui utilise une clef matérielle secrète pour sécuriser les opérations.

Le recours à de tels identifiants permet potentiellement de consolider un grand nombre de données relatives à un même utilisateur, ce qui a notamment justifié les interventions du groupe de l'article 29 à l'occasion du développement, par Microsoft, du système .NET Passport, utilisé par exemple par la plateforme de distribution de musique en ligne Pressplay[29]. Il pourrait notamment en être ainsi à l'occasion des mouvements de concentration capitalistique, fréquents dans le secteur des nouvelles technologies, comme l'illustre la tentative de DoubleClick après le rachat d'Abacus[30].

1.2 OPTIONS POUR LA LIMITATION DES RISQUES LIÉS AUX DRMS : DES PRINCIPES À LA GARANTIE CONCRÈTE DES DROITS

A partir de l'analyse développée ci-dessus, la commission s'est interrogée sur la capacité du cadre normatif existant, en matière notamment de protection des données personnelles, mais aussi de liberté de communication et de protection des consommateurs, à assurer la minimisation des facteurs de risques identifiés. Elle estime que, en l'état actuel et prévisible des techniques, l'adoption de règles spécifiques aux DRMS, qui seraient nécessairement redondantes par rapport aux dispositions transversales en matière de protection de la vie privée et courraient le risque de devenir rapidement obsolètes, ne s'impose pas. Il convient plutôt, dans le dialogue avec les différentes parties prenantes, d'assurer dans la pratique, selon des modalités souples et adaptées aux réalités de l'économie numérique, l'effectivité des garanties existantes.

1.2.1 Un encadrement juridique satisfaisant

[28] *Dynamic link library*.
[29] V. not le document de travail *concernant les services d'authentification en ligne* adopté le 29 janvier 2003, 10054/03/FR WP 68.
[30] En 1999, DoubleClick, régie publicitaire en ligne détenant des données de navigations anonymes sur des millions d'internautes, a tenté de recouper ses données avec celle des 88 millions de fichiers nominatifs détenus par Abacus Direct, société de marketing qu'elle venait de racheter. DoubleClick a renoncé provisoirement à son projet à la suite des réactions de l'opinion publique (S. Godeluck, *La géopolitique d'Internet*, La Découverte, 2002, pp. 128-129).

Le cadre juridique existant en matière de protection de la vie privée, qu'il soit de portée générale ou plus spécifiquement lié aux activités en ligne, a naturellement vocation à s'appliquer aux DRMS et aux prestataires qui les mettent en œuvre. Il présente l'avantage substantiel d'être, pour une grande part, d'origine communautaire, le caractère supranational des garanties étant de nature à en renforcer l'effectivité. La commission estime en particulier qu'une transposition complète et rapide des directives européennes pertinentes, et notamment de celle du 24 octobre 1995, est de nature à assurer une prise en compte adéquate des risques liés aux DRMS.

Les garanties les plus pertinentes au regard des facteurs de risques identifiés sont les suivantes.

(1) S'agissant en premier lieu du risque général d'utilisation à des fins non souhaitées, qu'elles soient licites ou illicites, des données à caractère personnel collectées à l'occasion de la distribution de contenus numériques, on rappellera, d'une part, que le b) de l'article 6 de la directive du 24 octobre 1995 exige que ces donnés soient « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités* », d'autre part, que l'article 17 § 1 du même texte fait obligation au responsable du traitement de « *mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite* ». La première de ces dispositions interdit par exemple, si des données sont collectées uniquement en vue de la facturation ou de la gestion des droits de propriété littéraire et artistique (laquelle est l'objet même d'un DRMS), de les utiliser à d'autres fins ; la seconde instaure une obligation générale de sécurité des traitements, proportionnée au caractère sensible des données collectées.

(2) Aux termes du c) de l'article 6 de la directive du 24 octobre 1995, les données collectées doivent être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement* ». En vertu de ce principe de proportionnalité, un distributeur de contenus numériques en ligne ne peut collecter que les données qui sont strictement nécessaires, notamment, à l'« *exécution du contrat* » qui le lie au consommateur. Comme cela a déjà été souligné[31], la logique commerciale incite spontanément, en général, le distributeur à limiter au maximum la quantité de données à caractère directement personnel qu'il collecte, afin de ne pas faire fuir les consommateurs, très sensibles aux problématiques de protection de la vie privée. Toutefois, au-delà de l'obligation faite aux responsables de traitements d'indiquer « *si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences d'un éventuel défaut de réponse* »[32], une réflexion approfondie sur l'équilibre des obligations dans les contrats de distribution de contenus numériques en ligne et sur les possibilité concrètes d'« *opting out* » offertes des consommateurs apparaît souhaitable afin d'assurer, dans la pratique, le respect du principe de proportionnalité.

(3) Comme le groupe de l'article 29 a eu l'occasion de le rappeler à de nombreuses reprises, « *pour que le traitement des données à caractère personnel soit légitime, il faut que la personne concernée soit informée d'un tel traitement et qu'elle en ait donc connaissance* ». Cette exigence découle notamment de l'article 10 de la directive du 24 octobre 1995[33], qui doit être regardé comme prohibant les traitements dits « invisibles », c'est-à-dire effectués à l'insu du consommateur (logiciels « espions »,…)[34]. On peut penser, par exemple, que ces dispositions excluent que l'envoi d'informations à caractère personnel vers un serveur aux fins d'octroi des droits puisse se faire sans que l'utilisateur en soit informé. Le groupe de l'article 29, comme la CNIL, soulignent en outre la nécessité d'une information fréquente sur ce type de traitements (normalement à chaque transmission de données).

On rappellera également que, lorsqu'est en cause un distributeur de contenus numériques, les obligations d'informations prévues par la directive du 24 octobre 1995 sont renforcées par les dispositions d'ordre public de la section II du chapitre I du titre II du livre I du code de la consommation, prises pour la transposition de la directive européenne du 20 mai 1997 concernant la protection des consommateurs en matière

[31] V. *supra*, 1.1.2.
[32] Directive du 24 octobre 1995, art. 10.
[33] V. aussi le 38e considérant de la même directive : « *le traitement loyal des données suppose que les personnes puissent connaître l'existence des traitements et bénéficier, lorsque les données sont collectées auprès d'elles, d'une information effective et complète au regard des circonstances de cette collecte* ».
[34] On peut indiquer, par contraste, que ce type de procédés est extrêmement fréquent dans les systèmes de *peer-to-peer*, sans qu'existe aucune garantie quant à l'usage qui sera fait des informations collectées.

de contrats à distance[35], et en particulier celles de l'article L. 121-18, qui prévoit la communication au consommateur, « *de manière claire et compréhensible, par tout moyen adapté à la technique de communication à distance utilisée* », d'un certain nombre d'informations spécifiques, sous peine de sanctions pénales. Plus généralement, l'intégration d'un DRMS dans un système de commerce électronique a pour effet de rendre applicable l'ensemble des garanties prévues par le droit de la consommation.

(4) Les possibilités de communication des données personnelles à des tiers sont, quant à elles, strictement encadrées. Ainsi, l'article 14 de la directive du 24 octobre 1995 prévoit par exemple un droit d'opposition à la transmission à des tiers à des fins de prospection. On peut par ailleurs estimer que l'article 3 de la loi du 30 septembre 1986 relative à la liberté de communication, en vertu duquel « *le secret des choix faits par les personnes parmi les services de télécommunication et parmi les programmes offerts par ceux-ci ne peut être levé sans leur accord* », interdit la communication à des tiers de données susceptibles de porter atteinte à ce secret, sauf accord exprès de l'intéressé. Il y a là une limite forte, propre au droit national, à la diffusion des données portant sur les contenus consultés[36].

(5) Enfin, le e) de l'article 6 de la directive du 24 octobre 1995 prévoit que les données personnelles peuvent être « *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement* ». C'est ce qu'il est convenu d'appeler le « droit à l'oubli ». Dès lors que, dans un DRMS, un certain nombre d'opérations statistiques, comme l'agrégation des données de consommation pour assurer la rémunération des ayants droit, peuvent être efficacement assurées avec des données anonymes, il est permis de penser que les dispositions précitées s'opposent à ce que les données soient conservées, à cette seule fin, sous une forme personnelle.

Dans l'état actuel des travaux parlementaires, le projet de loi relatif à protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, adopté en première lecture par le Sénat le 1er avril 2003[37], apparaît propre à garantir une transposition complète de la directive du 24 octobre 1995 sur les différents points évoqués ci-dessus. Il est important que l'adoption définitive de ce texte puisse se faire rapidement, afin de donner leur plein effet aux garanties qu'il prévoit.

1.2.2 Des garanties dont l'effectivité doit être assurée

Sous réserve de la complète transposition de la directive du 24 octobre 1995, le cadre juridique existant apparaît donc apte à assurer la minimisation des principaux facteurs de risque liés à la mise en œuvre des DRMS. Dans ces conditions, la commission s'est attachée à explorer les voies d'une garantie effective et réaliste des droits ainsi reconnus aux utilisateurs, afin de favoriser l'instauration d'un climat de confiance permettant aux différents acteurs de bénéficier pleinement des avantages offerts par ces systèmes.

A cet égard, deux pistes, qui ne sauraient évidemment prétendre à l'exhaustivité, lui sont apparues prometteuses.

- **Encourager l'intégration des préoccupations relatives à la protection de la vie privée dans la conception des DRMS**

Il ressort des travaux de la commission que le meilleur moyen de prévenir les risques potentiellement liés à la mise en œuvre des DRMS est d'intégrer les préoccupations relatives à la vie privée dans la conception même de ces systèmes. On a vu, en effet, que l'intensité de ces risques dépend beaucoup de l'architecture même du système, du type de technologies auxquelles il a recours, etc. C'est donc dès la conception qu'il convient d'intervenir – la technique, qui est fondamentalement à « double visage », comportant souvent en elle-même un début de réponse aux risques qu'elle génère[38].

[35] Directive 97/7/CE du Parlement européen et du Conseil, *J.O.C.E.*, L 144, 4 juin 1997, p. 19.
[36] V. aussi *infra*, 2.2.2.
[37] Sénat, texte adopté n° 96, 2002-2003.
[38] V. par ex., sur les moyens techniques de protection de la vie privée en ligne, L. Cadoux, « Les réponses technologiques », *Les Petites Affiches*, n° 224, 10 novembre 1999, p. 47.

Parmi de nombreux autres, l'exemple déjà cité de l'affaire .NET Passport montre comment un dialogue entre autorités de régulation (en l'occurrence le groupe de l'article 29) et concepteurs de solutions techniques (Microsoft) peut être fructueux en la matière. Cette logique de dialogue imprègne d'ailleurs nombre des dispositions du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel[39]. Le souci d'intégration des préoccupations relatives à la vie privée dès la conception des systèmes n'est pas non plus étranger au droit communautaire[40]. Ainsi le groupe de l'article 29 a-t-il pu, sur le fondement de la directive du 24 octobre 1995, « *encourage[r] l'industrie du logiciel et du matériel informatique à travailler sur des produits respectant la vie privée sur l'Internet qui fournissent les outils nécessaires pour se conformer aux règles européennes relatives à la protection des données* »[41]. Sa position constante consiste à souligner que le « *principe de proportionnalité (…) entre les droits fondamentaux des personnes objets des données et les intérêts des différents acteurs intervenant dans la transmission de données de télécommunication (…)* » implique que, « *bien que la technologie soit neutre par nature, les applications et la conception de nouveaux dispositifs de télécommunication devraient par défaut être compatibles avec le respect de la vie privée* ».

S'agissant plus spécifiquement des DRMS, on relèvera qu'aux termes du 57e considérant de la directive du 22 mai 2001, dès lors que « *les systèmes relatifs à l'information sur le régime des droits (…) peuvent (…), selon leur conception, traiter des données à caractère personnel relatives aux habitudes de consommation des particuliers pour ce qui est des objets protégés et permettre l'observation des comportements en ligne* », « *ces moyens techniques doivent, dans leurs fonctions techniques, incorporer les principes de protection de la vie privée, conformément à la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 (…)* ». Cette préoccupation se retrouve à l'article 9 de la même directive, en vertu duquel celle-ci « *n'affecte pas les dispositions concernant notamment (…) la sécurité, la confidentialité, la protection des données personnelles et le respect de la vie privée* ». On peut voir dans ces dispositions, en contrepartie de la protection juridique accordée aux mesures techniques, l'obligation pour celles-ci d'intégrer les principes de protection de la vie privée – et, plus généralement, un soutien à ce qu'il est convenu d'appeler les « technologies de protection de la vie privée » (*privacy enhancing technologies*)[42]. De nombreux observateurs soulignent d'ailleurs que les techniques utilisées par les DRMS, et plus largement l'architecture sur laquelle ils reposent, peuvent précisément être utilisées aux fins de protéger les droits des utilisateurs[43].

Dans cette perspective, la commission souligne l'intérêt du pouvoir, reconnu à la CNIL par le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, de « *délivre[r] un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elle les a reconnus conformes aux dispositions de la présente loi* » (art. 11, 2°, c, de la loi du 6 janvier 1978 dans sa rédaction issue de l'art. 3 du projet de loi). La voie de la labellisation, qui a déjà été empruntée par de nombreuses sociétés ou organisations pour garantir le

[39] V. not., sur ce point, le rapport de M. A. Türk, Sénat, 2002-2003, n° 218, p. 42 et s.

[40] V. par ex. la directive 1999/5/CE du Parlement européen et du Conseil du 9 mars 1999 concernant les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité, dont l'article 3 § 3 dispose notamment que « *la Commission peut décider que les appareils relevant de certaines catégories d'équipements ou certains types d'appareils sont construits de sorte : (…) c) qu'ils comportent des sauvegardes afin d'assurer la protection des données à caractère personnel et de la vie privée des utilisateurs et des abonnés* ».

[41] Recommandation 1/99 du 23 février 1999 *sur le traitement invisible et automatique des données à caractère personnel sur l'Internet effectué par des moyens logiciels et matériels*, WP 17, 5093/98/FR/final.

[42] V. toutefois sur ce point les vues sceptiques de L. A. Bygrave, « The Technologisation of Copyright : Implications for Privacy and Related Interests », *European Intellectual Property Review*, 2002, vol. 24, n° 2, pp. 51-57 (http://folk.uio.no/lee/publications/technologisation_copyright_eipr_final.pdf).

[43] V. not., développant la notion de « *privacy rights management systems* », L. Korba, S. Kenny, *Towards Meeting the Privacy Challenge : Adapting DRM*, ACM Workshop on Digital Rights Management, novembre 2002 (http://crypto.stanford.edu/DRM2002/KorbaKennyDRM20021.pdf).

respect de standards minimaux en matière de protection de la vie privée (TRUSTe[44], BBBOnLine[45], WebTrust[46], etc.), apparaît en effet prometteuse. La faculté ouverte à la CNIL par la disposition précitée pourrait tout à fait s'appliquer à des DRMS, ainsi qu'aux plateformes de distribution des prestataires de services qui les mettent en œuvre (par exemple les sites Internet de distribution de musique en ligne).

Si cette disposition du projet de loi devait être définitivement adoptée, la commission invite donc la CNIL à faire un usage effectif du pouvoir qui lui serait ainsi reconnu, en concertation avec les concepteurs et les utilisateurs de DRMS. Il convient de souligner que, pour être efficace, un mécanisme de labellisation supposerait un audit périodique des systèmes et plateformes concernés, et une possibilité corrélative de retrait du label en cas de résultat négatif – cette menace de retrait pouvant s'avérer, eu égard à la sensibilité des consommateurs à l'égard de la protection des données personnelles en ligne, particulièrement dissuasive pour les prestataires concernés.

► **Favoriser l'élaboration de codes de bonne conduite adaptés aux spécificités des secteurs concernés**

L'expérience montre que les dispositions destinées à assurer la collecte loyale des données personnelles ne peuvent atteindre leur objectif que si l'application qui en est faite par les opérateurs est elle-même loyale, c'est-à-dire conforme à l'esprit des textes[47]. Par ailleurs, l'application des dispositions générales de la loi du 6 janvier 1978 au cas spécifique des DRMS peut susciter des difficultés pratiques non négligeables : il en va ainsi, entre autres, de la notion de « responsable du traitement », malaisée à appliquer dans le cadre d'une architecture complexe, le flou parfois entretenu à cet égard étant de nature à favoriser la dilution des responsabilités[48].

Dans ces conditions, la commission estime que certaines modalités pratiques de mise en œuvre de la loi du 6 janvier 1978, dans sa nouvelle rédaction, et de ses décrets d'application pourraient être définies en tant que de besoin par voie de recommandations de la CNIL ou du groupe de l'article 29.

En outre, mériterait d'être plus systématiquement explorée la voie prometteuse des codes de bonne conduite.

On rappellera à cet égard que le 1er paragraphe de l'article 27 de la directive du 24 octobre 1995 dispose que « *les Etats membres et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions nationales prises par les Etats membres en application de la présente directive* ». Cette invitation doit être rapprochée, s'agissant des prestataires de services en ligne, des dispositions de l'article 10 de la directive européenne du 8 juin 2000 sur le commerce électronique[49], qui fait figurer, au nombre des informations à fournir aux consommateurs par le prestataire de service, les « *éventuels codes de conduite pertinents auxquels il est soumis ainsi que les informations sur la façon dont ces codes peuvent être consultés par voie électronique* », codes dont l'article 16 encourage l'élaboration, à l'initiative des Etats membres et de la Commission, en concertation avec les consommateurs.

La commission invite donc que les autorités compétentes à prendre l'initiative de rassembler les acteurs concernés afin de favoriser l'élaboration concertée de tels codes de conduite, qui pourraient jouer un rôle majeur dans la mise en œuvre effective des garanties prévues par les textes, tout en restant un instrument souple, adapté aux modes de régulation de l'économie numérique et aux évolutions rapides de la technique.

---

[44] Site Internet : www.truste.org.
[45] Site Internet : www.bbbonline.org.
[46] Site Internet : www.webtrust.fr.
[47] V. à ce sujet, par ex., l'évaluation de 100 sites français de commerce électronique diffusée par la CNIL en avril 2000 sous le titre « *Passer du discours sur la protection des données personnelles à la mise en œuvre effective des droits des internautes sur le Web* » (http://www.cnil.fr/thematic/docs/100sites.pdf).
[48] Il est vraisemblable que, dans le cadre de la plupart des DRMS, il conviendra d'identifier différents traitements et donc différents responsables.
[49] Directive 2000/31/CE du Parlement européen et du Conseil *relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur*, *J.O.C.E.*, L 178, 17 juillet 2000, p. 1.

♦♦♦

2 LUTTE CONTRE LA CONTREFAÇON SUR L'INTERNET ET RESPECT DES LIBERTÉS INDIVIDUELLES

Il est devenu banal de dire que la numérisation des œuvres, associée au développement de l'Internet, accroît considérablement les possibilités de contrefaçon. Les reproductions numériques peuvent être mises à disposition sans autorisation soit sur des sites spécifiques, soit par le biais d'échange sur le mode « *peer-to-peer* »[50]. A titre d'exemple, le site Napster comptait, au plus fort de son activité, 70 millions de clients, et les systèmes alternatifs apparus depuis sa fermeture ont permis jusqu'à l'échange de 3 milliards de fichiers musicaux par mois[51]. Par ailleurs, l'Internet permet de délocaliser facilement les sites de contrefaçons, et de les installer dans des « paradis » de propriété littéraire et artistique. Ainsi le site Kazaa était géré en 2002 par une entreprise australienne qui avait installé son serveur au Vanuatu, et accordé des licences d'exploitation à deux entreprises américaines pour l'activité aux Etats-Unis. Cette dissociation des éléments de production permet aux entreprises concernées d'échapper plus facilement aux poursuites, jusqu'à présent avec un certain succès.

Cette situation n'est pas sans rappeler l'évolution qui a eu lieu par le passé en matière de copie privée. Après l'apparition des appareils de copie analogique sur le marché grand public, les ayants droit ont dû accepter que des copies à usage privé soient réalisées en nombre croissant sans leur autorisation. Le législateur a rétabli l'équilibre ainsi rompu en instaurant en 1985 un mécanisme de rémunération pour copie privée, qui s'est substitué dans ce cas précis à l'usage du droit de reproduction.

Toutefois, la comparaison pourrait trouver ici ses limites. En effet, eu égard tant au caractère massif des infractions commises sur les réseaux, notamment par le biais d'échanges de fichiers contrefaisants en *peer-to-peer*, qu'aux possibilités de reproduction parfaite offertes par les technologies numériques, il paraît difficilement envisageable, comme certains ont pu le proposer, de recourir à un système de rémunération équitable (lequel pourrait, par exemple, être assis sur les recettes des opérateurs de télécommunications et/ou des fournisseurs d'accès à l'Internet). Ce n'est d'ailleurs pas la voie empruntée par le droit international et communautaire, qui a, au contraire, entendu accorder une protection juridique aux mesures techniques permettant d'empêcher les usages non autorisés. Les ayants droit entendent donc développer des moyens de lutter efficacement, par une action tant répressive que préventive, contre les infractions aux droits de propriété littéraire et artistiques commises dans l'environnement numérique, et notamment sur les réseaux ouverts.

C'est dans cette perspective que les développements qui suivent s'attachent à examiner dans quelle mesure l'adaptation des instruments traditionnels de lutte contre la contrefaçon est susceptible d'être opérée sans préjudicier aux libertés individuelles.

2.1 LES PROBLÈMES LIÉS À LA RÉPRESSION DES INFRACTIONS DANS L'ENVIRONNEMENT NUMÉRIQUE

La protection pénale accordée au droit d'auteur et aux droits voisins traduit la valeur sociale qui leur est reconnue par le législateur[52] ; la crédibilité de la sanction est également une condition essentielle de l'effectivité de ces droits. On doit donc se demander dans quelle mesure les outils traditionnels de répression de la contrefaçon, dans laquelle les sociétés de perception et de répartition des droits (SPRD)[53] jouent un rôle majeur, doivent être adaptés à l'environnement numérique.

---

[50] La notion de *peer-to-peer*, souvent abrégée en « *P2P* », fait référence à un modèle d'architecture de réseau informatique en vertu duquel, contrairement à ce qui prévaut dans l'architecture dite « client-serveur », les ordinateurs participant au réseau peuvent partager des ressources entre eux sans passer par un serveur central et jouent chacun le rôle de « client » et de « serveur ». On distingue le « *peer-to-peer* assisté » (type Napster), qui a recours à un serveur central jouant un rôle d'indexation, et le « *peer-to-peer* décentralisé » (type Gnutella).

[51] S. Godeluck, *op. cit.*, p. 103 et s.

[52] V. par ex. P.-Y. Gautier, *Propriété littéraire et artistique*, P.U.F., coll. « Droit fondamental », 3e éd., Paris, 1999, p. 623.

[53] Il est fait référence, par cette notion, aux sociétés civiles rassemblant des auteurs, des artistes-interprètes, des producteurs de phonogrammes ou de vidéogrammes, des éditeurs ou leurs ayants droit, régies par le titre II du livre III de la 1re partie du code de la propriété intellectuelle (art. L. 321-1 et s.). On rappellera que ces sociétés

A cet égard, la commission s'est attachée à examiner trois questions plus particulièrement sensibles du point de vue des libertés publiques.

2.1.1 La recherche et la constatation des infractions : problèmes liés aux règles d'administration de la preuve

La première difficulté consiste, pour les victimes de violations des droits de propriété littéraire et artistique, à apporter la preuve de la matérialité des infractions à ces droits[54], comme, par exemple, la mise à disposition sur l'Internet, sans autorisation, d'œuvres sous forme numérique (que ces œuvres soient ou non elles-mêmes contrefaisantes, pour avoir, par exemple, fait l'objet d'une numérisation – c'est-à-dire d'une reproduction – illicite) – étant rappelé qu'outre les modes traditionnels de preuve, comme les procès-verbaux des officiers et agents de police judiciaire, une telle preuve peut efficacement, en vertu de l'article L. 331-2 du code de la propriété intellectuelle, résulter des constatations d'agents assermentés désignés, entre autres, par les SPRD.

Au-delà des obstacles le plus souvent mis en exergue, comme la « volatilité » des contenus accessibles sur l'Internet, qui peuvent changer de localisation (par le biais, notamment, de « sites miroirs ») ou disparaître d'un instant à l'autre, mérite de retenir l'attention une difficulté spécifique, qui tient à ce que la communication, sur ce réseau, s'effectue le plus souvent à l'initiative de l'utilisateur, qui ne se trouve donc pas, comme dans le cas des médias traditionnels, en situation de recevoir passivement un signal[55]. Cette caractéristique, qui ne fait évidemment pas obstacle, comme cela a pu être soutenu par certains, à ce que la mise à disposition du public d'une œuvre sur un serveur soit regardée, notamment, comme une représentation au sens de l'article L. 122-2 du code de la propriété intellectuelle[56], est néanmoins susceptible de poser des problèmes délicats au regard des règles d'administration de la preuve, dont le respect conditionne l'admissibilité de celle-ci par les juridictions, notamment pénales, et qui peuvent, dans une certaine mesure, entrer en concurrence avec l'objectif de manifestation de la vérité judiciaire.

Concrètement, dans le cadre de la lutte contre la contrefaçon sur l'Internet, la question se pose de savoir sous quelles conditions peut être admissible devant les juridictions une preuve dont la constitution passe par le téléchargement ou la consultation, à l'initiative, par exemple, d'un agent assermenté d'une SPRD, d'une œuvre mise à la disposition du public, que ce soit sur un serveur classique ou, dans le cadre d'échanges en *peer-to-peer*, à partir de chacun des ordinateurs individuels des participants.

On relèvera, tout d'abord, qu'un tel agissement n'est certainement pas de nature à se heurter à la prohibition des atteintes à l'intimité de la vie privée, à l'inviolabilité du domicile ou au secret des correspondances – étant précisé qu'une preuve acquise au moyen d'une violation de ces droits, en dehors des hypothèses expressément prévues par les textes, qui prévoient l'intervention préalable d'un juge, ne pourrait qu'être entachée de nullité (au moins lorsque la violation est le fait d'un dépositaire de l'autorité publique, tel qu'un agent de police judiciaire). En effet, il n'est pas douteux que la mise à disposition sur l'Internet d'œuvres sous forme numérique est insusceptible de bénéficier en tant que telle de la protection accordée aux correspondances privées : la Cour de cassation a ainsi clairement jugé, au sujet du Minitel (mais le raisonnement est aisément transposable à l'Internet), qu'un service qui diffuse « *à des personnes indifférenciées des messages*

« *ont qualité pour ester en justice pour la défense des droits dont elles ont statutairement la charge* » (art. L. 321-1, al. 2). Elles peuvent dès lors, dans les conditions du droit commun, mettre en mouvement l'action publique par voie de citation directe des auteurs d'infractions devant le tribunal correctionnel ou, le cas échéant, en déposant plainte avec constitution de partie civile.

[54] La preuve de l'élément moral, qui caractérise normalement toute faute pénale, ne pose pas de problèmes spécifiques, eu égard notamment à la présomption de mauvaise foi qui pèse en général sur les auteurs d'infractions aux droits de propriété littéraire et artistique.

[55] V. sur ce point not. L. Tellier-Loniewski, C. Rojinsky, L. Masson, « Contrefaçon et droit d'auteur sur Internet », *Gaz. Pal.*, 21 octobre 1997, Rec. 1997, doctrine, p. 1337.

[56] V. not. TGI Paris, ord. Réf., 14 août 1996, *Sté Editions musicales Puchenel et a. c/ Ecole centrale de Paris et a.*, JCP, 1996, II, n° 22727, p. 441, note F. Olivier et E. Barbry, estimant, s'agissant des gestionnaires d'un site web, qu'il « *importe peu qu'ils n'effectuent eux-mêmes aucun acte positif d'émission, l'autorisation de prendre copie étant implicitement contenue dans le droit de visiter les pages privées* » ; v. aussi TGI Paris, ord. réf., 5 mai 1997, *Queneau c/ Leroy et a.*, JCP, 1997, II, n° 22906, p. 395, note F. Olivier, RTD com., 50 (3), juil.-sept. 1997, p. 457, obs. A. Françon. V. aussi A. Lucas, *Propriété littéraire et artistique*, coll. « Connaissance du droit », Dalloz, 2002, p. 57 et s.

dont le contenu ne peut, par définition, être personnel » ne saurait, dès lors, être considéré comme émettant des correspondances privées (Cass. crim., 25 octobre 2000, *Bull. crim.*, n° 317, p. 937). Seul un message envoyé, à raison de leur identité, à une ou plusieurs personnes déterminées, est, dans cette approche, susceptible de recevoir la qualification de correspondance privée.

En conséquence, on doit estimer que les offres de téléchargement accessibles au public sur l'Internet relèvent de ce que le projet de loi « *pour la confiance dans l'économie numérique* », adopté par l'Assemblée nationale en deuxième lecture le 8 janvier 2004[57], qualifie de « *communication publique en ligne* », par opposition à la correspondance privée[58]. Il en résulte notamment, comme le juge expressément l'arrêt précité de la Cour de cassation, que « *le fait, pour un enquêteur, de se connecter à un (…) réseau au moyen d'un terminal mis à la disposition du public par l'opérateur, sans modification préalable de l'installation* », ne constitue pas une « *interception de correspondances émises par la voie des télécommunications* » au sens des articles 100 et suivants du Code de procédure pénale – ni, d'ailleurs, une violation de domicile, la notion de « domicile virtuel », invoquée par certains plaideurs, ne pouvant sans abus être étendue à un serveur « web », dont l'objet même est d'être accessible au public constitué par les internautes[59].

D'appréciation plus délicate apparaissent en revanche les exigences liées au principe de loyauté dans la recherche des preuves, principe qui « *a pour objet d'interdire à celui qui administre la preuve l'utilisation de procédés déloyaux, de ruses ou de stratagèmes* »[60]. La portée de ce principe, qui trouve aujourd'hui un fondement conventionnel dans le 1er paragraphe de l'article 6 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, n'est pas aisée à déterminer, dans la mesure où la jurisprudence lui reconnaît une intensité variable selon les branches du droit[61] et la qualité des personnes concernées (les exigences étant plus fortes à l'égard des agents de police judiciaire qu'à celui des simples particuliers).

Quoi qu'il en soit, c'est plus spécifiquement au regard de l'interdiction des provocations à la commission des infractions, affirmée aussi bien par la jurisprudence de la Cour de cassation que par celle de la Cour européenne des droits de l'homme (v., d'une part, parmi de nombreux arrêts, Cass. Crim, 27 février 1996, *Bull. crim.*, n° 93, p. 273 ; d'autre part, Cour EDH, 9 juin 1998, *Texeira de Castro c/ Portugal*, Rec. 1998-IV), que le lancement de requêtes sur l'Internet aux fins de constitution de preuves d'activités contrefaisantes pourrait, dans certaines hypothèses, se heurter au principe de loyauté. Il importe toutefois de souligner que, selon une jurisprudence constante, la provocation n'est caractérisée que s'il est établi que l'agissement litigieux a déterminé la commission de l'infraction, c'est-à-dire que celle-ci n'aurait pas eu lieu sans son intervention (Cass. crim., 2 mars 1971, *Bull. crim.*, n° 71, p. 183). La Cour de cassation estime ainsi, en matière de stupéfiants, qu'une intervention policière dans un contexte préexistant de trafic ne constitue pas une provocation, dès lors que l'acte de police ne peut, dans ces conditions, être considéré comme ayant suscité l'infraction (Cass. crim, 22 juin 1994, *Bull. crim.*, n° 247, p. 592). Or l'infraction consistant dans la mise à disposition du public sans autorisation, sur l'Internet, d'œuvres sous forme numérique doit certainement, en vertu de la jurisprudence la mieux établie en matière de droit de représentation, être regardée comme constituée alors même qu'aucune consultation n'est effectivement intervenue : dans ces conditions, on peut valablement soutenir que la consultation ou le téléchargement de l'œuvre par un agent assermenté n'a aucun rôle dans la commission de l'infraction, qui préexiste et qu'il ne fait que constater. De ce point de vue, la situation n'est pas très différente de celle de l'agent qui se rend dans une boutique pour y dresser procès-verbal de la mise en vente de produits contrefaisants.

Faut-il alors estimer que le procédé consistant, pour un tel agent, à se faire passer, sur le réseau, pour un utilisateur comme un autre, en dissimulant sa qualité, constitue un stratagème déloyal, dont la mise en œuvre entacherait la validité des preuves rassemblées ? Outre qu'une telle interprétation se heurte à la réalité du mode

---

[57] Ass. nat., 2003-2004, texte adopté n° 235.

[58] L'article 1er de ce projet de loi définit la communication publique en ligne comme « *toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, qui s'appuie sur un procédé de télécommunication permettant un échange réciproque d'information entre l'émetteur et le récepteur* ».

[59] V. sur ce point P.-Y. Gautier, « Les œuvres du crooner dans la 'maison' de l'internaute : promenade collective, mais non autorisée, sur un site numérique », note sous TGI Paris, ord. Réf., 14 août 1996, *Sté Editions musicales Puchenel et a. c/ Ecole centrale de Paris et a.*, *Rec. Dalloz*, 1996, jurisp., p. 490.

[60] J. Buisson, V° Preuve, *Rép. Pén. Dalloz*, février 2003, n° 87.

[61] V. par ex. V. Perrocheau, « Les fluctuations du principe de loyauté dans la recherche des preuves », *Les Petites Affiches*, 17 mai 2002, n° 99, p. 6.

de fonctionnement de l'Internet (la consultation de contenus illicites ne nécessitant pas, par définition, de décliner son identité réelle), on peut relever à cet égard que, dans l'arrêt précité du 25 octobre 2000, la Cour de cassation a estimé que le fait pour un enquêteur d'agir sous un pseudonyme pour accumuler des preuves d'une activité délictueuse sur le Minitel ne constituait pas un stratagème susceptible d'entacher la validité desdites preuves, dès lors notamment que la règle, sur le réseau en cause, consistait justement à adopter un pseudonyme.

Au bénéfice de ces observations, la commission estime donc que, en l'état de la technique et de la jurisprudence, le lancement de requêtes sur l'Internet en vue de constater la mise à disposition de fichiers illicites n'est pas contraire au principe de loyauté dans la recherche des preuves. Dans cette mesure, elle ne pense pas qu'une modification législative soit nécessaire pour rendre possibles de telles recherches[62].

2.1.2 Le traitement des données relatives aux infractions : de la prohibition à la liberté encadrée ?

Le caractère massif des actes de contrefaçon dans l'environnement numérique et la très grande volatilité des informations transitant sur les réseaux impose, afin de développer une action préventive et, le cas échéant, répressive efficace, que des traitements automatisés puissent être effectués par les titulaires de droits, c'est-à-dire, en pratique, par les SPRD, bien armées pour lutter contre la contrefaçon et désireuses d'œuvrer de façon efficace pour la protection des ayants droit. Or, dans l'état actuel de la législation, il semble que de tels traitements (par exemple, la collecte d'adresses IP) ne puissent être mis en œuvre par les SPRD.

En effet, aux termes de l'article 30 de la loi du 6 janvier 1978, dans sa rédaction actuelle, « *sauf dispositions législatives contraires, les juridictions et autorités publiques agissant dans le cadre de leurs attributions légales ainsi que, sur avis conforme de la commission nationale, les personnes morales gérant un service public peuvent seules procéder au traitement automatisé des informations nominatives concernant les infractions, condamnations et mesures de sûreté* ». C'est sur le fondement de ces dispositions que la CNIL a eu l'occasion, à plusieurs reprises, de mettre en garde contre le phénomène des « listes noires » de mauvais payeurs ou de personnes suspectées de fraude[63]. C'est également pour cette raison que le président de la CNIL a pu estimer que n'était pas conforme à la législation relative à la protection des données nominatives le logiciel « Webcontrol », développé pour le compte notamment de la Société pour l'administration du droit de reproduction mécanique des auteurs, compositeurs et éditeurs (SDRM). Ce logiciel permettait en effet de repérer sur l'Internet les adresses IP des personnes proposant sur le mode *peer-to-peer* des fichiers musicaux en violation des droits de propriété littéraire et artistique, et d'envoyer à ces personnes un message leur indiquant le caractère illégal de cette mise à disposition – la SDRM s'étant réservé le droit d'utiliser les résultats ainsi obtenus aux fins de preuve devant l'autorité judiciaire. Dans l'analyse de la CNIL, une telle finalité faisait tomber les traitements ainsi réalisés sous le coup de la prohibition édictée par l'article 30 de la loi du 6 janvier 1978, dès lors notamment que, comme on l'a vu[64], les adresses IP sont considérées comme des données indirectement nominatives au sens de cette loi.

Dans ces conditions, deux solutions sont envisageables.

La première consisterait à ouvrir aux SPRD et aux personnes agissant pour le compte des titulaires de droits la possibilité de constituer des fichiers pendant une période limitée, pouvant aller jusqu'à trois mois, après autorisation du procureur de la République. Ces fichiers auraient pour unique objet la transmission au parquet, aux fins de poursuite, des informations ainsi rassemblées, et il ne pourrait en être conservé de copie après cette transmission. Il s'agirait de permettre aux SPRD de mener des « campagnes » de recherche d'infractions, mais non de leur donner cette compétence de façon permanente. Le contenu des fichiers et les méthodes régissant leur constitution seraient définis par un décret en Conseil d'Etat pris après avis de la CNIL.

---

[62] Au demeurant, même une loi ne pourrait en tout état de cause avoir pour effet de faire obstacle à l'application des garanties issues de l'article 6 § 1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

[63] V., en dernier lieu, *Les « listes noires » – Le fichage des « mauvais payeurs » et des « fraudeurs » au regard de la protection des données personnelles*, rapport adopté à la séance plénière du 27 mars 2003.

[64] V. *supra*, 1.1.2.

La seconde solution consisterait, comme le permet l'article 8 § 5 de la directive du 24 octobre 1995[65], sous réserve de l'édiction de « *garanties appropriées et spécifiques* », à ouvrir aux SPRD et aux personnes agissant pour le compte des titulaires de droits la possibilité de constituer des fichiers directement ou indirectement nominatifs concernant des personnes suspectées d'infractions. A cet égard, la commission se félicite de l'introduction, à l'occasion de l'examen par le Sénat du projet de loi de réforme de la loi du 6 janvier 1978, d'une disposition permettent le traitement de données à caractère personnel « *relatives aux infractions, condamnations et mesures de sûreté* » par « *les personnes morales victimes d'infractions, pour les stricts besoins de la lutte contre la fraude et dans les conditions prévues par la loi* ». Elle estime qu'une telle modification de l'état du droit, que la CNIL avait du reste elle-même appelée de ses vœux afin d'encadrer la pratique des listes noires[66] et dont elle a reconnu l'intérêt en vue de lutter contre la contrefaçon sur l'Internet, est propre à assurer un équilibre satisfaisant entre les droits de propriété littéraire et artistique et les libertés individuelles.

Pour que la faculté prévue par la disposition précitée puisse utilement être mise à profit par les SPRD et les ayants droit, plusieurs précisions devraient toutefois être apportées.

En premier lieu, la rédaction adoptée devrait permettre, sans ambiguïté, de regarder les violations des droits de propriété littéraire et artistique (c'est-à-dire la contrefaçon) comme incluses dans son champ d'application, la simple référence à la « fraude » n'étant pas exempte d'ambiguïté.

En deuxième lieu, comme cela a déjà été rappelé, les ayants droit laissent le plus souvent le soin à des organismes professionnels ou aux SPRD d'assurer pour leur compte la défense de leurs intérêts, notamment par le biais d'actions en justice. Il serait souhaitable que la faculté de procéder à des traitements relatifs à des infractions soit ouverte à ces organismes, alors même que, dans certains cas, ils ne pourraient être directement regardés comme « victimes » de telles infractions.

En troisième lieu, la commission estime que les garanties exigées par l'article 8 § 5 de la directive du 24 octobre 1995 pour la mise en œuvre de tels traitements devraient être prévues dans la loi du 6 janvier 1978 elle-même, sans renvoi à des interventions législatives ultérieures, l'adaptation sectorielle des règles générales ainsi fixées (avec une précision suffisante pour ne pas se heurter à des obstacles d'ordre constitutionnel) pouvant être efficacement opérée par la CNIL, dans le cadre des autorisations qu'elle serait amenée à délivrer. Ces garanties devraient porter notamment sur les délais de conservation des données collectées, sur la finalité précise des traitements autorisés, etc.

En quatrième lieu, enfin, il paraîtrait souhaitable de prévoir que les traitements autorisés puissent être effectués en vue de la prévention des infractions, notamment pour faire parvenir des messages d'avertissement aux auteurs de mises à disposition non autorisées d'œuvres numériques sur l'Internet.

---

[65] « *Le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national (…)* ».

[66] V. le rapport précité.

2.1.3 L'identification des auteurs d'infractions et le problème de la conservation des données de connexion

Les données permettant de constater les infractions réprimées par le code de la propriété intellectuelle recueillies et traitées par les services de police judiciaire ou les SPRD ne présentent évidemment un intérêt, du point de vue de l'efficacité de l'action répressive, que si elles permettent de remonter effectivement jusqu'aux auteurs de telles infractions. Or, comme on l'a vu, ces données ne sont, en général, qu'indirectement personnelles, et ne permettent de remonter (d'ailleurs pas systématiquement) jusqu'à l'identité réelle de l'utilisateur qu'associées à d'autres données. Ainsi, s'agissant de l'adresse IP, ce n'est que couplée aux données de connexion détenues par le fournisseur d'accès à l'Internet qui a attribué cette adresse qu'elle pourra acquérir un caractère directement personnel.

Or, aux fins notamment de garantir le secret des correspondances et celui du choix des programmes, il existe une séparation légale entre ces données de connexion et celles relatives aux contenus, qui seules peuvent permettre de caractériser les infractions réprimées par le code la propriété intellectuelle. En effet, le 2e alinéa du IV de l'article L. 32-3-1 du code des postes et télécommunications dispose que les données que, par exception, les opérateurs de télécommunications peuvent être autorisés à conserver « *ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre [des] communications* ». Des principes similaires inspirent les objectifs de la directive européenne du 12 juillet 2002 dite vie privée et communications électroniques[67], qui s'attache notamment à garantir la confidentialité des communications (article 5) – même si la notion de « *données relatives au trafic* » à laquelle elle a recours semble devoir être interprétée assez largement.

Cette séparation, qui constitue une garantie forte pour les utilisateurs, doit toutefois pouvoir être franchie pour assurer l'effectivité de la répression pénale des infractions commises par le biais de l'Internet – la question allant évidemment bien au-delà des infractions en matière de propriété littéraire et artistique. A cette fin, il est essentiel que les opérateurs de télécommunications soient astreints à conserver les données de connexion pendant une durée suffisante pour permettre aux victimes d'infractions d'obtenir la saisie de telles données, afin de pouvoir identifier les auteurs de ces infractions, notamment dans le cadre de la mise en oeuvre de l'article 60-1 du code de procédure pénale, qui permet la collecte d'informations relatives aux contenus consultés, sur réquisition du procureur de la République autorisée par le juge des libertés et de la détention.

C'est à cette fin qu'ont été prévues des dérogations au principe, affirmé tant par le I de l'article L. 32-3-1 du code des postes et télécommunications[68] que par le 1er paragraphe de l'article 6 de la directive du 12 juillet 2002[69], en vertu duquel les données relatives à une communication doivent être effacée ou rendues anonymes dès l'achèvement de celle-ci. Ainsi, l'article 15 de la directive du 12 juillet 2002 permet aux Etats membres d'adopter des mesures législatives visant notamment à limiter la portée de l'obligation d'effacement prévue au

[67] Directive 2002/58/CE du Parlement européen et du Conseil *concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques*, *J.O.C.E.*, L 201, 31 juillet 2002, p. 37.

[68] « *Les opérateurs de télécommunications (…) sont tenus d'effacer ou de rendre anonyme toute donnée relative à une communication dès que celle-ci est achevée (…)* ».

[69] « *Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes dès qu'elles ne sont plus nécessaires à la transmission d'une communication (…)* ».

1er paragraphe de l'article 6 « *lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'Etat – la défense et la sécurité publique, ou assurer la prévention, la rechercher, la détection et la poursuite d'infractions pénales ou d'utilisation non autorisées du système de communications électroniques (…). A cette fin, les Etats membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe* ». Cette faculté se concrétise, en droit national, dans le II de l'article L. 32-3-1 du code des postes et télécommunications, qui dispose : « *Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le IV, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs* ». Une obligation similaire de conservation des données permettant l'identification de créateurs de contenus sur l'Internet est, en outre, prévue par l'article 43-9 de la loi du 30 septembre 1986 relative à la liberté de communication.

Il convient de souligner que la conservation des données est entourée de garanties particulièrement fortes par le code des postes et télécommunications : ainsi que le précise le IV de l'article L. 32-3-1, ce traitement, dans la mesure où il porte sur des données nominatives, doit respecter les garanties prévues par la loi du 6 janvier 1978 ; l'obligation de sécurité qui pèse sur les opérateurs est rappelée par le dernier alinéa, qui leur impose de prendre « *toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article* » ; enfin, les données relatives aux communications ne peuvent être communiquées qu'aux fins de « *mise à disposition de l'autorité judiciaire* », et sur décision de celle-ci.

Eu égard à l'intérêt essentiel que représentent les données en cause pour l'efficacité de la répression de la contrefaçon, la commission considère qu'il est urgent que soient édictés les décrets en Conseil d'Etat pris après avis de la CNIL, dont tant l'article 43-9 de la loi du 30 septembre 1986 que l'article L. 32-3-1 du code des postes et télécommunications ont prévu l'intervention.

S'agissant de ces dernières dispositions, la commission estime que le délai de conservation des données de connexion ne devrait pas, dans l'état actuel de la législation, être inférieur à un an, ainsi que le permettent les dispositions du II de l'article L. 32-3-1. Un allongement, pour certaines catégories de données, du délai maximum fixé par la loi, dans des conditions compatibles avec les dispositions de l'article 6 § 1 de la directive du 12 juillet 2002, ne devrait par ailleurs pas être exclu à l'avenir, après évaluation des résultats des procédures judiciaires intentées par les ayants droit et des difficultés concrètes rencontrées à cette occasion, au regard notamment du délai de prescription de l'action pénale.

2.2 LES MOYENS JURIDIQUES ET TECHNIQUES DE PRÉVENTION DE LA CONTREFAÇON

Comme cela a déjà été évoqué, dans une situation caractérisée par l'explosion des échanges de fichiers contrefaisants, l'action répressive ne permet pas à elle seule de protéger efficacement les droits de propriété littéraire et artistique. Ses limites sont notamment mises en évidence par la difficulté de l'exécution des décisions de justice dans le contexte créé par l'Internet, comme l'a montré le conflit qui a opposé les juridictions françaises et américaines à propos de l'interdiction de mise en vente, sur le site d'enchères de Yahoo, d'objets à caractère nazi.

A cet égard, une conséquence importante des dispositifs préventifs est qu'ils atténuent les problèmes de conflit de lois. En effet, l'action préventive, qui vise par exemple à empêcher le téléchargement depuis la France de fichiers contrefaisants en provenance d'autres Etats, prend appui sur l'activité des prestataires techniques présents sur le territoire de réception (opérateurs de télécommunications et fournisseurs d'accès à l'Internet). Elle est donc fondée sur le droit de l'Etat de réception, ce qui évite les conflits de lois qui apparaissent lorsque l'on utilise l'instrument répressif.

Si une action préventive apparaît donc comme le contrepoint nécessaire de la répression, elle implique toutefois des garanties spécifiques, étant moins conforme à la tradition libérale des pays occidentaux, fondée sur la dialectique classique entre liberté individuelle et répression pénale.

2.2.1 Le cœur de l'action préventive : la mise en jeu de la responsabilité des prestataires intermédiaires

L'un des principaux enjeux de l'action préventive en matière de contrefaçon sur l'Internet consiste dans les modalités de mise en jeu de la responsabilité des « *prestataires intermédiaires* », définis par l'article 12 de la directive du 8 juin 2000 comme les prestataires qui ne sont pas à l'origine de l'information qu'ils transmettent ou stockent, ne sélectionnent pas les destinataires de cette information, et ne sélectionnent ni ne modifient cette dernière (fournisseurs d'accès à l'Internet, hébergeurs,…).

Il est important, en effet, pour les titulaires de droits de propriété littéraire et artistique, lorsqu'ils constatent par exemple qu'un site Internet met à disposition des fichiers sans autorisation, de pouvoir obtenir aisément de l'hébergeur qu'il cesse de diffuser le contenu de ce site, et, le cas échéant, du juge qu'il enjoigne au fournisseur d'accès de faire cesser le trouble constaté. L'action préventive résulte dans ce cas de la coopération rendue nécessaire par la menace d'engagement de la responsabilité des prestataires intéressés ; elle est prévue, mais aussi encadrée, par le droit communautaire.

(1) Le texte général en la matière est la directive du 8 juin 2000 sur le commerce électronique (chapitre II, section 4), qui définit en trois étapes les obligations incombant aux prestataires intermédiaires.

Dans un premier temps, elle affirme le principe de l'absence de responsabilité des prestataires intermédiaires à raison des contenus transmis (article 12) ou stockés (article 14), y compris sous la forme dite du « *caching* »[70] (article 13). Il ne peut, notamment, être imposé à ces intermédiaires « *une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites* » (article 15).

Dans un second temps, toutefois, elle précise les conditions auxquelles est subordonnée cette irresponsabilité de principe des intermédiaires – conditions qui révèlent évidemment, en creux, les conditions d'engagement de leur responsabilité. En particulier, s'agissant de l'hébergement, la responsabilité du prestataire intéressé n'est dégagée qu'à la condition qu'il « *n'ait pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information est apparente* » ou que, « *dès le moment où il a de telles connaissances, [il] agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible* » (article 14).

Dans un troisième temps, enfin, elle réserve la possibilité pour les juridictions ou les autorités administratives des Etats membres, « *d'exiger du prestataire qu'il mettre un terme à une violation ou qu'il prévienne une violation* » (articles 12, 13 et 14), « *d'instaurer des procédures régissant le retrait [des] informations [hébergées] ou les actions pour en rendre l'accès impossible* » (article 14), ou encore de mettre à la charge du prestataire « *l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement* » (article 15). L'article 18 de la directive invite en outre les Etats membres à veiller « *à ce que les recours juridictionnels disponibles dans le droit national portant sur les activités des services de la société de l'information permettent l'adoption de mesures, y compris par voie de référé, visant à mettre un terme à toute violation alléguée et à prévenir toute nouvelle atteinte aux intérêts concernés* ».

La transposition de ces objectifs, qui laisse une assez large marge de manœuvre aux Etats membres, est actuellement prévue par le projet de loi pour la confiance dans l'économie numérique, adopté en deuxième lecture par l'Assemblée nationale, avec de substantielles modifications par rapport au projet du Gouvernement, le 8 janvier 2004 (article 2 *bis*). L'adoption définitive de ce texte dans les meilleurs délais est, aux yeux de la commission, une condition essentielle au développement d'une action préventive efficace contre la contrefaçon dans l'environnement numérique.

Il importe, dans cette perspective, de garder présentes à l'esprit les exigences rappelées par le Conseil constitutionnel dans sa décision du 27 juillet 2000[71] : s'il est « *loisible au législateur, dans le cadre de la*

[70] Procédé permettant le stockage intermédiaire et temporaire des données sur le serveur du fournisseur d'accès.
[71] Décision n° 2000-433 DC, *Loi modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de*

concilitation qu'il lui appartient d'opérer entre la liberté de communication d'une part, la protection de la liberté d'autrui et la sauvegarde de l'ordre public d'autre part, d'instaurer, lorsque sont stockés des contenus illicites, un régime de responsabilité pénale des 'hébergeurs' distinct de celui applicable aux auteurs et aux éditeurs de messages », c'est à la condition de respecter le principe de légalité des délits et des peines. En l'espèce, le Conseil avait censuré le 3e alinéa de l'article 43-8 de la loi du 30 septembre 1986, faute pour le législateur d'avoir précisé les « *conditions de forme* » de la saisine des hébergeurs par un tiers estimant illicite le contenu hébergé, préalablement à l'engagement de leur responsabilité, et d'avoir déterminé les « *caractéristiques essentielles du comportement fautif* » de nature à engager une telle responsabilité.

En l'état actuel des travaux parlementaires, le texte du projet de loi pour la confiance dans l'économie numérique semble satisfaire aux exigences constitutionnelles, dans la mesure où il définit précisément les éléments constitutifs du comportement fautif du prestataire (connaissance effective de l'activité ou de l'information illicites et absence d'action prompte pour retirer ces informations ou en rendre l'accès impossible).

Il convient, en tout état de cause, de souligner que, plus les procédures prévues et les obligations des intervenants seront précisément définies, plus aisément pourra trouver à se concrétiser la logique de coopération en vue de la prévention des infractions qui sous-tend le mécanisme de responsabilité des intermédiaires.

(2) Par ailleurs, et plus spécifiquement, l'article 8 de la directive du 22 mai 2001 oblige les Etats membres à rendre leur législation plus efficace, en créant notamment des procédures permettant aux titulaires de droits de « *demander qu'une ordonnance sur requête soit rendue à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit d'auteur ou à un droit voisin* » (§ 3). Dans un tel cas, s'il ne défère pas l'injonction du juge, le prestataire engage sa responsabilité à l'égard des victimes des infractions.

La transposition de ces dispositions est efficacement opérée, dans le projet de loi pour la confiance dans l'économie numérique, par extension de la procédure de saisie-contrefaçon prévue à l'article L. 332-1 du code de la propriété intellectuelle à la situation de diffusion en ligne (en vertu de l'article 3 de ce projet, le président du tribunal de grande instance pourrait ainsi ordonner « *la suspension, par tout moyen, du contenu d'un service de communication publique en ligne portant atteinte à l'un des droits de l'auteur, y compris en ordonnant de cesser de stocker ce contenu ou, à défaut, de cesser d'en permettre l'accès* »). Cette procédure, qui a déjà fait ses preuves dans le contexte de l'économie numérique, offre des avantages de rapidité et d'efficacité, tout en assurant, par l'intervention d'un juge, la garantie des droits et libertés des différentes parties prenantes. La commission ne peut donc que souhaiter une adoption rapide de la disposition précitée.

2.2.2 Vers des systèmes de prévention des échanges illicites en *peer-to-peer* ?

Au cours de ses travaux, la commission a pris connaissance de certaines réflexions, auxquelles les représentants des producteurs et des artistes-interprètes ne sont pas associés, portant sur la possibilité de créer un système d'empreinte informatique qui permettrait, pour chaque fichier musical diffusé sur le réseau, de reconnaître l'œuvre encodée et de repérer si elle provient d'un site autorisé à la diffuser ou non. Ce système permettrait ainsi, hors de toute procédure judiciaire, de bloquer les fichiers lors de leur passage par le serveur d'un fournisseur d'accès ou par un routeur, et d'empêcher ainsi que ces fichiers parviennent jusqu'à leur destinataire, sans identification de ce dernier.

Un tel système, s'il devait effectivement être mis en œuvre dans de telles conditions, n'est pas sans se heurter à un certain nombre d'obstacles juridiques.

La mise à disposition illicite de fichiers sur l'Internet, notamment en *peer-to-peer*, ne bénéficie certes pas, ainsi qu'il a été dit[72], de la protection accordée aux correspondances privées. Ainsi, le blocage des échanges par des moyens techniques ne saurait être regardé comme une interception de correspondances, en raison du caractère ouvert au public de l'offre proposée. Toutefois, cette circonstance ne fait pas obstacle à l'application des règles relatives à la liberté de communication ; or l'interruption de communications, même non privées, constitue en elle-même une atteinte à cette liberté, protégée par la Constitution, par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et par la loi du 30 septembre 1986, qui pose notamment le principe du secret du choix des programmes.

---

communication, *Rec.*, p. 121.
[72] V. *supra*, 2.1.1.

Par ailleurs, le système envisagé comporte un risque d'atteinte aux droits et exceptions reconnus par la loi en faveur des utilisateurs des œuvres. Un certain nombre de questions se poseraient à cet égard : comment assurer que le système ne filtre pas également les œuvres du domaine public ? Comment ce système pourrait-il prendre en compte les différences entre les régimes d'autorisation des différents pays ? Il reviendrait dans ce schéma aux mesures techniques de protection des œuvres de permettre le respect des exceptions permises par les différents droits nationaux.

Ce système ne pourrait donc être mis en place qu'après la définition d'un cadre juridique approprié, conforme notamment au principe constitutionnel de protection de la vie privée et aux stipulations de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Cet encadrement devrait idéalement être élaboré au niveau européen, compte tenu de la nature du problème, mais tant la directive du 8 juin 2000 sur le commerce électronique (article 3 § 3) que celle du 12 juillet 2002 sur les communications électroniques (article 15 § 1) autorisent les Etats membres à prendre des mesures nationales portant atteinte au fonctionnement du marché intérieur ou à la liberté de communication en vue de prévenir les atteintes aux droits de propriété littéraire et artistique.

L'encadrement juridique ici envisagé devrait, en tout état de cause, assurer que les atteintes à la liberté de communication impliquées par le système de filtrage des fichiers sont strictement nécessaires et proportionnées au but recherché. Deux séries de dispositions devraient y figurer à cette fin : une définition très précise des cas dans lesquels il est permis de stopper un fichier par des moyens techniques appropriés, d'une part, et l'interdiction de repérer à cette occasion l'identité du destinataire du message, d'autre part.

Une fois ce cadre juridique mis en place, la définition des normes techniques applicables et des intermédiaires sur lesquels reposerait l'obligation de filtrage pourrait, soit être effectuée par l'Etat ou la Commission européenne, soit être renvoyée à des accords techniques entre SPRD et intermédiaires concernés, ces accords étant soumis à l'accord de l'autorité administrative compétente.

♦ ♦ ♦