

**COMMISSION DE L'ARTICLE L. 311-5 DU CODE DE LA PROPRIETE
INTELLECTUELLE**

**COMPTE RENDU DE LA REUNION DU 16 OCTOBRE 2003 ETABLI EN APPLICATION
DE L'ARTICLE 12 DU REGLEMENT INTERIEUR**

Version corrigée - Validée

1) Membres présents et quorum.

Le président constate que le quorum est atteint et ouvre la séance.

2) Examen et adoption du compte-rendu de la séance du 4 juillet 2003 et du relevé de discussion de la séance du 16 septembre 2003.

Le compte-rendu et le relevé de discussion des séances sus-visées ont, après avoir fait l'objet de corrections, été approuvés par les membres de la commission. Le secrétariat procédera aux corrections et enverra ces documents corrigés par courrier aux membres de la commission.

3) Audition de M.Diehl de la société Thomson sur les mesures techniques de protection et les DRM.

Le président accueille M.Diehl et le remercie pour avoir accepté de présenter à la commission de la copie privée sa vision des différents dispositifs de protection et de leur mise en place. Il l'invite ensuite à effectuer sa présentation.

M.Diehl indique tout d'abord qu'il est responsable du laboratoire de recherche en sécurité pour la société Thomson dont l'un des intérêts principaux est de protéger les contenus. Il indique que sa présentation sera principalement centrée sur les mesures de protection anti-copie mais qu'il présentera également une brève synthèse sur les DRM lesquels posent un problème similaire mais pas identique.

M.Diehl entreprend ensuite sa présentation sur l'état de l'art des technologies de protection de copie. Celle-ci est composée de quatre parties. La première parlera des menaces, la seconde dressera la panoplie des armes technologiques existantes, la troisième exposera les solutions commerciales que l'industrie se propose de mettre en place. La dernière enfin, présentera les solutions technologiques dessinées par Thomson et leurs spécificités.

1. Les menaces.

Concernant ce point M.Diehl a tout d'abord ciblé trois catégories d'attaquants. Le premier est le piratage de "cours d'école". Il s'agit du fait de personnes qui n'ont pas de grande connaissance technique et qui ont accès à des outils simples et facilement accessibles (matériel de bureau, petit logiciel). C'est ce qui se passe par exemple dans les écoles où les CD sont copiés pour les passer à des amisLe deuxième type est le piratage de garage. Il s'agit ici du fait de personnes qui sans être des experts ont de sérieuse connaissance et qui utilisent déjà des outils sophistiqués (analyseurs logiques, décodeurs). Le troisième type est le piratage organisé, voire mafieux qui fait appel à des experts et requiert de gros moyens financiers. Il s'agit par exemple de personnes qui réalisent des "master" et font de la duplication. Les systèmes de protection de la copie s'attachent aux deux premiers types de

menace et non au troisième. Ce dernier type de piratage relève de la législation, tous les systèmes anti-copie sont inefficaces.

Les types d'attaques peuvent également être divisés en trois catégories. La première est constituée par la copie de "bit à bit". Il s'agit de prendre un média et de le recopier en reconstituant exactement les bits au même endroit. C'est ce qui se passe par exemple avec la copie de CD audio. La deuxième est constituée par la copie avec changement de format et de support. Il s'agit par exemple du procédé utilisé pour transformer un DVD protégé en un CD lisible sur PC, pour cela on utilise des logiciels, du type DeCSS, qui permettent de désembrouiller les DVD, associés au système de compression DiVX. Enfin la troisième qui a les faveurs de la presse, est constituée par la copie avec diffusion sur Internet. Le "média" original est copié puis diffusé sur Internet et éventuellement sur les réseaux "peer to peer".

Les quatre types traditionnels de droit à la copie sont définis par le système "CGMS" - Copy Generation Management System-. Il s'agit : 1° des "copy free", les copies sont en nombre illimité. 2° des "copy once" où seule la copie de première génération est autorisée, en autant exemplaires que souhaité, mais les copies de copies ne sont pas possibles. 3° des "Copy no more" qui sont le résultat de copies marquées « copy once ». 4° enfin, des "copy never" qui ne donnent pas le droit de faire de copie du tout.

M.Desurmont s'interroge sur les différences existantes entre les "copy once" et les "copy never". M.Diehl lui précise que dans les « copy once » la copie de l'original sera marquée tandis que dans les "copy never" toute copie est interdite y compris la copie d'archivage ou de sauvegarde.

M.Diehl passe ensuite à la seconde partie de sa présentation

2. Les différentes technologies de défense

M.Diehl présente tout d'abord la technologie appelée "embrouillage" constituée en réalité par des algorithmes de chiffrement. Cette technologie protège le contenu par l'utilisation d'algorithme d'embrouillage à l'entrée et de clés de désembrouillage à la sortie. Il s'agit d'une protection forte, les techniques sérieuses d'embrouillages n'ont jamais été cassées. La protection passe par le secret de la clé. La clé définit également la granularité de la protection. Le mécanisme de distribution de la clé va en effet définir l'ensemble des appareils qui pourront avoir accès à l'information : si la clé est commune à tous les appareils, ils pourront tous désembrouiller le contenu. En revanche, si la clé est propre à un appareil, le contenu ne sera accessible qu'à cet appareil.

La "signalisation" constitue une autre technologie de défense. Elle consiste à ajouter une information dans le contenu laquelle est extraite à la réception du contenu. Elle permet ainsi, sans modifier le contenu, de définir des actions en fonction des informations données. Il s'agit d'une protection faible puisque l'information doit être extraite. Lorsqu'un appareil n'a pas accès à cette information, il peut avoir accès au contenu. Cette protection nécessite d'être portée par un signal légal, soit par des licences, soit par la loi. Aux Etats-Unis, par exemple, on essaye d'introduire le "broadcast Flag" qui introduit dans le contenu une mention d'interdiction de retransmission sur Internet. Dans cette technologie le "tatouage" mérite d'être signalé dans la mesure où l'information est cachée à l'intérieur de l'image. Elle n'est donc pas visible et sera difficilement altérable mais nécessite d'être extraite par l'appareil à défaut elle sera inefficace.

Un troisième type est constitué par les techniques dites de "localisation de fuite". Ces techniques qui utilisent le tatouage ou l'empreinte numérique consistent à ajouter une information de façon à pouvoir l'extraire à partir d'une copie pirate afin de déterminer l'origine de la fuite. Il s'agit d'une protection par crainte de la répression, si l'on trouve une copie sur Internet dans laquelle il y a une information d'interdiction de copie l'on peut ensuite s'adresser directement à la personne qui l'a réalisée.

M. Diehl poursuit ensuite sa présentation par l'exposé des solutions commerciales

3. Les solutions commerciales

Concernant le CD audio il expose qu'il y a, dans tous les systèmes commerciaux, deux types de techniques. Le premier consiste à rajouter sur le CD des formats qui sont compatibles avec la norme des appareils grand public définis par le "livre rouge" mais qui sont, soit incompréhensibles par un PC soit incompatibles avec sa norme, de telle sorte qu'un PC ne puisse les lire correctement. Le second type est la protection par logiciel qui consiste à ajouter un DRM avant le lancement de la lecture de façon à empêcher des actions illégales. Le plus connu de ces systèmes est « MediaMax CD3 » de SunComm Track, qui vient d'être cassé récemment. M.Diehl souligne qu'au jour d'aujourd'hui toutes les solutions proposées sur le CD audio n'ont pas résisté de manière sérieuse.

Concernant le DVD il indique que celui-ci a été protégé par un système d'embrouillage le « CSS ». Il s'agit d'un algorithme propriétaire. Ce système a malheureusement été cassé en 1999. Il existe pour cela un logiciel assez facile à trouver sur Internet qui s'appelle « DeCSS ». Afin de trouver des solutions à cette situation l'organisme chargé d'émettre les conformités, le DVD CCA, essaie d'introduire l'idée d'imposer un tatouage sur les DVD mais le problème reste la définition des normes de tatouage. Sur les protections de copie concernant les nouveaux formats de DVD - CPRM, CPPM, BDCPS- la nouveauté réside dans le fait que ces nouveaux formats ont tous introduit la notion de révocation de l'appareil. En effet, ils utilisent des technologies qui sont un mélange d'embrouillage, de tatouage, de détection de type de support, et d'identifiant unique qui leur permettent d'empêcher la copie "bit à bit". Le problème est qu'à chaque sortie de nouveau format il faut définir un nouveau standard, cela conduit à une multitude de système de protection qui ont chacun leur faiblesse.

Un autre problème de la technique d'embrouillage réside dans ce qui est appelé le "trou analogique" en ce que cette technique ne ferme pas la porte du passage du contenu numérique à l'analogique et ensuite au ré-engistrement du contenu de l'analogique au numérique. La seule arme pour cela réside dans l'utilisation du tatouage. Cette technique permet en effet de ne pas autoriser la copie du contenu au passage à l'analogique ou encore lors de son entrée dans le réseau.

M.Diehl conclut ce point en précisant qu'actuellement il existe 2 solutions commerciales valables. L'une menée par Digimarc, Philips, Sony et Nec, et une autre par Toshiba. Ces deux solutions ont la même force technique quoiqu'elles ont une robustesse discutable. Ces systèmes sont en concurrence faite au « DVD CCA » d'opérer un choix entre les deux procédés.

M.Diehl présente ensuite les systèmes de protection plus globales portant sur les réseaux domestique.

Il signale tout d'abord le « CPSA » - Content Protection System Architecture- . Il s'agit d'un ensemble de systèmes de protection qui, par un apport croisé, constitue une toile d'araignée de licences croisées où chaque système de protection protège son domaine. Il s'agit d'une solution par puzzle qui présente des lacunes certaines. Il indique ensuite le « DTCP » appelé encore le "5C" parce qu'il a été défini par 5 compagnies : Hitachi, Intel, Matsushita, Sony, Toshiba. Cette solution qui est aujourd'hui utilisée par des majors américaines consiste dans une technique d'embrouillage du contenu pendant le transfert sur la ligne. Elle permet de protéger le contenu d'un appareil A vers un appareil B par l'utilisation d'un algorithme propriétaire, ce qui veut dire qu'il est relativement faible. En effet, seul le transfert d'un appareil à l'autre est protégé, il n'y a pas de définition de la protection des deux côtés de la ligne. De plus, il n'y a pas de définition de la protection du DVD sur le disque dur ou sur la mémoire. Ce système est donc insuffisant et nécessite d'autres technologies pour être efficaces. D'autres systèmes existent tels que le « DVI-HDCP » qui est un format d'interface numérique, pour la protection de copie, qui a été défini par Intel. Ce système fonctionne par embrouillage des composantes vidéo et suivant un schéma d'authentification des appareils. De plus et c'est un de ses intérêts ce système n'autorise que la "copy never". Toutefois ce système a déjà été cassé sans que personne n'ait à ce jour trouvé de solution alternative.

Enfin, il y a les Digital Rights Management (DRM) qui sont plus conçus pour la protection de contenu distribué à travers Internet. Il existe de nombreuses solutions, la plus connue étant celle de Microsoft qui est leader, mais il en existe d'autres telles que Real Network, Intertrust, Open Magic Gate de Sony La protection par DRM fonctionne par embrouillage. Le contenu est livré embrouillé et le DRM livre la clé individuellement à chacun. Dans certains cas, il est rajouté une technologie de tatouage pour pouvoir faire du traçage. Le DRM a toutefois un certain nombre de contraintes. Il doit être présent dans le « player » et il a toujours besoin d'être connecté à une « voie de retour ». De plus un DRM ne peut pas donner un accès permanent à un contenu parce qu'il a besoin de gérer des droits pour être efficace.

M.Diehl entreprend ensuite la présentation du système développé par Thomson.

4. Le système Smart Right

M.Diehl expose tout d'abord que « Smart Right » est un système dédié à la protection de copie sur le réseau domestique. La vision de Thomson du réseau domestique est basée sur le fait que le futur des utilisateurs sera constitué par des contenus qui peuvent être livrés par le câble, le satellite, le réseau terrestre, Internet Ces contenus seront via « des bus numériques » liés à un ensemble d'appareils de lecture et d'enregistrement – téléviseurs, ordinateurs, disques durs, des DVD recorders, portables. Le tout fonctionnant en interconnexion. Le système Smart Right n'agit pas au niveau de la livraison du contenu, les ayants droit savent le faire. En revanche, une fois les droits validés, Smart Right prend le contrôle de ce contenu et le protège à l'intérieur du réseau numérique indépendamment, du type de contenu - audio, texte, image, vidéo- quel que soit son format et quel que soit le type de bus. Pour cela, Smart Right utilise le système de la carte à puce. Ce système - sans être inviolable - permet au moins un renouvellement si bien qu'en cas de piratage, il suffit de changer les cartes. En effet, dans cette matière, il faut garder en tête le fait que tout système de sécurité sera tôt ou tard battu, un système de sécurité inviolable n'existe pas dans le grand public.

Smart Right fonctionne de la manière suivante : le contenu arrive déjà protégé. Les DRM extraient les droits et les vérifient. Smart Right ne touche pas au contenu, il arrive protégé, et va le retransmettre tel quel sur le réseau. En revanche, le système Smart Right va envoyer une clé de désembrouillage à travers le réseau domestique de telle sorte qu'il réalise via un ensemble de technologie associé à une carte à puce, une protection de bout en bout sur l'ensemble des équipements sans pour autant toucher au contenu. Un des avantages de ce système c'est qu'il est indépendant de l'unité de stockage. Une autre nouveauté de ce système réside dans la création du concept de « domaine utilisateur ». Cette notion part du principe que l'utilisateur aura à l'intérieur de son domicile un ensemble d'appareils qui sont connectés entre eux. A ceux-ci pourront s'ajouter d'autres appareils si l'utilisateur a une voiture ou une résidence secondaire. Cet ensemble forme le « réseau personnel privé » et le système Smart Right permet de tous les protéger de façon à ce que l'utilisateur puisse voir le contenu sur n'importe quel de ces appareils. En revanche, ces appareils seront isolés du réseau appartenant à d'autres utilisateurs de façon à ne pas autoriser l'échange de contenus avec les voisins. La notion de réseau personnel privé donne une très grande liberté à l'utilisateur. Celui-ci conserve une liberté de copie, l'utilisateur peut faire un nombre illimité de copies sur n'importe quel support mais l'usage en est restreint au réseau privé de l'utilisateur. Il présente donc un avantage par rapport aux systèmes concurrents qui ne marchent que par appareil ou qui interdisent toute copie. Le système Smart Right permet à l'utilisateur de voir les copies sur ses appareils mais non sur les appareils de son voisin sauf à amener la carte à puce associée.

En conclusion il expose que Thomson s'est trouvé entre deux positions. D'un côté, les ayants droit américains qui voulaient quasiment interdire la copie, et, de l'autre, les utilisateurs qui voulaient faire toutes les copies qu'ils voulaient. C'est pourquoi, ils ont trouvé la solution dans la notion de réseau personnel privé qui autorise les copies privées mais limitées à un usage personnel.

Le président remercie M.Diehl pour cet exposé riche et éclairant et ouvre le débat.

M. Roger (Sorecop) demande si le système Smart Right est limité aux contenus protégés qui circulent sur des réseaux. M. Diehl lui précise que ce système empêche de faire de la duplication de contenu à travers les appareils domestiques de telle sorte qu'un utilisateur « lambda » ne pourra utiliser son graveur pour pouvoir reproduire un contenu. Toutefois Smart Right ne s'occupe pas du « pré-enregistré » il s'interface avec la protection des contenus « pré-enregistrés ». Si le contenu est en clair ou mal protégé à l'entrée, le système ne pourra pas mieux le protéger, en revanche si la protection est forte le système garantit la même force à l'arrivée.

M. Charriras (Sorecop) s'interroge sur la façon dont est gérée la carte à puce – est-elle transportée par l'utilisateur ? M. Diehl précise que les cartes à puce seront livrées de base dans les appareils, ce qui suppose que l'utilisateur achète un appareil à bus numérique. Il relève qu'il s'agit de la future génération d'appareil, il n'y a pas encore aujourd'hui d'appareil à puce numérique mais 'il s'agit d'un point de négociation fort pour les ayants droit puisque ceux-ci imposent de mettre en place un système de protection de copie sur la sortie des appareils numériques.

M. Rogard (Copie-France) relève que ce système présente un intérêt évident pour les ayants droit mais se demande quel est l'intérêt pour les consommateurs d'avoir de tels équipements ? Sur ce point M. Diehl précise qu'il évitera de rentrer dans la polémique de répondre à la question de savoir si les utilisateurs ont un intérêt à la protection de copie. Les ayants droit sont mieux à même d'y répondre. En revanche si l'on part du postulat qu'il faut une protection contre la copie, on peut s'interroger sur le point de savoir pourquoi Smart Right plutôt que d'autres systèmes ? A cet égard, il souligne que Smart Right offre une liberté de copie à l'utilisateur du fait de la notion de réseau personnel privé que n'offrent pas les autres systèmes de protection. Les autres systèmes basés sur le « CGMA » ou les DRM limitent les possibilités de l'utilisateur et ne permettent pas de transporter et de lire la copie sur plusieurs appareils. Le système Smart right est transparent, il respecte l'utilisateur. Celui-ci n'a pas à s'enregistrer, il n'y a pas de traçage. C'est l'appareil qui sera enregistré sur le réseau. La seule limite introduite, tient à l'imposition d'une taille maximum pour le réseau. L'utilisateur aura la possibilité d'y inscrire plus d'équipement mais le système vérifiera si cela correspond à un schéma d'usage illicite.

M. Du villier (Copie-France) relève que le système est limité au réseau personnel privé et demande comment cela fonctionne avec les équipements professionnels utilisés par l'utilisateur dans son entreprise par exemple. M. Diehl répond que ce point a fait l'objet de réflexions et qu'il est possible de faire en sorte qu'un appareil de bureau puisse aussi appartenir au domaine utilisateur tout en isolant les domaines.

M. Roger s'interroge sur la mise en œuvre concrète du système de protection et demande comment celui-ci pourrait-il être appliqué dans le domaine de la musique enregistrée ? Sur ce point M. Diehl précise que le postulat de départ de Smart Right suppose que le contenu soit protégé par embrouillage à défaut il est inefficace. Le problème du CD audio est que les protections mises sur le contenu ne sont pas fiables. Son opinion personnelle est que l'on ne saura pas protéger les CD audio tels qu'ils sont. En effet, par définition les CD audio doivent être lisibles sur une platine de salon donc le contenu ne peut être embrouillé. Il est nécessairement en clair sur le disque et un pirate malin arrivera toujours à le sortir. C'est aussi pourquoi les logiciels d'auto-protection ne seront pas suffisants, le contenu des clés est visible dans le code et il suffira d'un peu d'énergie au pirate pour pouvoir les trouver.

M. Roger relève alors que ce système inviterait l'ensemble des producteurs de disques à migrer vers d'autres formats tels le format DVD audio, au détriment du CD audio ? M. Diehl indique qu'effectivement la migration sur des nouveaux formats permettrait un embrouillage plus fiable de l'audio.

Le président demande si ce système suppose également qu'il y ait une filière normée matériel, support initial, matériel de lecture ou d'enregistrement ou est-ce un procédé qui permet un usage libre quel que soit le matériel que choisit le consommateur ? Sur ce point M. Diehl précise qu'effectivement il faut que les appareils soient Smart Right. Mais un des postulats de base du système repose sur le fait que,

de toute façon, un appareil à bus numérique devra avoir un système de protection de copie. C'est en effet ce que les majors américaines essaient d'imposer à tout les radiodiffuseurs.

Le président relève alors que cela signifie l'intronisation du format du DVD et la mort du CD. Il demande ensuite s'il existe un lecteur universel qui permet à un consommateur de pouvoir utiliser sa copie, le système exposé permet la copie mais ne permet pas par exemple à l'ordinateur d'enregistrer le contenu copié sur disque dur. Sur ce point M.Diehl précise que contrairement aux autres systèmes de protection Smart Right permet une liberté de copie mais d'usage limité sauf à ce que les ayants droit acceptent de tout mettre en copie privée libre.

M.Desurmont relève que s'il comprend bien, ce système permet à l'utilisateur de faire autant de copie qu'il le souhaite, mais la capacité d'utilisation des copies est limitée à son réseau privé. M.Diehl confirme ce point en ajoutant que la copie pourra être réalisée sur n'importe quel format et qu'elle pourra être transportée et lue sur tous les appareils -DVD, disque dur, disquette, etc-. Le réseau est en effet défini par l'utilisateur par les appareils qui lui appartiennent, le système a simplement défini une taille supérieure de manière à ce que le réseau personnel ne devienne pas un réseau d'immeuble

Le président demande comment est identifié le réseau privé et en cas d'enrichissement progressif comment cela se passe ? M.Diehl lui précise que l'identification du réseau s'opère par une clé unique qui sera ensuite intégrée dans les cartes à puces du réseau. La création du réseau génère aléatoirement son identifiant unique. En cas d'acquisition d'un nouvel appareil, la carte Smart Right sera dans un état vierge. Lorsqu'elle arrive pour la première fois dans le réseau, elle se crée son réseau et devient la carte génitrice. Lorsque celle-ci rencontre dans le réseau une nouvelle carte vierge, elle va lui donner le secret du réseau mais va devenir stérile et la nouvelle carte va devenir génitrice- et ce ainsi de suite au fur et à mesure que l'utilisateur va rajouter un appareil

M. Ducos-Fonfrede (Secimavi) demande comment cela se passe au dixième appareil ? M.Diehl indique que dans ce cas il y a un message pour demander à l'utilisateur de contacter Smart Right afin de pouvoir augmenter sa demande. Cela permet ainsi d'adapter le système à un réseau privé pour un hôpital ou un hôtel par exemple.....

Le président demande quels sont les opérateurs qui travaillent sur ce système ? M.Diehl lui précise que ce système est développé par un consortium regroupant dix compagnies dont Thomson, Canal Plus technologies, Gemplus, Schlumberger, Pioneer, Matsushita, SCM, STmicroelectronics, NAGRA et Micronas

M. Dourgnon (UFC-Que Choisir) demande qui a le contrôle de la carte centrale génitrice ? M.Diehl lui répond qu'il n'y a pas de carte centrale, le système marche de manière totalement autonome. Ce sont les cartes entre elles qui savent la limite des appareils et qui informent l'utilisateur.

Le président demande si un système de recours est prévu ? M.Diehl précise que lorsque le géniteur a perdu ses capacités d'insémination, un message arrive à l'utilisateur pour l'informer qu'il ne peut pas agrandir son réseau et qu'il doit contacter la Smart Right Association . A ce moment la Smart Right Association fera l'opération qui permettra d'agrandir le réseau.

Le président relève qu'il y aura alors une intervention humaine et M.Diehl précise que le système sera géré par une association à but non lucratif.

M. Duvillier relève que smart right est composé de grosses compagnies. Cela suppose-t-il que l'utilisateur devra s'équiper d'un matériel fabriqué par ces compagnies. Sur ce point M.Diehl précise que l'espoir de Smart Right repose en effet sur le fait que tous les fabricants suivent ce standard. L'objectif est de livrer la licence du système à tout le monde.

Le président s'interroge sur les rapports avec Microsoft » ? M.Diehl lui précise que le DRM est resté à l'entrée . Le contenu sera contrôlé DRM sur le PC mais, lorsqu'il ira sur le téléviseur par exemple, il devra passer dans le format Smart Right.

M. Roger relève que la mise en œuvre de cette protection suppose que l'ensemble du parc informatique et plus généralement de tous les réseaux, lecteurs ou appareils qui permettent d'assurer la circulation d'œuvres protégées, soient pré-équipé ou compatible avec l'implémentation de ce nouveau système. Ce qui n'est pas le cas aujourd'hui. Ce système ne pourra donc valoir que pour le futur et dans l'hypothèse où tout ou partie des fabricants acceptent ce standard. A cet égard, M.Diehl relève que si actuellement il n'existe aucun appareil de réseau domestique sur le marché, ceux ci se développeront dans trois ou quatre ans. Au moment où les appareils vont s'interconnecter, il faudra en effet prendre un standard, ce sera Smart right ou un autre système concurrent . Il souligne qu'il y a déjà de grandes fuites alors que les appareils ne sont même pas connectés numériquement. La situation sera encore pire, si l'on ne met pas de système de protection lorsque les appareils seront en numérique et permettront donc de faire des copies parfaites sans dégradation.

M. Rogard relève que ce système repose sur le fait qu'il y ait des mesures législatives de protection des copies. S'il n'existe pas en effet une obligation de développer ce système on ne voit pas pourquoi des particuliers y auraient intérêt. M.Diehl fait en effet observer que ce système sera dépourvu d'intérêt si personne ne demande la protection de la copie

M. Rogard fait alors remarquer que même si certaines personnes demandent des protections contre la copie il faudra en outre qu'elle soient imposées. Il existe en effet d'autres personnes qui ne veulent pas des mesures techniques de protection et qui sont satisfait du système qui permet de faire de la copie sans pour autant permettre le piratage. Cela étant, il estime que la conception du système exposé est plutôt intelligente et demande s'il permet aussi d'avoir une protection contre le "peer to peer" ?

M. Diehl précise que le système Smart Right a aussi intégré les réflexions relatives au "peer to peer". Le système de carte fonctionne de telle sorte que rien n'empêche l'utilisateur de prendre son appareil et de se brancher, à travers un "peer to peer", sur un réseau personnel privé ? Cependant le mécanisme des jetons géniteurs qui deviennent stériles fera en sorte de limiter la multitude des connexions et des transferts On ne peut donc pas constituer un réseau. De plus, les ayants droit peuvent très bien collecter des jetons sur le "peer to peer" et les personnes qui auront perdu leur jeton vont contacter la Smart Right Association si bien que celui-ci pourra déceler le schéma d'utilisation illicite.

M. Dourgnon évoque le problème de la compatibilité du système avec les autorisations permises par les DRM. Par exemple si on achète un contenu protégé dans le cadre d'un DRM extérieur il ne peut être téléchargé sur un téléviseur ou encore si on l'achète un contenu par le biais d'Internet et que le DRM accorde un nombre de copie limité alors que le système dans le réseau permet de faire des copies de façon illimité. N'y a t-il pas alors une contradiction avec ce qui est acheté au départ et ce que le système permet de faire ? . Et si tel est le cas, il faudra donc que les personnes de l'extérieur et de l'intérieur du système se mettent d'accord.

M.Diehl en convient et indique que Smart Right ne peut marcher qu'en accord avec les DRM, les accès conditionnels et autres. C'est pourquoi ils sont en discussion avec Microsoft.

M.Dourgnon relève que si finalement l'utilisateur ne peut plus transporter l'œuvre dans le cadre de sa maison, d'un appareil à un autre librement ,et, si il doit payer à chaque opération il y aura quand même un sérieux problème de définition de la copie privée.

M.Chite (SNSE) souhaite réagir de manière globale à la présentation de M.Diehl. Il relève tout d'abord qu'il y a eu, il est vrai, une multitude de développement de système de protection. Beaucoup d'argent a d'ailleurs été investi dans ces systèmes, à la fois du côté des ayants droit, des majors et des fabricants d'électronique. Cela est certain en tout cas pour le DVD. Concernant le CD, il indique qu'il est un peu rapide de le condamner. S'il est exact qu'il plus difficile de protéger le CD audio en raison

du grand parc de lecteur et du fait qu'on ne peut trafiquer le signal pour qu'il soit compatible à la lecture, il existe néanmoins d'autres solutions. En effet, des business models sont en marche sur la vente de CD enregistrés, avec un certain nombre de boni - ouverture à des clubs, achats préférentiels, vidéo-clips, etc. qui font en sorte que le CD vendu sera beaucoup plus attractif que le CD "piraté".

Concernant les développements relatifs au DVD, M.Chite relève que cette démonstration, si éclairante qu'elle soit, envisage néanmoins les choses à très long terme. Il faut penser qu'il y a un parc existant et il faut assurer au consommateur une compatibilité totale. Le système exposé suppose, quelque part, le renouvellement d'un parc adapté à ce système de protection. Plus fondamentalement, il souligne qu'on ne peut dénigrer les travaux effectués sur la protection du DVD c'est-à-dire de l'image. S'il est vrai qu'il y a de fortes chances pour qu'il soit difficile, techniquement, de protéger le CD, il y a encore de la place pour le travail sur le DVD. Dans ce domaine les travaux et les sommes investis sont énormes. Pour le groupe Sony qui représente Columbia Tristar, il y a 65 personnes qui travaillent à plein temps uniquement sur la protection des droits, et le groupe est en même temps fabricant de DVD vierges et diffuseur de DVD. Il estime quant à lui, que dans le domaine de la vidéo il y a de fortes chances que les systèmes de protection fonctionnent. A telle preuve que les investissements sont également réalisés par les ayants droit.

Enfin, il rejoint les analyses de M.Diehl pour ce qui concerne le réseau familial. A cet égard, il indique que Sony a, lors d'un récent salon professionnel, présenté un réseau entièrement compatible entre le PC, le téléphone, le téléviseur, le magnétoscope, le DVD enregistreur, le player, etc. Les technologies dans le domaine de la copie privée ont effectivement évolué. S'il y a encore quelques années, l'équipement familial se composait d'un VHS, d'une télévision, d'une radio et d'un enregistreur CD, aujourd'hui, le domaine de la copie privée s'étend. Il va de la chambre des enfants, au salon, au bureau des parents, les contenus sont échangés dans la surface privée, et il faut espérer qu'ils ne franchissent pas le palier du voisin. Le réseau familial doit être effectivement appréhendé comme tel aujourd'hui.

M. Diehl partage l'analyse de M.Chite concernant la vidéo et indique que ses développements allaient dans le même sens. Il estime également qu'une des meilleures protections contre le piratage des CD réside dans le développement de business model qui les rendront plus accessibles et agréables pour l'utilisateur. Il est évident que la copie pirate perdra son intérêt en face d'une offre normale plus attractive.

M.Chite relaie ses propos et exprime sa conviction quant à l'apport des nouveaux business model sur l'audio. En effet, actuellement la copie pirate procure exactement la même chose au consommateur que l'achat de l'original. Si demain les business model changent et si l'achat d'un CD apporte des plus values- clips vidéo, posters, ... - Il y aura une différence indéniable entre le produit acheté et le produit piraté. Il souligne que Sony croit fermement en cette solution et commence à la mettre en place sur le net où les CD audio seront accompagnés de boni. En revanche, pour le DVD, Sony travaille sur la protection.

M.Desurmont, sans préjuger de la validité et du bien-fondé de l'analyse de M.Chite sur les business model, exprime néanmoins son scepticisme quant au fait que les boni proposés suffisent, dans l'esprit des gens, à faire la différence entre le payant et le gratuit pour les dissuader de ce dernier.

M. Dourgnon fait observer que ces propos reflètent une triste vision des consommateurs français. Il indique que l'album de Florent Pagny s'est vendu à 800.000 exemplaires alors qu'il s'agit d'un album non protégé et qu'on peut le télécharger sur Internet.

M.Chite répondant aux propos de M.Desurmont précise qu'il a conscience que les business model ne représentent pas une solution idéale. Néanmoins des entreprises comme Sony Musique sont très préoccupées par le fait que la vente de CD est revenu au niveau de 1993. Par conséquent toutes les idées qui pourraient contribuer à remotiver des générations à acheter du CD sont mises en œuvre.

M. Desurmont précise que ses propos n'étaient pas une critique de la stratégie, mais il craint que les business model ne soient pas, de loin, la panacée. Cela ne veut pas dire pour autant qu'il ne faille pas les essayer. De ce point de vue-là, les intérêts des ayants droit sont totalement convergents avec ceux des industriels.

M. Roger souhaite réagir aux propos de M. Chite. Il expose tout d'abord qu'il est en partie d'accord avec le raisonnement suivant lequel les producteurs phonographiques, sont obligés pour lutter partiellement contre le phénomène copie privée et de piratage de s'acheminer vers la voie des plus-produits sur Internet, et ce, indépendamment des systèmes de protection. Il s'agit d'un modèle économique qui consiste à investir massivement sur l'exploitation de la musique en ligne pour essayer de développer un relais de croissance tout en évitant la "calamisation" des ventes. Il précise que telle est en effet la voie qu'un certain nombre de producteurs sont en train de suivre. Mais pour sa part, il partage les craintes exprimées par M. Desurmont. Cette solution est nécessaire mais pas suffisante pour contrecarrer le phénomène du piratage. Il rappelle qu'en France les ventes de CD ont baissé de 10 % depuis le début de l'année. La piraterie est directement responsable de ce phénomène et la France n'échappe pas à la situation mondiale. Il y a un lien entre le développement du haut débit et le développement du « peer to peer » qui participe au « pompage » massif de façon illicite de la musique. Pour ce qui concerne les mesures techniques de protection des CD, il ne peut quant à lui croire à la mort de ces systèmes. Il relève que les éditeurs phonographiques testent des systèmes de protection et ne sont pas prêts à renoncer à cette solution sur les CD. A cet égard, il évoque le système développé par MPO qui assure une compatibilité avec un système de double session. En tout état de cause si l'on suit les analyses exposées par M. Diehl quant à l'inefficacité des mesures de protection sur le CD et si celui-ci a raison, la conclusion basique qu'il faut en tirer est qu'il n'y a alors aucune raison de remettre en cause la rémunération pour copie privée, en tout cas pour le sonore.

M. Chite relève que personne n'a remis en cause la redevance au titre de la copie privée sur l'audio. Ce n'est pas le sujet. En revanche, il n'est pas tout à fait exact de dire qu'il n'y aura plus jamais de possibilités de protection sur le CD audio. Il existe en effet des mesures de protection [des disques sur les PC]. C'est une première limite, même si elle n'est pas intégrale. Ce qu'il faut signaler, c'est que la production de CD est mondiale et que, vis-à-vis du consommateur, quel que soit l'endroit dans le monde où on achète le CD, ce CD doit être lisible sur l'ensemble du parc de lecteur. C'est ce qui rend ce compromis difficile pour les CD alors que, les nouvelles générations de DVD sont encore dans une phase technologique de définition de standard et que le parc n'est pas encore défini.

Le président invite les membres de la commission à recentrer le débat sur la question des conditions de mise en œuvre des mesures techniques de protection. Il comprend l'importance des enjeux et des investissements industriels, néanmoins il relève que l'enjeu principal aujourd'hui c'est le piratage et le "peer to peer". Il est aujourd'hui sonore. Il sera demain audiovisuel. C'est pourquoi il souhaite avoir des éclaircissements sur l'analogie des mesures de protection avec celles concernant la gestion des droits pour savoir ce qui se passe dans ce domaine.

M. Dourgnon souhaite également avoir les précisions de M. Diehl sur les nouveaux systèmes qui arrivent tels celui de MPO ou le CD 300 de « Macrovision ». Ces systèmes présenteront-ils un bon équilibre entre fiabilité, efficacité et "jouabilité", c'est-à-dire à la fois lecture et copie privée ? A défaut dans quel sens vont-ils ? Verrouilleront-ils les utilisations où seront-ils plus permissifs ?

M. Diehl souhaite d'abord réagir aux propos tenus concernant les problèmes de protection sur le CD audio. Il indique que ce problème est historique. En effet, les standards ont été définis il y a une vingtaine d'années par le « livre rouge ». Pour donc être lisible sur un lecteur de salon le CD audio doit être compatible avec le livre rouge et cela signifie que les pistes doivent nécessairement être en clair à défaut on perd toute compatibilité. C'est ce qui explique que certaines expérimentations de systèmes qui avaient un peu essayé de jouer sur les standards du « livre rouge » ont posé certains problèmes de lecture. Est ensuite arrivé le format du CD-Rom qui intègre des multi-sessions, c'est à dire qu'il ajoute des pistes supplémentaires sur lesquelles des appareils vont pouvoir lire la session principale qui est la session audio. Tous les nouveaux systèmes travaillent sur le multi-session. Un PC

par exemple va lire l'ensemble des sessions et va réagir en fonction. Il ne va pas aller directement sur la session audio. Sur le système « mediamax » par exemple, la première session lançait un « driver » qui se trouvait écrit sur le CD avec un code de DRM qui contrôlait les usages. Il souligne en conclusion de ce point que ses propos concernant le fait que les pirates vont probablement toujours gagner, viennent de la simple constatation, que ceux-ci ont probablement lu le « livre rouge » et savent où sont les vraies pistes et les systèmes multi-session. Si bien qu'ils pourront se débrouiller pour faire un programme pour empêcher de lire les sessions. Un « hacker » trouvera un moyen parce que l'information, quelque part, est disponible et visible.

M. Diehl présente ensuite le fonctionnement d'un système Digital Right Management DRM.

Il expose tout d'abord que les DRM sont un ensemble de technologies qui permettent de contrôler et d'obliger à répondre à un certain nombre de business model, associés à des « digital rights ». Ceux-ci sont des spécifications de droits, d'usages, par exemple des permissions à copier, à imprimer, à déplacer. Ou encore des contraintes diverses par exemple : « Vous pouvez le voir 5 fois » « Vous pouvez le voir 4 heures ». « Vous pouvez le voir uniquement en Europe ». etc. Les DRM associent aussi des obligations. Un type d'opération est associé à un paiement ou à des mentions informatives sur les « Right Owner », c'est-à-dire sur ceux à qui appartiennent les droits.

Les DRM sont donc des langages de description de ces droits. Deux langages sont en passe d'émerger, le « XRML » et le « ODRL » (Open digital right langage). On assiste actuellement à un mouvement de standardisation des DRM mais il porte seulement sur l'expression de ces droits et non la manière de les renforcer ni la manière dont on va protéger les contenus.

Le DRM fonctionne de la manière suivante : une fois le contenu reçu, il est packagé, par un système d'embrouillage, les droits sont chiffrés et le tout est ensuite mis sur un serveur. Le client qui souhaite lire le contenu n'aura pas toutes les informations des droits. Il ira les chercher sur une « clearing house » qui va l'informer que le contenu voulu est payant. Une fois que la « clearing house » a reçu l'argent, elle va aller à un serveur de licence qui, connaissant le contenu, va transmettre de manière sécurisée la clé qui va permettre de prendre connaissance des informations. Un DRM a nécessairement besoin, au moins une fois, d'avoir une voie de retour parce que la clé n'est pas livrée avec, contrairement au monde du « broadcast » où la clé est cachée et livrée, de base, dans le contenu.

En conclusion de cette brève présentation il indique que les DRM sont adaptés à tout type de contenu : audio, vidéo, texte. Il cite enfin les principaux : « Windows Media right manager » de Microsoft qui sera peut être livré de base dans la prochaine version d'OS, « Helix » de Real Network, « Open Magic Gates » de Sony, « Intertrust », racheté récemment par Philips et Sony]

M. Dourgnon demande si les DRM sontinteropérables : un consommateur qui achète un CD muni du dispositif de Microsoft par exemple pourra-t-il techniquement et si il en a l'autorisation faire une copie et la mettre sur un iPod. Sur ce point M. Diehl répond qu'il ne devrait pas avoir de problème si MPO a fait en sorte que les drivers multi-session soient aussi compatibles OS X. De manière générale M. Diehl explique qu'il n'y a pas aujourd'hui de DRM interopérables. Les forums actuellement se battent pour chercher l'interopérabilité. Le seul niveau d'interopérabilité qu'ils ont réussi à trouver, est dans l'expression des droits, où il n'y a que deux langages, mais les DRM ne sont pas encore arrivés à trouver une interopérabilité au niveau des contenus. C'est d'ailleurs un combat que Thomson essaie de mener en cherchant des solutions techniques sur les players car Thomson est aussi utilisateur.

M. Chite rebondit sur ces problèmes en expliquant par exemple que le contenu enregistré sur mini disque ne peut être exporté sur un disque dur pour ensuite être envoyé par Internet. Le système de protection du mini-disque, conçu pour protéger les enregistrements par micro, ne peut pas fonctionner dans ce sens.

Le président clôt ensuite le débat. Il remercie monsieur Diehl pour avoir éclairé la commission sur les perspectives, à la fois stratégiques et techniques sur lesquelles travaillent les laboratoires de recherche.

A cet égard le dialogue entre Thomson et le représentant à la commission du groupe Sony est intéressant.

M. Diehl remercie également la commission de l'avoir accueilli et indique qu'il tiendra la présentation à la disposition de toute personne intéressée.

Le président propose une suspension de séance avant de reprendre le débat.

4) Reprise des débats. Point sur les études et questions diverses.

Le président ouvre la discussion. Il expose tout d'abord que si la commission confirme son intérêt pour cette audition, M. Chantepie qui conduit une mission interministérielle portant notamment sur les mesures techniques de protection, pourrait exposer à la commission l'état de ses constats. D'autre part, il rappelle qu'il serait également utile que la commission puisse discuter de la stratégie et des intentions des « majors », notamment en matière de techniques de protection. A cet effet, il indique qu'il a rencontré M. Eric Tong Cuong président de EMI France et que celui-ci serait d'accord pour être auditionné par la commission. La commission pourrait également convier M. Pascal Negre. Il propose si la commission en est d'accord d'organiser ces auditions.

M. Dourgnon relève que l'audition des présidents des majors sera intéressante si elle porte sur les intentions des maisons de disques en termes d'usage de mesures techniques de protection. Il ne s'agit pas de les auditionner sur les problèmes de «peer to peer» ou du téléchargement.

Le président précise que le débat est contrasté sur ce point. Il considère que si pour la commission il est important d'explorer la mise en œuvre et les réactions quant à l'implantation des mesures techniques de protection, il comprend également que, pour l'industrie musicale, l'urgence est quand même le «peer to peer». Par conséquent la commission ne peut interdire à un des dirigeants de l'industrie musicale de parler du «peer to peer» lorsqu'il vient parler de copie privée. D'autant plus, que la commission ne peut se désintéresser du lien entre ces problèmes pour mesurer notamment l'impact de la mise en place des systèmes de protection et gestion des droits sur ses propres réflexions concernant l'assiette et la gestion de la copie privée.

M. Dourgnon relève que cela dépend de la stratégie des maisons de disque. Si celles-ci sont favorables à la licence légale sur le «peer to peer», cela intéresse la commission. Si en revanche il s'agit de faire des business model pour de la vente ligne, cela ressort, selon lui, du droit d'auteur direct. A cet égard, il fait observer que cela est exclu du champ de la copie privée dans la directive. En effet, cette dernière rappelle que la rémunération de la copie privée, lorsque les Etats l'ont choisie, se mesure au regard des mesures techniques de protection lorsque le bénéficiaire a eu un accès licite à l'œuvre.

Le président indique qu'il comprend ces arguments. Cependant il fait observer que même si la priorité pour la commission est de connaître l'attitude des maisons de disque par rapport à la mise en place de mesures techniques de protection, il est difficile d'auditionner un patron de l'industrie musicale sans qu'il expose ses problèmes. D'autant plus qu'il rentre dans les compétences de la commission d'évaluer, en tant qu'utile, l'impact sur l'assiette et sur les taux de la rémunération des opérations de téléchargement et, par conséquent, d'enregistrement sur tel et tel support.

M. Desurmont tient à signaler qu'il est en désaccord avec la lecture que fait M. Dourgnon de la directive.

M. Rogard suggère d'auditionner M. Didier Mathus.

M. Rioult (SFIB) souscrit à cette proposition et indique qu'il sera intéressant de le rencontrer même si ses positions peuvent être critiquables à certains égards.

Le président indique que cela peut être envisagé. Il est intéressant en effet de rencontrer certains parlementaires, et en particulier M.Mathus qui s'intéresse à la copie privée, dans la perspective du débat parlementaire de la transposition de la directive. La commission va en effet être confrontée à plusieurs attitudes qui peuvent conditionner la suite des travaux. Certains pourront estimer que rien ne doit être protégé que tout doit être copiable. D'autre l'inverse, d'autre encore pourront avoir une position plus nuancée. Ce débat va forcément arriver et il est probable que les parlementaires auront des difficultés à appréhender les choses avec une conscience très claire. C'est pourquoi, il est important que les industriels et les ayants droit trouvent des positions convergentes et la commission peut y contribuer.

M.Rogard relève l'intérêt d'auditionner également des représentants de l'édition video sur le problème des mesures de protection technique, la problématique des DVD est quand même différente de celle des CD. Il suggère à cet effet l'audition de la présidente du syndicat de l'édition vidéo (SEV) .

Le président agréé cette proposition puis aborde le problème des études. Il indique tout d'abord que le questionnaire Médiamétrie pour le lancement de la seconde vague d'étude a été validé et envoyé à Médiamétrie (document distribué en séance). Concernant le questionnaire sur les mesures techniques il expose que celui-ci a été examiné lors de la réunion du comité de pilotage du 2 octobre. Un compromis est en voie d'être trouvé entre les positions de M.Dourgnon et celles de M.Guez. Le problème de la discussion qui a animé l'élaboration du cahier des charges, réside dans la difficulté de faire une enquête sur le comportement du consommateur face aux mesures techniques de protection sans pour autant la transformer en une étude sur le piratage puisque ce n'est pas l'objectif de la commission. Mais il se trouve que les frontières ne sont pas faciles à situer. Il fallait donc trouver une manière de poser des questions sans qu'elles apparaissent, soit comme légitimant des pratiques, soit comme relevant d'une enquête sur des pratiques de piratage. Un projet de cahier des charges devrait être transmis au secrétariat afin que celui-ci puisse être finalisé lors de la prochaine réunion du comité de pilotage qui a été fixée le 27 octobre. Il souligne en effet l'importance de conclure ce questionnaire assez rapidement afin que la commission soit en mesure de lancer un enquête, au plus tard au début de l'année prochaine, et, puisse rapidement en exploiter les résultats. En effet, il sera intéressant d'évaluer l'évolution des comportements et des usages du public afin, le cas échéant, rectifier certaines idées fausses qui circulent.

Par ailleurs, il relève que les ayants droit et les industriels disposent d'un appareillage d'étude notamment de la part de TMO, GFK. Il souligne qu'il serait utile pour le programme des études de la commission d'en effectuer un recensement en termes de consistance, caractéristiques, fréquence et résultats. En effet, ces études ou enquêtes peuvent si elles contiennent des données utilisables par la commission contribuer à l'éclairer et à faciliter la discussion en son sein. Il y aura bien évidemment des précautions à prendre pour respecter le devoir de confidentialité exigé mais il y a en même temps une possibilité d'information intéressante. Si la commission est d'accord sur le principe, M. Sauvanaud ou M. Ducos-Fonfrède pourrait se charger de faire cette revue de détail du côté industriel et M. Van der Puyl et Charles-Henri Lonjon du côté des ayants droit.

Le président propose ensuite de faire un point, vu l'heure tardive, concernant l'avancée des discussions sur l'évolution des DVD.

5) Point sur l'avancée des discussions concernant l'évolution des DVD et autres supports émergents sur le marché.

M.Sauvanaud indique qu'il y a deux sujets que le SNSE souhaiterait traiter. Le premier concerne le DVD 8 centimètres. Le SNSE souhaite en effet avoir une réaction rapide des ayants droit sur ce point car ces supports arrivent sur le marché et rappelle que les ayants droits s'y sont engagés. Sur le second, concernant l'évolution des DVD en général il indique que le SNSE poursuit son travail de collecte d'information et sera en mesure de présenter un argumentaire et des propositions pour la séance du 18 décembre.

Le président relève que la question du DVD-8 cm peut être dissocié de la problématique générale sur les DVD à moins que ceux-ci constituent une nouvelle famille de DVD.

M. Sauvanaud précise que pour le SNSE, les problématiques sont dissociées. Le DVD 8 cm a vocation à être sur les caméscopes et il devrait donc suivre la logique des supports intégrés dans ces appareils. En revanche, si on assimile contre l'avis du SNSE, le DVD 8 cm à un DVD normal, il fera partie de ce paquet. Pour le SNSE le DVD 8 cm est une problématique qu'il faudrait régler rapidement.

M. Rogard relève qu'il y a en effet deux sujets différents. Sur la problématique générale posée par le DVD, il répète que sa position est claire. Les contentieux menés par l'UFC que Choisir font peser une incertitude sur le fait de savoir si l'on peut protéger des DVD enregistrés. On change la donne et il est difficile de prendre position tant que cette question ne sera pas réglée.

Le président comprend ces arguments. Toutefois il souligne qu'il faut distinguer les débats extérieurs de ceux de la commission. Il est important que la commission puisse poursuivre ses travaux en tenant compte du fait qu'il y a des incertitudes de nature juridique -ou politique le cas échéant- sur ce point. La commission ne peut, soit prendre, soit différer ses décisions, sans bien étudier tous les aspects du problème. C'est pourquoi, et cela a été délibéré au sein de la commission, elle doit poursuivre ses débats sur l'évolution des formats et des usages concernant les DVD et les supports équivalents. A cet égard, il souhaiterait en premier lieu que le SNSE clarifie bien, lors de sa prochaine présentation, ce que représente le format du DVD-8 cm au sein de la famille des DVD et dans quelle mesure on peut considérer qu'il est bien circonscrit à un type d'usage. En second lieu, il faut poursuivre et conclure le débat engagé depuis 4 mois sur l'évolution des DVD et son rapport avec l'économie de la copie privée.

M. Desurmont relève que le SNSE, depuis plusieurs séances, développe les arguments qui justifient dans son esprit une baisse de la rémunération sur les DVD. Il souhaite que les ayants droit, une fois la présentation du SNSE terminée, puissent à leur tour faire valoir leur point de vue de manière structurée et argumentée comme cela a été le cas lors des débats précédents de la commission sur d'autres sujets.

M. Rogard relève que lors de la séance du conseil supérieur de la propriété littéraire et artistique, le directeur de cabinet de Jean-Jacques Aillagon a expliqué que le projet de loi de transposition était en phase d'adoption par le Conseil d'Etat et allait être prochainement présenté au conseil des ministres. De plus, il devrait être soumis en première lecture au parlement premier trimestre 2004 ce qui donnera déjà une vision des choses. Il répète qu'il ne peut honnêtement se prononcer sur des niveaux de rémunération pour copie privée par rapport au DVD en face d'un environnement qui pourrait radicalement changer. Il souligne avec force que - comme cela a été confirmé par M. Chite-, le moteur de l'industrie cinématographique actuellement, c'est le cinéma enregistré sur DVD et non plus la salle. L'environnement est radicalement changé et les ayants droit de l'audiovisuel ne peuvent prendre de risque.

M. Desurmont partage l'opinion de Pascal Rogard. Il relève néanmoins que cela n'empêche pas les ayants droit de présenter leurs observations, à environnement constant, c'est-à-dire dans le cadre des éléments connus aujourd'hui. Mais, bien évidemment, le problème d'une suppression des mesures techniques de protection sur les DVD est tout à fait de nature à modifier la situation de manière fondamentale.

M. Sauvanaud souligne que ce problème intégrera les réflexions de la commission mais qu'il faut continuer à débattre.

M. Dourgnon relève que le raisonnement tenu par Pascal Rogard est un peu exagéré. La décision du tribunal n'aura pas l'incidence qu'il lui prête sur les travaux de commission. Il souhaite par ailleurs avoir confirmation du fait que la ventilation des sommes de la copie privée s'effectue à partir de la diffusion sur les télévisions hertziennes. Dans ce cadre, il faudrait évaluer la copie privée uniquement à partir des œuvres protégées diffusées sur les chaînes hertziennes et exclure la proportion des œuvres non protégées et toutes les œuvres protégées diffusées à partir du câble, des chaînes à péage, etc.

Le président relève qu'il faut cesser les différentes polémiques internes et progresser. Il souhaite donc répondre en ce sens aux propos tenus. Il indique à l'attention de M. Dourgnon qu'on ne peut appauvrir le droit. Ce que disent les ayants droit des œuvres cinématographiques, c'est qu'on ne peut pas faire de copie privée à partir d'un DVD puisque ce DVD est protégé. En revanche, toutes les autres sources d'enregistrement ne présentent pas le même obstacle. Par conséquent, elles sont toutes concernées. Il rappelle que si la commission, dans sa grande sagesse, pratique des abattements pour tenir compte des usages, juridiquement, toute forme de copie, quelle que soit sa durée, qu'elle soit éphémère ou pas, est naturellement éligible à la rémunération. De même que juridiquement, toutes les formes de source, pour autant qu'elles soient licites, dit la directive -quoique sur ce terme peut encore donner lieu à de multiples interprétations-. Il s'agit donc d'un débat d'orientation et non d'un débat juridique au sens propre du terme.

Il souligne à l'attention de M. Desurmont et de M. Rogard, que si l'environnement est incertain la commission peut contribuer à le rendre relativement plus stable. Il rappelle que la commission a décidé de réviser périodiquement les termes d'assujettissement de tel ou tel support à la copie privée, en fonction de l'évolution de l'environnement. La commission ne peut donc s'interdire de réfléchir aux mesures techniques de protection mais aussi à la situation des différents supports qui ont déjà été considérés. Par ailleurs, il fait observer que la commission n'a pas rendu éligible l'ensemble des supports qui potentiellement le sont. Les raisons sont connues et la commission a parfaitement le droit de procéder ainsi parce qu'elle peut hiérarchiser et sélectionner les supports. Pour autant, elle ne peut pas commettre d'erreur manifeste de droit ou de fait, et il convient d'être attentif à cela. La commission doit respecter un équilibre global, juste, équitable entre à la fois les différents supports mais aussi entre les différentes catégories d'assujettis et d'ayants droit. C'est pourquoi la démarche consistant à expliquer comment l'univers a changé et quelles sont les conséquences en tirer est en elle-même légitime. Ce débat sera d'ailleurs vraiment utile que s'il prend en compte l'ensemble de l'univers de concurrence de tel ou tel support. C'est aussi un problème qui se pose.

M. Desurmont relève que ce problème est effectivement un problème de fond, important. Ce sujet mérite certainement une discussion approfondie et il n'est pas, pour sa part, absolument certain des conclusions à en tirer.

M. Rogard relève que l'univers de concurrence, commence à se stabiliser sur la musique en revanche il n'est pas encore complètement déterminé sur l'image. On est dans la phase où cela commence à changer, avec le développement du haut débit, etc. Il n'y a donc pas encore de véritable visibilité sur l'univers de copie privée audiovisuel numérique tel qu'il va se développer dans les quatre ans qui viennent. A cela s'ajoute les incertitudes législatives. Ce n'est pas seulement les incertitudes liées aux contentieux, il y a aussi celles de nature législative liées à la transposition de la directive. Si la législation change et permet un certain nombre de copies, cela va changer complètement l'environnement économique et l'univers des ventes des DVD.

Sur ce point M. Dourgnon relève que le projet de loi tel qu'il est, n'apporte pas de modification sur la définition de la copie privée par rapport à ce qui existait.

Le président clôt le débat et prend acte du fait que le SNSE présentera ses arguments et propositions lors de la séance du 18 décembre. La séance qui la suivra sera consacrée à la présentation complète, par les ayants droit de leur argument et position sur la demande de révision de la rémunération sur les DVD.

Il remercie les membres de la commission et leur rappelle que, comme convenu, la prochaine séance aura lieu le 18 novembre.