DROIT & NOUVELLES TECHNOLOGIES

Présente :

DROIT D'AUTEUR ET NUMERIQUE : QUELLE REFORME ?

Les Systèmes numériques de gestion des droits
(« Digital Rights Management Systems »)

Par

Patrick Boiron
Avocat à la Cour
Cabinet Paul Hastings
patrickboiron@paulhastings.com

Colloque organisé par le CEJEM
Centre d'Etudes Juridiques et Economiques du Multimédia
Université Panthéon-Assas (Paris II)

Date de mise en ligne : 29 juillet 2004

Colloque organisé par le CEJEM

Centre d'Etudes Juridiques et Economiques du Multimédia

Université Panthéon-Assas (Paris II)

DROIT D'AUTEUR ET NUMERIQUE : QUELLE REFORME ?

Les Systèmes numériques de gestion des droits

(« Digital Rights Management Systems »)

Paris, 12 février 2004

Patrick Boiron
Avocat à la Cour

« LA GESTION NUMERIQUE DES DROITS »

> « *The machine is the answer to the machine… A system must be able to identify copyright materials, to track usage, to verify users, and to record usage and appropriate compensation. In addition, the system should provide security for the integrity of the copyrighted material (freedom from tampering) and some level of confidentiality or privacy for the user* ».
>
> Charles Clark, The Publisher in the Electronic World.

Les technologies numériques ont transformé l'environnement du droit de la propriété littéraire et artistique et ouvrent la possibilité d'un énorme marché pour la diffusion des contenus.

L'arrivée sur le marché des réseaux à large bande passante et la capacité de ceux-ci à transmettre des valeurs considérables d'informations protégées par le droit d'auteur de manière quasi instantanée ou à très haute vitesse rend impérative la nécessité de s'assurer que ces informations numériques sont mises à disposition de l'utilisateur dans des conditions autorisées et sécurisées.

Les techniques numériques génèrent des risques importants pour les titulaires de droits. Si la numérisation démultiplie les modes d'exploitation d'une œuvre, elle génère en contrepartie des possibilités de manipulation, de piratage qui ne sont pas simplement théoriques.

Le secteur de la musique paye actuellement un lourd tribut au monde numérique, et surtout celui des réseaux ; la copie numérique est facile à réaliser et sa qualité est identique à l'original, quelque que soit le nombre de copies réalisées.

Dans un tel monde, que vaut la seule protection juridique par le droit d'auteur et des droits voisins ?

Dans le même temps, l'environnement numérique rendait possible la création de dispositifs techniques de protection des droits des auteurs et autres titulaires de droits de propriété littéraire et artistique (contrôle de l'accès aux œuvres, des copies réalisées, information sur les droits, etc…). Mais ces dispositifs, que les techniques numériques avaient permis de créer, se voyaient contournées, en utilisant ces mêmes techniques.

La défense des ayants-droit exigeait que la protection technique des œuvres soit complétée par une protection juridique et des sanctions contre la neutralisation des mesures techniques mises en œuvre par les auteurs (ou les artistes-interprètes) et contre l'atteinte aux informations sur le régime des droits.

Ce sont les traités OMPI (WCT et WPPT) du 20 décembre 1996 qui ont introduit dans l'ordre juridique international ces logiques de protection juridique de dispositifs techniques ; plus précisément, les articles 11 et 12 du Traité relatif aux droits d'auteur et 18 et 19 du Traité relatif aux droits visés dans le domaine musical (« interprétation et phonogrammes »). Apparaissent ainsi des obligations de la part des Etats liés par le Traité de protéger les « effective technological measures » (mesures technologies efficaces) et les « rights management information » (information sur le régime des droits).

La Directive européenne du 22 mai 2001 sur le droit d'auteur et les droits voisins dans la société de l'information reprend dans ses articles 6 et 7, ainsi que dans ses considérants 47 à 58, des dispositions inspirées des Traités OMPI de 1996 et traitent des dispositifs techniques de protection et des différentes mesures juridiques qui y ont trait.

L'adoption de ces traités a ainsi consacré une construction à trois niveaux :

- la protection juridique qu'offrent les droits de propriété intellectuelle (monopole de l'auteur, se traduisant par le droit exclusif d'autoriser ou d'interdire l'exploitation de son œuvre, et créant à son profit des droits patrimoniaux et moraux, etc…) ;

- la protection technique, consistant en des mesures techniques et des informations sur le régime des droits, qu'apportent les dispositifs de contrôle d'accès, de copie, d'identification ou d'authentification, etc… ;

- la protection juridique qui sanctionne les actes de contournement ou de neutralisation des mesures de protection technique ou d'information sur le régime des droits.

Pour le dire autrement, l'environnement du droit d'auteur comprend :

- les droits proprement dit, protégés par le droit de la propriété intellectuelle et les exceptions à ces droits (par exemple l'exception au droit de reproduction qu'est la copie privée) ;

- les mesures d'application de ces droits (sanction pour les copies illicites ou pour le commerce de dispositifs de contournement des mesures de protection, par exemple) ;

- la gestion des droits ou leur exploitation.

Le concept de « Digital Rights Management Systems » (DRMS) ou Sytèmes Numériques de Gestion des Droits prend appui sur ces protections juridiques nouvelles, sans toutefois s'y résoudre.

I – LES « DIGITAL RIGHTS MANAGEMENT SYSTEMS » (DRMS) : UNE TECHNOLOGIE, RIEN QU'UNE TECHNOLOGIE

1.1 Essai de définition

Il existe plusieurs définitions des DRMS, selon la sphère à laquelle appartient celui qui la donne, ou selon que l'accent est mis sur les fonctionnalités ou la finalité.

Pour faire simple, on retiendra néanmoins la définition suivante : les systèmes numériques de gestion des droits (DRMS) sont des technologies qui permettent (i) d'identifier et de décrire des contenus numériques protégés par des droits de propriété intellectuelle et d'en définir les règles d'exploitation, et (ii) de garantir les règles d'exploitation de ces contenus numériques, telles qu'elles sont définies par les ayants-droit ou prescrites par la loi.

Dans l'Union Européenne, le cadre juridique dans lequel s'inscrivent ces DRMS est la Directive 2001/29/EC du 22 mai 2001 sur l'harmonisation de certains droits d'auteurs et droits voisins dans la société de l'information (Directive qui aurait dû être transposée au plus tard fin décembre 2002).

Le développement des DRMS est une condition indispensable et préalable à l'expansion sur les réseaux tels qu'Internet des contenus protégés par les droits de propriété intellectuelle. Ils visent à instaurer un « espace de confiance » depuis la numérisation du contenu jusqu'à la dernière exploitation de l'œuvre. Espace de confiance veut dire que du début jusqu'à la fin, la chaîne des transactions qui affectent un contenu protégé est sécurisée. La frilosité de la mise en ligne de contenus audio ou vidéo tient notamment à ce que les DRMS ne permettent pas d'assurer efficacement cet espace de confiance entre les titulaires de droits, les distributeurs et les utilisateurs. Cette condition est nécessaire et suffisante. La réalisation d'un espace de confiance continu et interopérable conduira, avec certitude, à une explosion de la diffusion des œuvres de l'esprit sur les réseaux.

1.2 Essai de description

Revenant sur les sphères concernées, il est permis de distinguer :

- la sphère des ayants-droit, titulaires de droits d'auteurs ou de droits voisins ;

- la sphère des distributeurs qui vont (1) appliquer à l'œuvre numérisée, les mesures techniques de protection permettant une circulation de celle-ci sauvegardant son intégrité, permettant un contrôle de son accès et de sa copie, évitant son piratage ou le détournement de sa finalité, (2) intégrer les informations sur le régime des droits et s'assurer que celles-ci ne sont pas éliminées, ou modifiées pendant tout le parcours de distribution de l'œuvre, (3) assurer les flux entre les auteurs et les utilisateurs portant sur les requêtes de droits et les contrats et les contreparties financières ;

- la sphère des utilisateurs qui vont acquérir soit des supports physiques des œuvres (supports optiques), soit des licences d'utilisation.

Si maintenant on suit les différentes fonctions d'un DRMS, on peut distinguer trois phases ou fonctions :

- la gestion numérique des droits, qui comprend :

    * l'identification des contenus auxquels les droits sont attachés,
    * la description des droits,
    * le chiffrement des contenus

- la mise à disposition des droits, qui comprend :

    * la distribution,
    * la reconnaissance des contenus et la requête des droits,

et qui suppose :

* une identification et une authentification de l'utilisateur,
* l'autorisation d'exploitation

- l'exploitation des droits, c'est-à-dire :

* le contrôle de l'accès aux œuvres,
* le contrôle de la copie.

Si, maintenant, nous reprenons ces points, nous constatons que le préalable à la mise en œuvre d'un DRMS complet et efficace est que les différents titulaires de droits, auteurs ou titulaires de droits voisins, essentiellement artistes-interprètes et producteurs aient « harmonisé » les données relatives à l'information sur les droits qui constituent le « régime des droits », objet d'une protection juridique appropriée selon l'article 7 de la Directive du 22 mai 2001. La mise en place d'une guichet commun ou à tout le moins d'une plate-forme d'information et d'orientation commune à l'ensemble des SPRD, assurant par l'interconnection de leurs bases de données, l'identification en une seule consultation des œuvres, des titulaires de droits, de la nature des droits, bref des informations sur le régime des droits serait à même d'orienter l'utilisateur vers les titulaires de droits afin qu'il puisse procéder à l'acquisition des droits en ligne.

1.2.1 LA GESTION NUMÉRIQUE DES DROITS

S'agissant de l'identification, celle-ci doit permettre la reconnaissance du contenu d'une œuvre, sans ambiguïté ; la règle étant qu'il ne doit y avoir qu'un seul identifiant pour un contenu donné (cf. l'ISBN pour les ouvrages littéraires, ISWC, ISAN, etc…).

Une fois que les contenus ont été identifiés, les droits doivent être décrits. Cette phase est essentielle car elle permet d'intégrer les informations concernant le régime des droits : auteur, date de

publication, pays d'origine, etc…, sous forme de métadonnées, mais elle permet aussi de décrire les licences qui seront consenties et leurs limites ; ainsi, le titulaire de droits pourra-t-il autoriser l'impression d'un texte, mais pas sa copie (Mibrary.com) ou encore autoriser une copie privée une fois ; la copie étant stérile, ou N fois les copies de copies étant stériles (Windows Media Rights Manager de Microsoft) ; ou encore réaliser une copie privée ou autant qu'il le souhaite sur un réseau privé personnel, copie qui ne sera pas lisible par un autre utilisateur, en dehors de ce réseau.

Les langages de description de droits permettent ainsi de communiquer à un serveur de droits (société de gestion collective ou ayant-droit individuel ou encore société de gestion de DRMS) les licences que l'ayant-droit autorise quant à l'utilisation de son œuvre sur le réseau (à signaler un langage particulièrement performant, le XrML extensible rights Markup Language, ex : DPRL (Digital Property Rights Language)).

Le langage permet de décrire et fixer les conditions du « contrat » qui sera passé entre le titulaire des droits de l'utilisateur, mais n'a pas pour fonction de détecter et encore moins de s'opposer à un utilisateur qui ne veut pas respecter le contrat. Il convient donc de protéger le contenu et la description des droits par des « mesures techniques » au sens de l'article 6 de la Directive précitée.

Cette protection s'opère par un chiffrement du contenu, en ayant recours à la cryptologie.

1.2.2 LA MISE À DISPOSITIONS DES DROITS

L'œuvre ainsi « packagée » est prête à être distribuée sur le réseau : le serveur de droits, habilité par les ayants-droit à consentir l'autorisation d'exploiter, en contrepartie d'une rémunération de l'utilisateur, peut confronter le régime des droits (description) avec l'autorisation qui lui a été confiée par l'ayant-droit ; l'œuvre chiffrée peut être transmise via le réseau à un utilisateur.

Il convient de noter à ce stade que la transmission de l'œuvre s'effectue toujours séparément de l'information sur le régime des droits (description). L'œuvre est transmise sous une forme inexploitable

(chiffrée) et la clé de déchiffrement est transmise en même temps, mais séparément, que la représentation des droits.

Le serveur de droits reçoit des titulaires de droits, l'ensemble des licences définies, avec un langage de description des droits, de façon générique pour chaque œuvre ; il reçoit de la part des utilisateurs des requêtes de concessions éventuellement accompagnées d'un paiement. Il émet en sortie, vers les titulaires de droits, le nombre de requêtes pour chaque œuvre et le total des sommes perçues et, vers les utilisateurs, les concessions de licences.

C'est la fonction d'échange de droits et de données.

Notons qu'à ce niveau, le risque peut exister que la protection des données personnelles (articulation Privacy Right Management Systems et DRMS) ne soit pas assurée. En effet, dans le cas d'un usage de DRMS par un distributeur opérant comme intermédiaire entre titulaires de droits et diffuseur de contenus, l'opérateur de DRMS/distributeur a accès au nom ou pseudo de l'utilisateur, à son adresse e-mail pour la formation du contrat et le numéro de carte bancaire pour les opérations financières : le distributeur doit alors opérer comme tiers de confiance ou il convient d'avoir recours à une autorité tierce, neutre et indépendante (cf. critiques sur Palladium (Microsoft) et TCPA Trusted Computing Platform Alliance (cherche à doter les PC de fonctionnalités de sécurité – centralisation de données nominatives)).

a) *La distribution*

En matière de distribution, la diffusion sur les réseaux fermés (bouquet de chaînes satellitaires, films à la demande), qui concerne essentiellement des œuvres audiovisuelles, jouit d'une sécurité plutôt « robuste » (cf. système européen de chiffrement DVB, par exemple). Sur les réseaux ouverts comme Internet, la sécurisation est moins forte car elle est obtenue à partir de logiciels plus facilement «craquables» que les cartes à puce (signature Windows Media Rights Manager de Microsoft ou Medialine).

Il convient de remarquer que l'essentiel du piratage en matière audio provient du fait que le CD, contrairement au DVD, ne contient pas de protection active. Les standards sécurisés comme le Super Audio Compact Disc (SACD) ou le DVD audio peinent à se développer.

b) *La reconnaissance des contenus de la requête*

Mais, ainsi qu'on l'a vu plus haut, l'œuvre ainsi distribuée à l'utilisateur est inexploitable si celui-ci n'a pas acquis, auprès du serveur de droits, les droits nécessaires. C'est le processus de requête et d'octroi de concession de licences qui a été décrit ci-dessus.

Dans cette requête, l'identification et l'authentification de l'utilisateur sont des éléments essentiels, au même titre, naturellement, que l'identifiant de l'œuvre ou la nature des droits demandés.

Une remarque à ce stade : dans le cas d'un authentifiant logiciel, le pirate va opérer un « reverse engineering », facilité par des outils de debuggage et de décompilation qu'on peut trouver sur Internet. Ici, il me semble que des mesures techniques d'accès aux œuvres garanties par l'article 6 de la Directive du 22 mai 2001, laissent intacte la possibilité à « l'utilisateur du logiciel » de procéder à une décompilation à des fins d'interopérabilité, prévue expressément par l'article L. 122-6-1-IV du Code de la Propriété Intellectuelle.

c) *Le chiffrement de la mise à disposition des droits*

Puis l'œuvre est mise à disposition sous forme chiffrée (slide)

1.2.3 L'EXPLOITATION DES DROITS

Enfin, pour terminer cette revue des fonctions des DRMS, intéressons-nous à l'exploitation des droits, entendue comme étant le contrôle de l'accès aux œuvres et le contrôle de la copie.

a) *Le contrôle de l'accès*

Pour accéder à l'œuvre, dès lors que la représentation des droits est acquise, il convient de la déchiffrer, opération qui se fait via un décodeur, soit matériel, soit logiciel selon la logique inverse qui a présidée aux opérations de chiffrement.

Là encore, notons que la sécurité est plus grande lorsqu'il s'agit d'un décodeur matériel (carte à puce ou circuit intégré) que lorsqu'il s'agit d'un logiciel.

b) *Le contrôle de la copie*

Le contrôle de la copie numérique de l'œuvre peut se faire par le décodeur, logiciel ou matériel. Lorsque l'utilisateur désire copier une œuvre, le décodeur vérifie que l'utilisateur possède les droits de copie sur cette œuvre.

S'il n'a pas les droits au moment où il souhaite avoir accès à l'oeuvre, l'utilisateur, si le décodeur peut être connecté à un serveur de droits (décodeur logiciel sur un ordinateur connecté à Internet par exemple), peut les acquérir auprès de ce serveur en offrant une rémunération, sauf si le régime des droits propres à cette œuvre ne permet pas à l'utilisateur, soit d'effectuer une seule copie de l'œuvre, soit d'en effectuer le nombre qu'il désire.

Le principe de la protection contre la copie illicite est de ne diffuser des œuvres qui ne sont compatibles qu'avec des décodeurs qui interdisent la copie ou bien ne l'autorisent que sous certaines conditions. Le développement des « réseaux privés personnels », constitués pour un utilisateur ou un foyer déterminé, d'un ensemble d'appareils connectés entre eux et interopérables (ordinateur, téléviseur, décodeur, lecteur de DVD, etc…) conduit à se poser la question de la protection contre le risque de voir se développer des piratages à l'occasion du transfert des œuvres d'un appareil à un autre ou encore de voir proliférer les réseaux P2P. Il faut donc que le système de contrôle de la copie permette le transfert des œuvres entre équipements d'un même utilisateur et interdise un tel transfert

entre équipements d'autres utilisateurs. Au sein d'un réseau privé personnel, il convient que les informations qui sont transmises d'un équipement à un autre soient chiffrées (cf. système Smart Right dit de « protection de bout en bout »).

Dans un tel système, si la copie privée est interdite, l'enregistrement est toujours physiquement possible, mais les copies obtenues sont illisibles, même au sein d'un réseau privé personnel.

Reste le problème du contrôle de ce que l'utilisateur fait des copies numériques qu'il a pu réaliser, ce qui représente un enjeu considérable pour les ayants-droit, notamment, mais aussi pour les utilisateurs. Cette question trouve sa réponse, d'une part, dans la représentation des droits que le décodeur matériel ou logiciel a reçus du serveur de droits et qui peut être stockée : y-a-t-il possibilité ou non de réaliser des copies numériques à partir d'une copie numérique, d'autre part, dans la traçabilité de la copie grâce au « suivi » de la copie d'une œuvre que permettent les techniques de « tatouage », watermarking ou fingerprinting. Il restera néanmoins toujours la possibilité de réaliser une copie, à partir de la représentation analogique, en bout de chaîne, seule représentation que l'être humain peut appréhender avec ses sens. Mais la re-munérisation d'un signal analogique donne des résultats dégradés (même si sa nouvelle reproduction est identique en qualité, logique du clone) qu'on ne peut que douter de l'intérêt réel que représente une telle copie. Ne pas oublier, non plus, que le watermarking permet de savoir quel utilisateur s'est livré à cette opération !

II - LES « DIGITAL RIGHTS MANAGEMENT SYSTEMS » (DRMS) : UNE TECHNOLOGIE, RIEN QU'UNE TECHNOLOGIE, QUI S'INSCRIT DANS LE DROIT ET L'INFLUENCE

2.1 L'inscription dans le droit

2.1.1 LA « PROTECTION JURIDIQUE APPROPRIÉE »

Comme cela a été indiqué au début de cet exposé, les DRMS s'inscrivent dans le cadre des articles 6 et 7 de la Directive 2001/29.

On sait que ces articles font obligation aux Etats membres de l'EU d'assurer la protection juridique des dispositifs techniques. Il est néanmoins permis de s'interroger sur la surprotection que ces mécanismes engendrent et sur la difficulté des DRMS à appréhender toutes les situations.

Que restera-t-il de la « balance des intérêts » si, par exemple, l'accès n'est pas libre à une œuvre tombée dans le domaine public ou si n'est pas, en pratique, garanti l'exercice des exceptions légalement prévues ?

La construction en trois stades de la protection tend à consacrer une espèce de droit nouveau : « le droit « d'accès » qui serait en quelque sorte la prérogative éminente en matière de droit d'auteur et qui conditionnerait l'exercice des autres droits, conduisant ainsi, notamment, soit à un double paiement lorsqu'un utilisateur ayant payé une première fois pour l'accès à l'œuvre ne pourra en conserver un exemplaire si cette mise à disposition est conditionnée par l'existence d'un dispositif anti-copie ; soit à un verrouillage de l'œuvre, combiné avec la prohibition du contournement, empêchant ainsi l'accomplissement par l'utilisateur d'actes pourtant légalement admis (exceptions au droit exclusif, par exemple).

Une distinction doit être faite entre les dispositifs qui restreignent mais ne suppriment pas la faculté de reproduction, et ceux qui rendent impossible la reproduction d'une œuvre ou qui permettent un contrôle de l'accès.

Les dispositifs qui rendent impossibles la copie doivent s'apprécier dans le monde numérique. Le « trou analogique » permet toujours la copie, certes de moins bonne qualité, mais c'est une copie !

S'agissant de la législation sur les moyens de contournement, la mise à disposition de tels moyens sera licite dans certains pays (exceptions inexistantes et donc exemptions inutiles) et illicites dans d'autres (exceptions inexistantes et donc exemptions inutiles), d'où la question : comment empêcher la circulation de matériel d'un pays à l'autre ?

La solution du médiateur pour régler les différends entre titulaires de droits et utilisateurs au cas où ceux-ci estimeraient qu'une mesure technique de protection les empêche de bénéficier de l'exception de copie privée peut déboucher sur une injonction prescrivant des « mesures appropriées ».

2.1.2 DES OUTILS JURIDIQUES NÉCESSAIRES

a) *La libéralisation de la cryptologie* est désormais effective. La rigueur du régime adopté par la France, qui faisait figure d'exception parmi les Etats démocratiques, avait été assouplie progressivement depuis 1990. Mais désormais l'article 1.8 du projet de loi pour la confiance dans l'économie numérique, qui transpose notamment la Directive « Commerce Electronique » du 8 juin 2000, dispose : « l'utilisation des moyens de cryptologie est libre », même si certaines exceptions sont prévues.

b) *La signature électronique* a été consacrée par la loi du 13 mars 2000 qui a modifié les articles 1316 et suivants du Code Civil, puis devrait être étendue pour satisfaire à l'impératif de transposition de la Directive Commerce Electronique précitée par la loi pour la confiance dans l'économie numérique. Sous réserve de la mise en place effective du mécanisme de certification, et des tiers de certification, cet outil devrait grandement faciliter, une fois la loi votée et les textes d'application publiés, le commerce électronique dans un environnement sécurisé.

2.2 Les conséquences sur le droit

2.2.1 LA PROTECTION DES DONNEES PERSONNELLES

La protection des données personnelles et de la vie privée peut être mise en jeu à l'occasion de la communication d'informations personnelles, notamment au niveau du serveur de droits.

Certains projets comme Palladium de Microsoft qui tendent à implanter sur le disque dur de l'ordinateur personnel des éléments de sécurisation, mais qui peuvent également donner accès à des données personnelles dont le traitement informatisé est protégé par la loi paraissent inquiétants. Il faut

rappeler avec force, comme le fait le considérant 57 de la Directive 2001/29, que les DRMS ou tout système équivalent doivent respecter les dispositions de la loi du 8 janvier 1978 « Informatique et Liberté » et de la Directive 95/46 du 24 octobre 1995 relatives à la protection de la vie privée et des personnes physiques à l'égard du traitement et de la circulation des données personnelles.

2.2.2 LE DEVENIR DE LA COPIE PRIVEE NUMERIQUE

Certains pensent que la capacité des DRMS à devenir une solution alternative à l'application de la redevance pour copie privée décidera du succès des DRMS. Ainsi, dans de nombreux Etats, la liberté de copie privée reposait sur l'impossibilité pratique et juridique de vérifier ce que les utilisateurs faisaient chez eux, dans le secret de leur domicile privé, et sur l'idée que la perte économique était négligeable, le copiste reproduisant difficilement l'œuvre protégée. Ces deux raisons ont aujourd'hui disparu. Les dispositifs techniques permettent de limiter la faculté de copie au domicile et la numérisation (sans verrous) permet la confection facile de « clones » qui bouleversent l'économie des œuvres. Pourquoi encore admettre des solutions, qui n'étaient que des pis aller ? Si le droit et la technique donnent désormais les moyens de parvenir à d'autres solutions au nom de quoi faudrait-il maintenir les anciennes constructions ? En quoi la tolérance d'hier a-t-elle conféré un droit à l'exception aujourd'hui ?

Est-ce la gestion des redevances pour les copies privées, soit de manière collective sur la base des schémas actuels forfaitaires, ou individuellement grâce aux DRMS qui décidera du succès ou de l'échec des DRMS ?

Sur ce point, l'attitude des différentes parties prenantes est directement dictée par leurs intérêts économiques. On peut distinguer :

- les équipementiers, qui plaident en faveur du « phasing out » et du remplacement des mécanismes de copie privée par les DRMS ;

- les « majors » du disque, qui plaident également pour les DRMS ;

- les « petits » titulaires de droits, les SPRD et les groupes particuliers d'utilisateurs, qui demeurent sceptiques quant à la généralisation de DRMS. Pour eux, les DRMS manquent de sécurité et d'interopérabilité. Ils seront entre les mains des « majors » uniquement, qui ne répartiront pas équitablement les droits comme les SPRD le font actuellement. Quant aux exceptions légales pour copie privée, assorties d'une rémunération en contrepartie de l'abandon du droit exclusif, elles sauvegardent davantage les droits des consommateurs que des droits exclusifs gérés grâce au DRMS.

Conformément à la Directive du 22 mai 2001, il est prévu une « compensation équitable » pour trois exceptions au droit de reproduction listée dans la Directive et, en particulier, l'exception pour copie privée (article 5 (2) (b)).

Le terme « compensation équitable » vise la réparation d'un dommage, une indemnisation (considérant 35), et n'est pas identique au concept de « rémunération équitable », ce qui donne une grande souplesse aux Etats Membres qui peuvent décider de ne pas introduire de rémunération pour copie privée.

S'agissant de la copie privée numérique, le considérant 38 indique que la confection de ces copies est susceptible d'être plus répandue et d'avoir une incidence économique plus grande et qu'il y a lieu de faire une distinction entre copies privées numériques et analogiques.

Dans le même temps, l'article 6 prévoit un cadre qui protège l'utilisation des mesures techniques, tels que les dispositifs de contrôle de copie et les DRMS, qui peuvent également être conçus pour permettre, et pour gérer, la copie dans la sphère privée et assurer une rémunération directe dans l'environnement numérique. C'est le considérant 39 qui met en parallèle la copie privée numérique et les redevances y afférents. Ce cadre juridique vise à assurer que les schémas de rémunération et de

« compensation équitable » prennent en compte l'utilisation de ces mesures techniques. Mais ceci n'oblige pas un Etat Membre à supprimer la rémunération pour copie privée une fois que les titulaires de droits sont techniquement à même de protéger et d'obtenir le paiement sur la base d'une licence. En fait, la Directive ne prend pas partie pour ou contre les systèmes de rémunération par rapport aux DRMS.

CONCLUSION

Les DRMS ne sont ni largement développés, ni largement acceptés. Un certain nombre de questions doivent être réglées avant que les DRMS ne soient reconnus comme la solution de gestion et de protection des droits numériques.

A. A ce jour, la technologie n'est pas assez robuste. On l'a vu avec les défis lancés par CSS ou SDMI où dans les deux cas des étudiants d'universités américaines ont réussi à « cracker » ces technologies. Puisqu'aucun système ne peut prétendre être à 100 % inviolable, la technologie doit être rapidement évolutive et renouvelable, afin d'être en avance (ou très légèrement en retard) par rapport aux pirates. Une telle nécessité disqualifie l'électronique grand public, au profit des appareils à carte à puce ou, encore mieux, des solutions logicielles.

B. Les utilisateurs craignent que les DRMS ne leur imposent des contraintes et limitent leur faculté d'accès ou de copie des œuvres. Si demain les DRMS organisent l'accès et la copie des livres « numériques », il est clair que les anciennes habitudes de relire un livre autant de fois qu'on le souhaite, de le prêter à ses amis ou à sa famille, seront mises à mal. Mais la comparaison s'applique-t-elle au livre ? Et n'y-a-t-il pas de bonnes raisons de protéger les droits des ayants-droit, des fournisseurs de contenus et des distributeurs de données numériques ? Plus important et préoccupant : on voit bien en quoi les DRMS protègent les ayants-droit et autres titulaires de droits contre l'utilisation illicite de leurs œuvres ; on voit moins ce qu'apportent les DRMS à la protection de l'utilisateur honnête. Il est impératif que les DRMS démontrent que les solutions que ces systèmes proposent ne restreignent en aucune façon l'usage licite des œuvres.

C. Ainsi que cela a été indiqué, l'objet fondamental des DRMS est de protéger les droits économiques et de propriété intellectuelle des ayants-droit, dans le respect de la loi. Mais les DRMS, afin d'assurer cette fonction essentielle de protection des œuvres, collectent et

traitent des données personnelles d'une part et suivent de près, on pourrait dire « pistent », l'utilisation qui est faite par chaque utilisateur du contenu numérique protégé auquel il a eu accès.

De plus, la tentation peut être grande de constituer des fichiers d'utilisateurs, et de créer ainsi des « profils » de consommateurs à valeur économique certaine, en fonction des œuvres qu'ils « consomment ». (On remarquera simplement que les cookies remplissent déjà cet office.) Aussi, est-il nécessaire de rappeler, comme le fait le considérant 57 de la Directive du 22 mai 2001, que les DRMS doivent prendre en compte les règles posées par la Directive 95/46/EC relatives à la protection des données personnelles. En particulier, chaque personne doit être informée de l'objet du traitement des données, de l'identité du contrôleur, et de tous autres éléments lui permettant de s'assurer que les données personnelles sont traitées dans le respect des dispositions de ladite Directive.

De même, aucune donnée personnelle recueillie dans le cadre des DRMS ne devrait être utilisée à des fins de marketing ou autre, sans l'accord express des personnes concernées.

D. Des mesures techniques comme les DRMS peuvent déboucher sur des solutions techniques lourdes et complexes que les utilisateurs refusent. Etre confronté avec de nombreux systèmes et logiciels, incompatibles mais qui doivent tous être téléchargés ou activés avant d'avoir accès à l'œuvre n'est pas acceptable pour l'usager. Il est impératif, pour le développement des DRMS, que les systèmes soient standardisés, donc interopérables, souples et ouverts.

E. Les DRMS devraient être suffisamment ouverts et souples pour permettre aux titulaires de doits, dans le respect des dispositions légales, de décider des règles qu'ils veulent appliquer à l'utilisation de leurs œuvres. Idéalement, pourquoi ne pas créer un environnement qui permettrait aux créateurs de choisir s'ils veulent protéger leurs droits et recevoir une rémunération ou non.

F. La non-maturité, l'absence d'efficacité suffisante prouvée et la faible disponibilité commerciale des mesures de protection techniques ne permettent pas une évolution résolue vers le « phasing out » de la rémunération forfaitaire pour copie privée ! Au contraire, a été récemment étendue aux disques durs intégrés à un téléviseur, magnétoscope, décodeur, baladeur ou autre appareil hi-fi (décision n°3 du 4 juillet 2002, art. 1er) et aux disquettes 3 pouces et demi (décision n° 4 du 10 juin 2003) la rémunération pour copie privée prévue à l'article L. 311-1 du Code de la Propriété Intellectuelle.

La mise en œuvre des DRMS peut conduire à un double paiement par l'utilisateur de l'œuvre, d'une part comme condition d'un droit à copie, d'autre part, sous forme de rémunération pour copie privée intégrée dans le prix de son décodeur, par exemple.

Au-delà de la problématique du double paiement se trouve posé la justification de la rémunération forfaitaire pour copie privée. L'efficacité et la fiabilité des DRMS doivent conduire l'ayant-droit à percevoir une rémunération proportionnelle sur chaque copie numérique de l'œuvre, permettant ainsi de se réinscrire dans la logique du droit exclusif dont la copie privée n'est qu'une exception (cf. article L. 122-5 du Code de la Propriété Intellectuelle). Ainsi, la généralisation des DRMS et de la mise en place des « mesures techniques efficaces » prévus à l'article 6.1 de la Directive du 22 mai 2001 devraient-elles conduire à la suppression progressive de la redevance pour copie privée numérique (« phasing out »).