

nent l'autorisation de copier, de transférer ou de charger. Les droits d'interprétation concernent l'autorisation de jouer et d'imprimer. Les droits de reproduction concernent l'extraction d'information, l'édition de cette information et son insertion dans d'autres publications. D'autres droits régissent la création et l'utilisation des copies de sauvegarde.

La sécurisation à l'œuvre

Les exigences de sécurité variant avec la nature des œuvres intellectuelles, les systèmes sécurisés permettent aux éditeurs de définir le degré de maîtrise qu'ils veulent conserver sur les documents écrits, sonores ou vidéo. Les œuvres numériques les plus précieuses peuvent être protégées par des systèmes qui détectent toute tentative de déverrouillage, déclenchent alors des alarmes et effacent l'information abusivement utilisée. À un niveau inférieur, les systèmes sécurisés pourraient seulement éviter les tentatives d'effraction banales en demandant un mot de passe. À un niveau encore plus élémentaire, ils marqueraient seulement les œuvres d'une signature numérique, de sorte le propriétaire soit associé à son œuvre de façon indélébile (certains logiciels de manipulation d'images apposent déjà ce type de filigrane numérique).

La plupart des ordinateurs sécurisés savent reconnaître un autre système sécurisé, faire respecter les droits d'usage et présenter les œuvres de sorte qu'elles ne puissent être copiées exactement ou qu'elles contiennent constamment la marque de leur origine. Pour exécuter les transactions en toute sécurité, deux systèmes sécurisés utilisent un canal de communications, tel le réseau Internet, pour s'échanger des preuves de leurs identités. On peut ensuite gérer les communications sur un canal sécurisé à l'aide d'un cryptage et de ce que l'on nomme un protocole d'authentification.

Par exemple, si un ordinateur A veut communiquer

avec un ordinateur B, il doit prouver à B qu'il est un système sécurisé et que son identité est bien celle qu'il déclare sienne. L'interaction commence alors par l'envoi, de A à B, d'un certificat numérique qui confirme qu'il est enregistré en tant que système sécurisé. L'ordinateur B déchiffre alors ce certificat, mais il doit s'assurer que A est bien celui que le certificat atteste, et qu'il n'utilise pas frauduleusement un certificat volé : aussi, l'ordinateur B compose une chaîne de nombres aléatoires, qu'il chiffre à l'aide d'une clé publique contenue dans le certificat numérique envoyé par A. La clé publique permet à B d'envoyer des messages que seul A comprend lorsqu'il les déchiffre avec sa propre clé.

A doit ainsi déchiffrer le message renvoyé par B et retourner un message non chiffré contenant la chaîne aléatoire sélectionnée. Si la chaîne renvoyée en clair est bien celle qui avait été envoyée par B, ce dernier sait qu'il est en communication avec A, car seul A pouvait déchiffrer le message avec sa clé privée. Quelques étapes supplé-

mentaires permettent ensuite aux deux ordinateurs d'effectuer la transaction prévue, telle que le transfert d'un livre sous une forme numérique.

Les systèmes sécurisés n'utilisent pas tous un protocole d'authentification, mais la plupart échangent des œuvres sous une forme cryptée. Ils peuvent aussi comporter d'autres systèmes de sécurité : des horloges infalsifiables qui empêchent un utilisateur d'exercer des droits périmés ; des mémoires inviolables qui enregistrent les opérations financières ; des connexions permanentes avec un bureau central lors des transactions.

Les systèmes sécurisés peuvent placer des filigranes d'identification qui permettront de localiser des copies ou des modifications non autorisées. Ces filigranes enregistrent la désignation de l'œuvre, le nom de l'acheteur et le code des appareils sur lesquels l'œuvre est utilisée. Dissimulée dans les blancs d'un texte, une telle information ne gênerait pas les utilisateurs honnêtes, mais elle ne pourrait être effacée par les fraudeurs.

Les éditeurs devraient continuer à surveiller la diffusion non autorisée de leurs œuvres, car on pourra toujours photocopier une page que l'on aura imprimée, ou filmer un écran d'ordinateur à l'aide d'une caméra vidéo. En revanche, les systèmes sécurisés empêchent la diffusion à grande échelle de copies parfaites des originaux numériques. En outre, certains filigranes permettront de suivre à la trace les copies piratées.

Grâce à ces systèmes, les pratiques commerciales de l'édition numérique ne devraient guère différer de celles de la diffusion des œuvres imprimées. Supposez que Christian veuille acheter un livre numérique proposé par un éditeur du réseau Internet. La copie du livre résulte d'une transaction entre le système du vendeur et l'ordinateur de Christian ; lors de la transaction, Christian doit notamment utiliser sa carte de crédit ou son argent numérique pour payer l'exemplaire du livre qu'il lira sur son ordi-



1. ÉCOUTEZ AVANT D'ACHETER! Cette technique de vente pratiquée dans les magasins de disques pourrait apparaître sur le réseau Internet, grâce aux systèmes sécurisés, qui permettent de «tester» les œuvres numériques avant de les acheter.