

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.

nateur personnel ou sur tout autre dispositif de consultation. Toute la transaction, naturellement, est précédée d'un échange d'informations qui garantit au vendeur que la machine de Christian est sécurisée.

Applications des droits d'usage

Christian peut offrir son livre numérique comme il le ferait avec un livre papier : si son ami Jean-Baptiste lui demande le livre, Christian lui cède gratuitement ses droits, mais, à la fin de la transaction entre Christian et Jean-Baptiste, le livre se trouve sur le lecteur de ce dernier et il n'est plus sur celui de Christian. Jean-Baptiste peut alors lire le livre, et Christian ne le peut plus. Ainsi le nombre total d'exemplaires n'est pas modifié par le transfert ; les ordinateurs de Christian et de Jean-Baptiste, après avoir lu les droits insérés dans le fichier contenant le livre, effectuent le transfert sans que les utilisateurs interviennent.

Christian peut également prêter un livre à un ami. Si Raphaël veut lui emprunter un livre pour une semaine,

Christian transfère le livre sur l'ordinateur de Raphaël, mais, tant que le livre est prêté, Christian n'y a pas accès. Une fois la semaine écoulée, l'ordinateur de Raphaël désactive la copie du livre, et celui de Christian récupère le droit d'utiliser le livre. Sans la moindre intervention des deux amis, le livre a été « rendu ». Le droit de prêt est une clause essentielle à la constitution de bibliothèques numériques.

Les droits d'usage peuvent s'appliquer à la lecture des œuvres, à leur impression ou à la création d'œuvres dérivées. Certains droits peuvent être gratuits, et d'autres non, selon les volontés des auteurs et des éditeurs. Pour certaines œuvres, l'éditeur peut autoriser la copie, mais faire payer la lecture. Les droits peuvent être limités dans le temps ou dans l'usage ; ils peuvent concerner uniquement l'acquisition de l'ouvrage ou bien s'appliquer à chaque utilisation. L'éditeur peut faire des ristournes, des soldes, accorder des utilisations gratuites. Il peut limiter la diffusion aux personnes appartenant à des groupes, tels les membres d'un cercle de lecture, des personnes d'une classe d'âge ou d'un pays particulier.

Les systèmes sécurisés peuvent aussi respecter les clauses qui sont aujourd'hui en vigueur dans les bibliothèques et dans quelques autres institutions, autorisant, par exemple, un nombre raisonnable de copies ou de citations. Certaines catégories professionnelles – les bibliothécaires, les chercheurs, les enseignants – pourraient acquérir des licences leur permettant de faire gratuitement ou à prix réduit un certain nombre de copies d'une œuvre, à condition de respecter les droits d'auteur. Pour remédier aux copies illégales, on pourrait créer des caisses de compensation qui dédommageraient les éditeurs des manques à gagner.

Quels avantages les systèmes sécurisés procureront-ils aux utilisateurs ? Pourquoi ces derniers devraient-ils accepter un système ne leur offrant pas, c'est le moins qu'on puisse dire, un contrôle absolu sur le matériel et les données en leur possession ? Pourquoi devraient-ils payer alors qu'ils pourraient avoir tout gratuit ? Parce que, si les droits de propriété intellectuelle ne sont pas respectés, les grandes œuvres ne seront jamais proposées sous forme numérique, ni gratuitement ni à titre

TRANSFERT



PRÊT



2. LE TRANSFERT D'UNE ŒUVRE NUMÉRIQUE d'un système sécurisé à un autre ressemble à un transfert d'argent entre deux comptes bancaires. L'argent ne peut se trouver simultanément sur les deux comptes. Les droits de propriété distinguent le droit de copier une œuvre numérique (ce qui accroît le nombre d'exemplaires) et le droit de transférer cette œuvre (ce qui conserve le nombre d'exemplaires). La copie

d'une œuvre exige ordinairement une rémunération, tandis que son transfert est gratuit. Le prêt d'une œuvre numérique est une autre transaction, distincte de la copie et du transfert. Il est analogue au prêt d'un livre : il accorde temporairement la jouissance de l'œuvre à une autre personne ; le propriétaire de l'œuvre ne peut l'utiliser tant qu'elle est prêtée.