

## ARIANE DELVOIE, AVOCAT À LA COUR, CABINET BENSOUSSAN

### La protection du logiciel au cœur de l'architecture DRM



Ariane Delvoie

La protection accordée au dispositif technique de verrou et de traçage d'une œuvre, notamment par le biais du projet de loi DADVSI, est-elle efficace et nécessaire au regard des autres modes de protection des logiciels ?

L'implémentation des logiciels dans les techniques n'a cessé de croître depuis vingt ans. Une des plus récentes applications est celle des technologies DRM (Digital Rights Management), conçues pour protéger les titulaires des droits d'une œuvre éditée sur support numérique. Pour remplir cet objectif, l'architecture DRM suppose :

- un cryptage des données de l'œuvre ;
- l'installation d'un logiciel sur le support numérique de l'œuvre (un CD) qui tracera les utilisations et éventuellement, les bloquera ;
- un lecteur qui contient un système de décryptage des données et se connecte avec un serveur qui vérifiera si l'accès aux données est autorisé ou non et enregistrera les utilisations faites de l'œuvre.

Or, le logiciel qui, au cœur de l'architecture DRM, a la double fonction de verrou et de traçage, peut lui-même protéger une œuvre logicielle, ce qui n'est pas sans conséquence quant aux réglementations applicables.

Les architectures DRM, appelées « mesures techniques de protection efficaces des œuvres », ont tout d'abord été consacrées au niveau international par les Traités de l'OMPI en 1996, puis, aux Etats-Unis par le Digital Millennium Copyright Act (DMCA) de 1998, puis au niveau de l'Union Européenne avec la Directive du 22 mai 2001 qui a inséré des dispositions relativement similaires à celles figurant dans le DMCA.

En France, le processus de réglementation a été plus progressif. Certes, les dispositifs de protection sont envisagés à l'article L.122-6-2 du code de propriété intellectuelle, mais ne visent que ceux qui ont pour objet de protéger une œuvre logicielle. Pour les œuvres autres que logicielles, la réglementation des dispositifs de protection est un des objets du projet de loi dit DADVSI (relatif aux droits d'auteur et aux droits voisins dans la société de l'information), actuellement examiné auprès d'une commission mixte paritaire composée de sept députés et sept sénateurs.

Toute la question est de savoir si la protection du logiciel en tant que dispositif technique de verrou et de traçage d'une œuvre est utile au regard des autres modes de protection existants, à savoir :

- le droit des marques pour la dénomination du logiciel à condition de démontrer une antériorité et de procéder à un dépôt auprès de l'INPI ;
- le droit d'auteur, si l'originalité est démontrée et si la protection concerne uniquement le programme (code source et code objet), la documentation technique, le matériel de conception préparatoire (dossier des spécifications externes, spécifications internes, dossiers de programmation, maquette, prototype), la documentation d'utilisation, ainsi que le « look » (présentation, pages écran, etc..) ; en revanche, le « feel » (exemple : les schémas d'arborescence) est exclu de ce type de protection ;
- le droit des brevets pour l'ensemble du dispositif auquel est intégré le logiciel et à conditions de démontrer la nouveauté et son caractère inventif ainsi que de procéder à un dépôt aux différents offices de brevets dans les pays prévisibles d'exploitation ;
- la concurrence déloyale, uniquement en cas de contrefaçon et de démonstration d'une faute ainsi que d'un préjudice subi.

Les limites de ces modes de protection peuvent-elles être comblées par la protection accordée au dispositif technique de verrou et de traçage d'une œuvre ? Le code de propriété intellectuelle français ne visait jusqu'à présent que les dispositifs techniques destinés à protéger les œuvres logicielles et n'interdisait nullement la fabrication, commercialisation ou

mise à disposition de logiciels de « déplombage » de mesures techniques de protection d'une œuvre logicielle, à la condition toutefois que la publicité relative à ces outils mentionne que leur utilisation illicite est constitutive d'une contrefaçon.

Quant aux actes de contournement des logiciels de « déplombage », ils sont identifiés à des actes de contrefaçon par le code de propriété intellectuelle français sauf en cas d'utilisation licite du logiciel, ce qui renvoie directement à l'article L.122-6-1 du même code<sup>(1)</sup>. Le projet de loi français DADVSI, censé durcir et généraliser le régime relatif aux dispositifs techniques de protection des œuvres, présente certains paradoxes. Tout d'abord, s'il reprend les dispositions présentes à la fois dans le DMCA américain et dans la Directive Communautaire de 2001 précitées quant à l'interdiction de fabrication, commercialisation ou mise à disposition de dispositifs destinés à contourner les mesures techniques de protection d'une œuvre<sup>(2)</sup>, il n'étend nullement cette interdiction aux moyens de contournement des mesures de protection des œuvres logicielles. Ainsi, il reste parfaitement licite de fabriquer et de commercialiser des logiciels de « déplombage » d'œuvres logicielles, avec certes l'obligation de mentionner que seul l'utilisateur licite de l'œuvre logicielle peut utiliser ces logiciels de « déplombage ».

Autre paradoxe : si les actes de contournement des dispositifs de protection des œuvres autres que logicielles sont permis pour l'utilisateur légitime<sup>(3)</sup> de l'œuvre, à l'instar de ce qui est prévu pour les œuvres logicielles à l'article L.122-6-2, les sanctions pénales prévues pour les actes de contournement sont en revanche moins fortes quand il s'agit d'accéder à une œuvre quelconque que quand il s'agit d'accéder à une œuvre logicielle. En effet, quand l'accès à une œuvre logicielle est visé, le code de propriété intellectuelle prévoit l'application des sanctions pénales relatives aux actes de contrefaçon, c'est à dire trois ans d'emprisonnement et 300 000 euros d'amende<sup>(4)</sup>. Quand l'accès à une œuvre autre que logicielle est visé, l'Amendement 262 adopté dans le cadre du Projet de loi DADVSI prévoit :

- une simple contravention si la personne a utilisé un logiciel tiers (750 euros d'amende selon un décret à prendre en Conseil d'Etat) ;
- un délit que si la personne est un hacker qui a créé son propre moyen de contournement (3 750 euros d'amende).

Ces deux niveaux de répression ont probablement pour objet de faire peser davantage la responsabilité sur les fabricants de logiciels de « déplombage » que sur les utilisateurs de tels moyens de contournement. Les nombreuses exceptions et modérations aux interdictions de contournement des dispositifs techniques de verrou et de traçage d'œuvres de l'esprit peuvent amener à douter sur l'efficacité d'un tel mode de protection pour le titulaire des droits sur le dispositif en cause. ■

#### ANTI-DRM ET LOGICIEL LIBRE

Lors de la journée de protestation organisée le 9 juin 2006 contre les technologies DRM par le collectif StopDRM, est intervenu Richard Stallman, le gourou du logiciel libre. Il est le fondateur de l'organisation DefectiveBy Design, visant à dénoncer les abus possibles par les DRM aux droits des utilisateurs légitimes des œuvres de l'esprit. Dans le même esprit, le projet de nouvelle licence GPL relatif au logiciel libre prend ouvertement position contre les technologies DRM en interdisant toute mesure de protection logicielle à toute personne souscrivant ladite licence. (« GNU, General Public License, Discussion Draft of version 3 », 16 janvier 2006, <http://gplv3.fsf.org/gpl3-current.txt>).

(1) Ce qui signifie qu'il y aura contrefaçon si l'utilisateur de l'œuvre logicielle en cause n'est pas cessionnaire des droits d'utilisation, ou si le contournement du dispositif technique de protection a pour objet de réaliser des actes non permis par le titulaire des droits sur l'œuvre logicielle.

(2) Sauf dans certains buts louables : s'il s'agit de logiciels tels que la recherche, la sécurité collaboratif.

(3) Par rapport à l'article L.122-5 du code de propriété intellectuelle, et notamment par rapport au droit à la copie privée, ou pour certains buts louables tels que la recherche, la sécurité informatique ou l'interopérabilité. Voir « Les DRM habilités, la copie privée sacrifiée », Ariane Delvoie, L'Oeil Expert, Avril 2006.

(4) Article L.122-6-2 et L.335-2 du code de propriété intellectuelle