



I A L T A

***Digital Rights Management
et
identification des utilisateurs***

Recommandation pour l'utilisation des certificats électroniques dans le DRM

**Conclusions du Groupe de Travail
Signature Electronique et Propriété Intellectuelle (SE-PI)**

Janvier 2004

Version 1.07

Membres du groupe de travail ayant participé à la rédaction de ce document :

- Michel CHEVRIER, Ialta
- Thierry PECQUET, Thalès
- Etienne PELLETIER, Ialta
- Isabelle PETIT-PEUCELLE, Advance Technologies
- Thierry PIETTE-COUDOL, avocat
- Jean-Jacques RAYNEL, avocat
- Hervé SCHAUER, SH Consultants
- Frédérique TASTET-CHEREL, Thalès Communication

Les membres du groupe de travail tiennent tout particulièrement à remercier de leurs contributions les personnes et entreprises suivantes :

Claire Albouy (CNAM-TS), Raphaël Alimi (Thalès), Frédéric Bernard (Thalès Secure Solutions), Pierre Bresse (Breese et M.), Jérôme Chouraqui (consultant), François Coutillard (Teamlog), Samuel Deschamps (Breeze et M.), Céline Guyot-Sionnest (Deloitte & Touche), Magali Julin (étudiante), Hervé Martin (KPMG), Ahmed Serhrouchni (ENST), Philippe Thorel (MPO), Bertrand Warusfel (avocat).

Sous la direction de Jean-Jacques RAYNEL, avocat au barreau de Nice (cabinet Raynel, Million & associés), président du GT et de Thierry Piette-Coudol, avocat au barreau de Paris (cabinet Bertrand & associés), rapporteur.

Un Comité de Suivi procédera à une mise à jour du document. Toute observation, contribution ou critique peut lui être communiquée à l'adresse suivante via le site de l'association : www.ialtafrance.org

La reproduction du document autorisée, moyennant la citation de l'intitulé du document et de l'auteur, l'association IALTA, en mentions claires, apparentes et parfaitement lisibles, et son affectation à une utilisation personnelle ou strictement non commerciale, quel que soit le support. Cependant, toute reproduction sur un support tel que CD / DVD, disquette ou tout autre média permettant une diffusion de masse, y compris mais sans limitation une diffusion sonorisée, visualisée, etc., doit être autorisée préalablement par écrit par l'auteur. La demande d'autorisation sera transmise via le site de l'association.

1. LE MANDAT DU GROUPE DE TRAVAIL

Le GT s'est donné pour mandat d'étudier le thème suivant :

La signature électronique, prise uniquement dans sa dimension technique¹, garantit l'origine d'un fichier, quel que soit son contenu (texte, graphisme, multimédia...), ainsi que son intégrité par rapport à son contenu d'origine. Dans quelle mesure, ces caractéristiques peuvent-elles constituer des garanties pour les droits d'auteur portant sur les œuvres numériques ?

Lors des premières séances, l'attention des membres du GT a été attiré par le rapport rédigé au Ministère de la Culture par MM. Philippe CHANTEPIE, Marc HERUBEL, Frank TARRIER, "*Mesures techniques de protection des œuvres & DRMS – Un état des lieux janvier 2003*". Le GT considérant que le rapport faisait un panorama complet de la situation juridique, des besoins techniques et des moyens de protection, s'en est tenu à l'étude des relations entre le DRM et la certification électronique dont la promotion constitue l'objet de l'association.

Le GT a fonctionné de mars à novembre 2003.

Index

<i>1. Le mandat du groupe de travail</i>	3
<i>2 Les besoins et le contexte d'utilisation</i>	4
21 La notion d'œuvre numérique.....	4
22 La propriété intellectuelle et la protection de l'œuvre numérique	4
23 La protection des e-services et des formulaires électroniques	6
<i>3- Les moyens de protection actuels et l'approche sécuritaire</i>	8
31 L'approche générale sécuritaire	8
32 L'identification et l'intégrité par la signature électronique	8
<i>4- La Protection globale du DRM – Le rôle de la signature électronique</i>	10
41 Approche du concept de Gestion des Droits Numériques.....	10
411 Définition et effets attendus.....	10
412 L'architecture technique du DRM	11
42 Le DRM et la protection des utilisateurs.....	12
421 Les risques pesant sur les droits individuels des utilisateurs	12
422 L'avis du CSPLA	12
43 L'apport de la signature électronique	13
431 Le pseudonyme dans la Directive Signature Electronique	13
432 Le pseudonyme dans la réglementation française sur la signature électronique	14
<i>Glossaire</i>	15
<i>Bibliographie</i>	15

¹ La signature électronique des juristes correspond au concept technique appelé *signature numérique*. Standardisée au niveau international, elle est décrite et connue sous le nom de "*digital signature*". Cette signature est définie par la norme ISO 7498-2 de la façon suivante : "*Données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données permettant à un destinataire de prouver la source et l'intégrité de cette unité en la protégeant contre la contrefaçon (par le destinataire par exemple)*".

2 LES BESOINS ET LE CONTEXTE D'UTILISATION

21 La notion d'œuvre numérique

Par numérisation d'une œuvre, il faut entendre la technique consistant à traduire le signal analogique qu'elle constitue en un mode numérique ou binaire qui représente l'information dans un symbole à deux valeurs ou une dont l'unité est le bit.

L'œuvre numérique peut être qualifiée d'œuvre de l'esprit dans la mesure où elle est le résultat d'une activité créative s'exprimant dans une forme extérieure indépendamment du support (conception retenue par Lucas). Cela conduit à écarter du champ d'application du droit d'auteur, la mise en œuvre d'un simple savoir-faire ou d'un processus entièrement automatisé. La notion de "forme extérieure" doit être entendue dans un sens large, l'intangibilité de l'œuvre n'étant pas une condition de protection de l'œuvre.

22 La propriété intellectuelle et la protection de l'œuvre numérique

Peu importe la nature du support de l'œuvre car selon l'article L111-1 Code de Propriété Intellectuelle, l'auteur jouit d'un monopole sur son œuvre du seul fait de sa création ; et l'exigence de concrétisation n'implique pas celle de fixation (ex : enregistrement d'un programme d'ordinateur sur une mémoire morte). En l'état actuel de la technique, c'est toujours une personne physique qui est à l'origine de l'œuvre résultante, d'où la protection de l'œuvre numérique par le droit d'auteur.

De nouveaux types d'œuvres peuvent toutefois soulever des interrogations. C'est le cas des pages Web et des liens hypertextes. Concernant les pages Web, la question qui se pose est de savoir si elles sont l'expression d'un effort de créativité suffisant pour être protégé par le droit d'auteur. La page Web pourra être qualifiée d'œuvre dès lors qu'elle résulte d'un arrangement particulier et original d'éléments de différentes natures ; cette appréciation se fera donc au cas par cas.

Le même type de réponse peut être avancée concernant les liens hypertextes, certains pouvant être couverts par l'exception de courte citation (article L122-5 3^{ème} Code de Propriété Intellectuelle), d'autres couverts par le droit d'auteur s'ils sont organisés de façon particulière dont la construction est l'expression d'une création intellectuelle. A cet égard, un site Web faisant figurer un lien hypertexte devrait préalablement recueillir le consentement du site concerné. La jurisprudence distingue toutefois le lien simple (qui ne nécessite pas d'autorisation), et le lien profond qui selon le cas nécessite que le titulaire du site vers lequel il dirige en soit informé.

Les articles L122-2 et L122-3 du code de la Propriété Intellectuelle confèrent à l'auteur les droits exclusifs d'autoriser la représentation et la reproduction de son œuvre :

- L'article L122-2 définit la représentation comme «*la communication de l'œuvre au public par un procédé quelconque*». Le vecteur permettant la représentation est aussi indifférent que le support pour le droit de reproduction et il n'y a pas lieu de distinguer selon les moyens techniques utilisés pour établir la relation entre l'œuvre et public. La seule exigence est celle d'une communication au public.
- L'article L122-3 du code de la propriété intellectuelle définit la reproduction comme «*une fixation matérielle de l'œuvre par tous procédés qui permettent de la communiquer au*

public d'une manière indirecte », ce qui est assez large pour viser tous les supports permettant les enregistrements numériques.

- Selon l'article L122-5 du code de la propriété intellectuelle, « *l'auteur d'une œuvre divulguée ne peut interdire les représentations gratuites et privées effectuées dans un cercle de famille, ni les copies ou reproduction réservées à l'usage privé du copiste et non destinées à une utilisation collective* ».

Mais cette exception pose un certain nombre de problèmes concernant la copie privée numérique. En effet la technologie numérique rend la copie beaucoup plus aisée et la copie devient un « clone » de l'œuvre originale. A cet égard l'avant projet de loi relatif au droit d'auteur et aux droits voisins dans la société de l'information, crée un article L331-5 qui prévoit que l'auteur d'une œuvre autre qu'un logiciel peut mettre en place des mesures techniques de protection des droits qui leur sont reconnus.

Ainsi les procédés anti-copie deviendraient légaux et empêcheraient la copie privée de l'œuvre numérique par l'utilisateur s'étant procuré l'œuvre d'une manière licite, en assimilant à la contrefaçon le fait de « porter atteinte », « de fabriquer, d'importer ou de mettre à disposition » ou de « faire connaître » toute technologie ou moyen conçu pour annuler ces protections. L'exception au droit d'auteur que constitue la copie privée disparaîtrait alors et c'est pour cette raison que les opposants aux dispositions de l'avant projet de loi demandent que la copie privée devienne un droit pour l'utilisateur.

Les mesures techniques destinées à empêcher la copie numérique et sa diffusion sont le marquage et le cryptage.

- L'article 11 du Traité de l'OMPI sur le droit d'auteur de 12/96 impose aux Etats de prévoir des sanctions juridiques contre la neutralisation des mesures techniques efficaces qui visent à protéger les œuvres d'actes non autorisés par leurs auteurs ou non permis par la loi.
- L'article 12 du même traité demande aux Etats de prévoir des sanctions juridiques appropriées et efficaces contre toute personne qui tenterait de supprimer ou de modifier sans y être autorisée l'information relative au régime des droits se présentant sous forme électronique, et contre toute personne distribuant, ayant importé aux fins de distribution, radiodiffusion ou communication au public des œuvres en sachant que les informations relatives au régime des droits se présentant sous forme électronique ont été supprimées ou modifiées sans autorisation.

La directive sur la société de l'information du 22 mai 2001 prévoit que les mesures techniques sont efficaces lorsque :

« L'utilisation d'une œuvre protégée ou celle d'un autre objet protégé est contrôlée par les titulaires du droit grâce à l'application d'un code d'accès ou d'un procédé de protection tel que le cryptage, le brouillage ou toute autre transformation de l'œuvre ou de l'objet protégé d'un mécanisme de contrôle de copie qui atteint cet objectif de protection ».

L'avant projet de loi relatif au droit d'auteur et aux droits voisins dans la société de l'information qui transpose la directive du 22 mai 2001, outre la mise en place de mesures techniques portant atteinte à la copie privée numérique, transpose l'article 5.1 de la directive.

Il prévoit ainsi que les fixations provisoires qu'implique la circulation d'une œuvre sur les réseaux numériques ou son utilisation par le destinataire final à travers son ordinateur,

échappent au droit de reproduction (ajout d'un 6^{ème} à L122-5 du code de la propriété intellectuelle). Cette exception couvre les actes de reproduction provisoire qui sont transitoires ou accessoires et constituent une partie intégrante et essentielle d'un procédé technique, ayant pour unique finalité de permettre :

"Une transmission dans un réseau entre tiers par un intermédiaire ou une utilisation licite d'une œuvre ou d'un objet protégé, à condition que ces actes n'aient pas de signification économique indépendante."

Les rédacteurs du texte ont retenu une approche assez favorable aux utilisateurs puisqu'ils se prononcent sur cette base pour la licéité du browsing (consistant pour l'internaute à se déplacer sur le réseau de site en site) et du caching (forme de stockage temporaire dans la mémoire cache des serveurs).

La protection des œuvres numériques pourrait également être accordée par le droit des dessins et modèles. Le critère pour que la protection soit accordée est la nouveauté :

- Il faut apprécier l'œuvre dans son ensemble pour dire si elle est nouvelle et non en séparant chaque élément.
- Il faut que l'œuvre ait un caractère apparent résultant de sa forme indépendante d'un procédé de fabrication (pas de résultat dû au hasard ou à un effet mécanique quelconque).
- Il faut également que l'œuvre ne soit pas similaire dans sa forme à une œuvre antérieurement protégée par le droit des dessins et modèles.

La protection pourrait également être recherchée par le droit des marques :

- Il faut que le signe choisi à titre de marque ait un caractère distinctif (et non générique ni descriptif),
- Il faut qu'il soit disponible (c'est à dire non déjà déposé à titre de marque),
- Il faut que le signe choisi à titre de marque ait un caractère licite (article L711-3 code de la propriété intellectuelle : pas contraire à l'ordre public ou aux bonnes mœurs, pas de signe trompeur, frauduleux ou déceptifs).

23 La protection des e-services et des formulaires électroniques

Sous l'impulsion de la communauté européenne, la France comme d'autres pays membres s'est engagée dans un programme de e-gouvernement. Les objectifs de ce programme sont multiples : recentrage des services publics sur les préoccupations des citoyens, amélioration de l'efficacité au regard des nouveaux enjeux qui se profilent : papy-boom des fonctionnaires, contraintes budgétaires, réduction du temps de travail, obligations de résultats (ordonnance de 1959 revue par loi LOLF). Pour atteindre ces objectifs, l'administration française a mis à profit les dernières avancées technologiques comme l'Internet, le téléphone mobile pour offrir de nouveaux services aux usagers.

Les systèmes d'information des ministères se recentrent progressivement sur la problématique des usagers et leurs portails d'accueil tendent à présenter un compte simplifié à chacun des citoyens. Des téléprocédures se mettent aussi en place qui permettent de dématérialiser les échanges entre les citoyens et l'administration.

Mais par soucis d'égalité entre les usagers, L'Etat doit s'assurer à ce que les nouveaux services en ligne ne remettent pas en cause les services traditionnels existant et que le niveau de qualité des services reste le même quelque soit le mode proposé.

De plus, un usager doit avoir la faculté d'initier une procédure en ligne et de la terminer selon un mode classique. Par exemple retirer un formulaire en ligne, le remplir, l'imprimer et ensuite le transmettre par voie postale.

La juxtaposition de ces deux modes d'échanges (électronique et papier) n'est pas sans poser des problèmes ou tout du moins des questions.

Par exemple, Ne doit-on pas utiliser des moyens cryptographiques pour garantir que des informations imprimées issues d'un compte simplifié soient fidèles à la version électronique et que l'administration puisse être reconnue comme étant l'auteur de ces informations ?

Si le besoin était avéré de prouver la paternité d'un document imprimé depuis un site, quels seraient les moyens cryptographiques nécessaires ?

Quels seraient aussi les moyens nécessaires pour montrer le lien entre une version électronique et papier d'un même document ?

3- LES MOYENS DE PROTECTION ACTUELS ET L'APPROCHE SECURITAIRE

31 L'approche générale sécuritaire

Les besoins généraux en termes de sécurité des échanges électroniques sont la confidentialité, l'identification, l'intégrité le droit d'accès. Il convient d'exposer leur signification dans un contexte de transmission d'œuvres numériques

Ces besoins de sécurité sont satisfaits par des moyens techniques mettant en œuvre des techniques cryptographiques dont l'usage est resté longtemps étroitement encadré par la loi².

Le besoin de confidentialité s'exprime par un objectif unique : « s'assurer qu'une entité non autorisée, le plus souvent une personne, ne pourra pas prendre connaissance de certaines informations ». Ce besoin simple peut être mis en œuvre de façons variées en utilisant des mécanismes appropriés au contexte auquel ils s'appliquent. Le service de confidentialité peut être motivé pour les raisons suivantes :

- Respect de la vie privée (dans ou en dehors de tout cadre légal)
- Respect du secret médical
- Confidentialité commerciale ou concurrentielle
- La sécurité nationale

En ce qui concerne le domaine commercial et concurrentiel, le besoin de confidentialité est réel pour la catégorie de données concernant la vie de l'entreprise et dont la divulgation non contrôlée peut lui porter préjudice. On peut citer à ce titre des données structurelles ou opérationnelles comme des fichiers de prospects, des prix de revient, des négociations commerciales, etc. Il faut classer également dans cette catégorie le savoir-faire de l'entreprise comme des formules de produits, des procédés de fabrication, des schémas etc. Mais il ne faut pas oublier non plus des données qui peuvent revêtir un caractère sensible au sein même de l'entreprise comme des données relatives à la gestion du personnel qui pourraient être utiles dans des négociations sociales internes.

Dérivé du précédent quoique plus spécifique, le besoin opérationnel de confidentialité concerne la diffusion d'informations payantes comme du logiciel, des images ou des émissions télévisuelles numériques en paiement à la carte (Pay per view). Des sociétés tirent leur chiffre d'affaires de la vente en ligne de ces produits, il est donc essentiel que ces produits ne puissent être accessibles qu'aux utilisateurs ayant payé la redevance associée.

32 L'identification et l'intégrité par la signature électronique

Au préalable, il sera rappelé qu'il existe sur le marché des procédés de protection classiques pour les oeuvres numériques comme *sténographie* et le tatouage numérique ou *watermarking*. Le lecteur intéressé est invité à se reporter au Web pour y trouver toute l'information nécessaire.

² L'usage de la cryptologie a longtemps été réservé au monde militaire et assimilé. Son emploi dans les télécommunications a cependant été admis dès la loi de réforme des télécommunications du 29 décembre 1990. Assoupli au cours du temps par divers textes, le régime de la cryptologie devrait être encore considérablement allégé à l'occasion de l'adoption de la Loi sur la confiance dans l'économie numérique (LCEN).

En prenant pour base la "*digital signature*" des techniciens, les juristes de l'American Bar Association ont émis les premières réflexions tendant à l'implémentation de la signature technique dans un environnement juridique³. Des initiatives de même nature sont apparues dans de nombreux pays du monde. En Europe, les instances communautaires ont adopté une Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques⁴, texte qui a été transposé en droit français par la Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique⁵.

Depuis cette loi, la signature électronique est intégrée dans le Code civil sous un article 1316-4 qui déclare :

"La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.

Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat. "

La signature électronique est mentionnée dans l'alinéa 2 de l'article 1316-4. On retrouve dans le texte le renvoi aux deux garanties de sécurité, identification et intégrité, qui nous ont permis de retenir la signature électronique comme moyen de protection des oeuvres numériques. L'alinéa 1 quant à lui fixe les caractéristiques légales de la signature quelle que soit sa modalité, signature écrite (manuelle) et signature électronique. A cet égard, on note deux caractéristiques qui ne correspondent pas à ce que nous recherchons :

- d'une part, la signature est apposée sur un acte juridique,
- d'autre part, elle manifeste le consentement du signataire quant au contenu de l'acte.

Une œuvre, numérique ou non, n'est pas en soi un acte juridique. C'est plutôt un fait juridique auquel le droit accorde une protection particulière. Dans ces conditions, la signature électronique du Code Civil n'est pas l'instrument qu'il faut retenir pour la protection des oeuvres numériques. Les garanties sécuritaires de l'instrument sont au contraire tout à fait appropriées. Il en résulte que la signature électronique peut être retenue en négligeant ses aspects proprement juridiques se signature. En d'autres termes, c'est la signature numérique des techniciens qui sera préférée.

³ Voir le rapport "Digital Signature Guidelines" qui incorpore également l'US Model Digital Signature Law publié en 1995 par l'ABA. Les Guidelines sont téléchargeables sur le site de l'ABA : www.abanet.org/scitech

⁴ JOCE du 17.1.2002 n°L 15/24

⁵ JO du 14 mars 2000 p. 3968

4- LA PROTECTION GLOBALE DU DRM – LE ROLE DE LA SIGNATURE ELECTRONIQUE

41 Approche du concept de Gestion des Droits Numériques

411 Définition et effets attendus

La DRM⁶, acronyme de *Digital Rights Management*, permet de diffuser des contenus sonores, textuels, etc. par voie numérique tout en protégeant les droits d'auteur associés. La DRM est issue d'un constat très simple : les supports numériques sont particulièrement propices à la copie : il suffit d'un clic de souris pour dupliquer le contenu d'un fichier sur un autre support. D'où l'intérêt de chiffrer ces fichiers en mode natif, pour qu'on ne puisse les lire qu'avec un lecteur adapté et sécurisé. La santé de l'édition est étroitement liée aux performances des solutions de DRM hors desquelles il deviendra rapidement risqué - voir inconscient - de pousser des médias vers un ordinateur.

Parmi les mesures de sécurisation, toute plate-forme de type Palladium⁷ permettra de déployer une "gestion numérique des droits" (Digital Rights Management – DRM, au cas par cas, sur chaque PC. Tous les médias sont concernés à partir du moment où ils peuvent être diffusés sous forme numérique. A commencer par le son, qui est à l'heure actuelle le premier marché de la DRM. Loin derrière, la vidéo attend patiemment son heure, suivie par la protection des images et celle des textes. Au demeurant, dans son acception la plus large, la protection des droits numériques inclut d'autres types de fichiers : les contrats, les documents scientifiques et les logiciels, même s'ils ne sont pas à proprement parler des médias mais plutôt des productions entrant sous le couvert de la propriété intellectuelle.

L'utilisation des logiciels pourrait évoluer grâce au DRM. Il ne sera plus possible d'utiliser des logiciels sans posséder la licence correspondante. Les logiciels utilisés sans droits pourront être détectés et même effacés à distance. Par contre, la location de logiciels et l'ASP seront facilités. Mais faute du paiement du loyer, non seulement le logiciel ne fonctionnera plus mais peut-être également les fichiers de données qu'il aura servi à créer. Ce type de protection des droits d'auteur pourrait montrer des effets pervers dans le droit de la concurrence. Les éditeurs de logiciels pourraient aussi rendre plus difficile le passage vers les produits de leurs concurrents. Pour la musique et les films en ligne, les maisons de disques pourront vendre de la musique en ligne. Mais les fichiers ne pourront ni être copiés ni échangés et leur écoute pourrait être limitée à un certain de fois.

Microsoft ne reste pas étranger à ce mouvement. Dans sa prochaine version, Office devrait intégrer pour la première fois un système de gestion des droits numériques. Un dispositif qui permettra aux utilisateurs de définir des règles d'accès suite à la création d'un document.

⁶ D'après DRM et gestion des droits numériques : http://solutions.journaldunet.com/0212/021203_drm.shtml

⁷ *Palladium* ou *Next-Generation Secure Computing Base* est un logiciel que Microsoft déclare vouloir incorporer dans les futures versions de Windows et qui s'installera sur des machines de type TCPA. *Trusted Computing Platform Alliance* (TCPA), est un projet développé par Intel, une "alliance pour une informatique de confiance". TCPA fournit un composant de surveillance à insérer dans futurs PC, un circuit intégré ou un périphérique *dongle* soudé à la carte mère appelé *Fritz*. Cette puce vérifie que le PC a démarré dans un "état de confiance" bien déterminé, avec une combinaison de matériels approuvés et de logiciels dont les licences d'utilisation sont en cours de validité. Le contrôle est ensuite transféré à un logiciel de surveillance du système d'exploitation, *Palladium* (pour les dos de type Windows).

Proche du DRM, cette nouvelle couche s'applique exclusivement au format Windows Media, cet outil cible de son côté les producteurs et diffuseurs de contenus audio et vidéo, c'est-à-dire les maisons de production et les grands média principalement. Qualifié de logiciel d'IRM (pour Information Rights Management), le nouveau module d'Office avance de nombreuses fonctions d'administration⁸. Il permettrait de définir des niveaux de restriction touchant à l'ensemble des documents de la suite bureautique (Excel, Word et PowerPoint). Au programme : la possibilité de lier des utilisateurs à des droits particuliers (lecture, modification, impression, etc.) ou encore d'empêcher l'ouverture d'un fichier au delà d'une certaine date. La mise en oeuvre de ces fonctions devrait nécessiter l'installation d'un logiciel client particulier (Windows Rights Management Services) mais aussi le déploiement du serveur de Microsoft dans sa dernière version (Windows Server 2003). Le rôle de cette seconde brique ? Elle a pour but de centraliser les règles définies par les créateurs de contenus en vue de gérer les demandes d'accès (exécutées en mode client/serveur) et accorder les permissions.

Le DRM pourrait avoir des effets positifs en influençant les comportements, ainsi :

- Tricher aux jeux sur ordinateurs sera plus difficile ;
- Le spamming sera supprimé ou considérablement diminué ;
- Certains sites ou services pourraient obliger les internautes à n'employer que des logiciels accrédités, par exemple, il ne serait plus possible d'enchérir de manière tactique sur les sites d'enchères ;
- La confidentialité serait plus facilement garantie : les textes créés sur traitement de texte pourraient se voir revêtus d'une mention "confidentiel" pour les entreprises ou d'une mention "secret défense" pour certaines administrations, le système empêchant toutes les fuites.

A l'opposé, certains aspects négatifs sont à craindre, telle la censure en ligne. Les mécanismes conçus pour effacer à distance des logiciels ou des fichiers multimédia piratés pourraient être utilisés pour effacer des documents qu'un prétendu auteur (qu'un tribunal ?) aurait déclaré contrefaits, injurieux, préjudiciables, ou encore pornographies ou politiquement incorrects... Quant à l'IRM de la future version d'Office (Microsoft), jusqu'à ce jour, il était toujours envisageable d'ouvrir un fichier Office au sein d'une version antérieure de la suite ou encore depuis des outils bureautiques tiers, tels que des applicatifs StarOffice (Sun) ou OpenOffice (projet Open Source). Dans Office 2003, les documents sous couvert du mécanisme d'IRM ne devraient plus être exploitables dans ces environnements...

412 L'architecture technique du DRM

Un système de DRM se décompose en quatre composants :

- L'*encodeur* qui transforme les fichiers traditionnels en fichiers chiffrés, tout en les compressant à la volée dans de nombreux cas.
- Le *serveur de streaming* qui diffuse les fichiers transformés sur Internet par l'intermédiaire
- Le *player* est le composant situé sur le PC du client qui doit être capable de déchiffrer le fichier reçu et de le diffuser. C'est le composant le plus problématique, car les progrès constants de l'encodage nécessitent de fréquentes mises à jour. Or, tout téléchargement est un facteur dissuasif du côté du client.
- Enfin le *gestionnaire de droits* qui couvre toute la chaîne de l'édition et de la diffusion. Il permet de spécifier à qui reviennent les droits, selon quelle répartition (pour chaque

⁸ D'après http://solutions.journaldunet.com/0309/030904_microsoft.shtml

modèle de diffusion), qui permet de vérifier si le client respecte bien les modalités du contrat et de piloter tout ce qui est relatif à la gestion de la chaîne de diffusion

Le mode de fonctionnement du gestionnaire de droits appelle quelques réserves au niveau des libertés individuelles.

42 Le DRM et la protection des utilisateurs

421 Les risques pesant sur les droits individuels des utilisateurs

S'agissant du DRM, le Forum des Droits de l'Internet note que ces outils informatiques peuvent revêtir plusieurs formes. Il peut ainsi s'agir de protections techniques destinées à garantir que l'utilisation qui sera faite de l'œuvre correspond aux autorisations données par le titulaire de droits lors du téléchargement du fichier. A côté de cette utilisation qui demeure la plus connue, les DRM peuvent également servir à subordonner l'accès à une œuvre ou sa reproduction à l'utilisation par le consommateur d'un système d'identification communiqué au prestataire. De même, une autre technique peut consister à obliger l'utilisateur, chaque fois qu'il souhaite utiliser une œuvre, à se connecter au site d'un prestataire pour prouver son identité.

Compte tenu de ces utilisations, la commission "libertés individuelles" du Conseil Supérieur de la Propriété Littéraire et Artistique⁹ (CSPLA) relève qu'une partie des personnes auditionnées met en avant quatre types de risques pour la protection de la vie privée, n'étant visés que ceux résultant de pratiques légales. Ainsi, les DRM pourraient permettre "*de connaître de façon très précise des pans entiers de la vie privée des individus*", "*de collecter des données allant au-delà de ce qui est simplement nécessaire à l'exercice des droits de la propriété littéraire et artistique*", d'être "*couplées avec [les informations] rassemblées sur d'autres sites grâce à des systèmes d'identifiants uniques, tel que celui du système .NET Passport développé par Microsoft*", et poseraient des problèmes en cas de rachat de sociétés, permettant à ces dernières de constituer des "fichiers portant sur un grand nombre de caractéristiques".

422 L'avis du CSPLA

Saisi par le ministre de la culture et de la communication de la question de la conciliation entre la protection des droits de propriété littéraire et artistique et le respect des libertés individuelles, le CSPLA a adopté, lors de sa séance du 26 juin 2003, un avis¹⁰ n°2003-1 relatif à la propriété littéraire et artistique et libertés individuelles où on peut relever le point de vue suivant¹¹ :

⁹ Le CSPLA est issu du rapport au Premier ministre du député Patrick Bloche, *Le désir de France*, qui proposait de "*créer, auprès du ministère de la culture et de la communication, une instance de médiation pour les questions de propriété intellectuelle liées à la société de l'information et plus particulièrement à l'internet, assisté d'un conseil scientifique composé de juristes et de représentants des différents acteurs*". Le Conseil a été créé par un arrêté du Ministre de la Culture du 10 juillet 2000, l'organisation fixées et les membres nommés par les arrêtés du 30 avril 2001 et du 27 février 2002.

¹⁰ Le président du CSPLA rend compte des travaux du conseil au Ministre de la culture et de la communication par voie d'avis écrits dont il lui est accusé réception et par l'établissement d'un rapport annuel.

¹¹ <http://www.culture.gouv.fr/culture/cspla/avislibertes.htm>

2. Pour certains, les systèmes numériques de gestion des droits pourraient entraîner des atteintes à la vie privée, en permettant la collecte et le traitement de données personnelles à l'insu des personnes concernées. Le Conseil supérieur souligne toutefois que ces systèmes s'inscrivent dans le cadre général du commerce électronique et des règles, y compris pénales, applicables en matière de protection des données personnelles. A cet égard, les obligations figurant dans la directive du 24 octobre 1995, qui est à l'origine du réexamen actuel par le Parlement de la loi n° 78-17 du 6 janvier 1978, semblent de nature à compléter le dispositif actuel et à assurer le respect de la protection des données personnelles par les systèmes numériques de gestion des droits. La transposition de cette directive devrait permettre selon toute vraisemblance de préserver les avantages que ces systèmes représentent tant pour les usagers que les ayants droit.

43 L'apport de la signature électronique

La notion de signature électronique telle que définie plus haut est insuffisante et pourrait se révéler inadaptée à la vérification passé un certain laps de temps. Cette opinion¹² énoncée dans un contexte purement technique est très préoccupante au regard des questions juridiques. Un organisme comme l'ETSI a développé une définition plus riche et plus complexe que les définitions traditionnelles :

"Signature électronique : indice sous forme numérique qui peut être traité afin d'avoir confiance en ce qu'un événement ou une action a été explicitement reconnu sous une politique de signature, à un instant donné, par un signataire sous un identifiant (par exemple un nom ou un pseudonyme, et optionnellement un rôle)".

On voit ici la notion de pseudonyme prendre place aux côtés du nom.

431 Le pseudonyme dans la Directive Signature Electronique

Le document COM503 de la Commission envisage l'éventualité du pseudonyme dans le certificat. La Directive européenne a adhéré à ce principe. Son article 25 indiquait :

"Il convient que les dispositions relatives à l'utilisation de pseudonymes dans des certificats n'empêchent pas les Etats membres de réclamer l'identification des personnes conformément au droit communautaire ou national".

L'éventualité du pseudo est prévue par l'annexe I de la Directive qui liste les exigences applicables aux certificats en termes d'informations à inclure. : "c- le nom du signataire ou un pseudonyme qui est identifié comme tel". La légitimité de l'emploi d'un pseudonyme se réfère comme dit plus haut à la protection des données. La Directive indique dans son article 8 *Protection des données* :

"3. Sans préjudice des effets juridiques donnés aux pseudonymes par la législation nationale, les Etats membres ne peuvent empêcher le prestataire de service de certification d'indiquer dans le certificat un pseudonyme au lieu du nom du signataire".

¹² Cf. "Comprendre la différence entre signature électronique et numérique" par PINKAS Denis. Le texte a été diffusé sur le Web et par écrit (Actes de la conférence Trusting Electronic Trade'99 à Marseille).

432 Le pseudonyme dans la réglementation française sur la signature électronique

Le troisième alinéa de l'article 1316-4 du Code civil indique que l'identité du signataire doit être assurée, renvoyant à un décret en Conseil d'Etat pour en fixer les conditions. Le décret¹³ d'application donne mission au PSCE de contrôler l'identité. Le point 6-II-m du décret dispose que le PSCE doit "*vérifier (...) l'identité de la personne à laquelle un certificat électronique est délivré, en exigeant d'elle la présentation d'un document officiel d'identité*". Suite à cette vérification et à quelques autres contrôles, le PSCE pourra inscrire l'identité du signataire ainsi que la clé publique de celui-ci dans le certificat électronique à émettre. Et pourtant, on notera que l'article 6-I qui liste les informations qui doivent être contenues dans le certificat indique au titre de l'identité dans le point C seulement le "*nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel*".

A ce point de l'étude, cette lecture du décret permet de revenir sur une erreur fréquente chez les utilisateurs de signature, comme chez les PSCE qui s'inquiètent d'endosser une responsabilité professionnelle que la loi ne leur impose pas. Le rôle du PSCE n'est pas de garantir l'identité d'état civil d'une personne, mais de garantir l'identité, authentifier, qui lui est présentée, serait-elle un simple pseudonyme. Est-ce à dire que l'assurance de l'identité du signataire par le PSCE est fort aléatoire et n'apporte aucune sécurité aux destinataires d'écrit électronique signé ? Non, car même si le certificat n'est émis qu'au titre d'un pseudonyme, clairement énoncé comme tel il faut le rappeler, le PSCE connaît, lui, l'identité réelle sans doute d'état civil, car il aura obtenu du demandeur de certificat "*la présentation d'un document officiel d'identité*" (art.6.II-m).

¹³ Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique modifié par l'article 20 du Décret no 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

GLOSSAIRE

Confidentialité : Propriété qui assure la tenue secrète des informations avec accès aux seules entités autorisées. Elle est assurée par les techniques de chiffrement.

Cryptographie : Discipline incluant les principes, moyens et méthodes de transformation des données, pour cacher leur contenu sémantique, pour empêcher leur utilisation non autorisée ou pour permettre la détection des modifications.

La cryptographie conçoit des algorithmes que l'on souhaite inviolables.

Cryptologie : Science du chiffrement

Identification : Opération de vérification consistant à s'assurer sans ambiguïté de l'identité de l'utilisateur d'un service.

Intégrité : Propriété assurant que des données n'ont pas été modifiées, insérées ou détruites de façon non autorisée.

Signature électronique (ordinaire) de la Directive Européenne : Donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification.

Signature électronique sécurisée : Signature établie grâce à un dispositif sécurisé (mise en œuvre d'une clé privée) et dont la vérification repose sur l'utilisation d'un certificat électronique.

Stéganographie : Technique de chiffrement qui consiste à cacher des messages secrets au sein de messages anodins, qui peuvent être rendus publics.

Tatouage numérique (en anglais : watermarking) : Technique de marquage qui consiste à insérer une signature invisible et permanente à l'intérieur des images numériques transitant par les réseaux, tel Internet, afin de lutter contre la fraude, le piratage et d'assurer la protection des droits de propriété intellectuelle.

BIBLIOGRAPHIE

- *Le Livre Vert sur le copyright et les droits associés au sein de la société de l'information*, Publications de l'Union Européenne, 1991
- *Le rapport Bangemann*, Publications de l'Union Européenne¹⁴, 1994
- *Les systèmes de protection électronique de droits d'auteurs de documents numériques*, par Edmond F. KOUKA
- *Technologies de sécurité pour les médias digitaux - Rapport Final*, Parlement européen, par Franck LEPRÉVOST, Université de Grenoble et Bertrand WARUSFEL, Université de Paris V, mai 2001 (PE 296.705)
- *Mesures techniques de protection des oeuvres & DRMS – Un état des lieux janvier 2003*, par Philippe CHANTEPIE, Marc HERUBEL, Frank TARRIER, Ministère de la Culture, rapport n°2003-02.

¹⁴ Nom du Commissaire en charge du marché intérieur 1990-1995. Le "Rapport sur L'Europe et la Société de l'information planétaire ", du 26 mai 1994, préparé par un groupe d'industriels, plus connu sous le nom de Rapport Bangemann. Ce rapport consacrait une approche libérale de la convergence, considérant la politique de la concurrence comme essentielle pour consolider le marché unique et attirer les capitaux privés nécessaires à la croissance et à l'infrastructure transeuropéenne de l'information. Il recommandait de poursuivre la création d'une industrie audiovisuelle européenne libéralisée et compétitive.