Comment fonctionnent exactement les DRM qui protègent les livres numériques ?

Les livres protégés par DRM ne peuvent être copiés qu'un nombre limité de fois. Mais qu'est ce qu'on entend par copie ? Est ce qu'on peut copier plusieurs fois un livre sur le même support sans que ça compte pour autant de copies utilisées ? Est ce que le nombre de copies correspond uniquement à un nombre de supports différents ? Et comment fonctionne la détection d'une nouvelle copie : comment le livre « sait » qu'il a déjà été copié plusieurs fois ?

Notre réponse du 03/14/2015 :
En réponse à votre question, il existe plusieurs types de DRM (gestion numérique des droits (GND), ou gestion des droits numériques (GDN), en anglais *digital rights management* (*DRM*)), qui utilisent des techniques de chiffrement.

La note se poursuit ainsi :
L'utilisation du chiffrement des oeuvres pour la mise en place des DRM repose sur l'utilisation de deux grands types d'architectures.
***Une architecture dite matérielle**, où la clé de déchiffrement est directement intégrée à l'appareil de lecture de l'oeuvre, comme par exemple pour les lecteurs DVD.*
Ce type d'architecture possède néanmoins un gros défaut. En effet, la clé de déchiffrement intégrée à l'appareil ne change jamais, ainsi, une fois celle-ci trouvé, le DRM appliqué aux oeuvres peut être facilement contourné.
***La seconde architecture, purement logiciel**, repose sur l'environnement client-serveur [4]. Cette architecture se décompose en quatre parties: l'encodeur qui chiffre les*

oeuvres numériques, le serveur de contenu qui s'occupe de la diffusion des oeuvres chiffrées, le logiciel de lecture du client qui permet de déchiffrer l'oeuvre et pour finir le gestionnaire de droits qui est utilisé pour vérifier si le client respecte bien les droits de l'oeuvre.
Lorsque le consommateur souhaite acquérir une oeuvre, le client du consommateur envoie à l'encodeur son identifiant qui permet de chiffrer l'oeuvre, lorsque le chiffrement est terminé l'encodeur met à disposition l'oeuvre sur le serveur de contenu. Ainsi le client télécharge l'oeuvre chiffrée sur le serveur de contenu.

Ensuite le client se connecte au gestionnaire de droit, aussi appelé serveur de licence. Le serveur de licence vérifie si l'utilisateur est autorisé, par exemple s'il a payé l'oeuvre, avant d'envoyer au client la clé de déchiffrement et les conditions d'utilisations de l'oeuvre. Pour finir le client déchiffre l'oeuvre avec la clé fournit par le gestionnaire de droits.

Vous mentionnez dans votre question les livres numériques. En général, ils reposent sur un chiffrement de type logiciel. Dans ce cas,**ce que vous appelez copie est en réalité un accès dans ce système qui comptabilise soit le nombre d'appareils qui accèdent au livre numérique** (cas d'Apple avec ibook store) au delà de 5 appareils, l'accès est bloqué. Ainsi l'utilisateur doit déclarer un appareil au système logiciel de chiffrement, ce n'est donc pas automatique. Dans ce cas, le nombre de « copies » est en réalité le nombre d'appareils utilisés. Ce fonctionnement est celui utilisé par Apple mais aussi pour les livres verrouillés par Adobe Digital Editions. Voici un exemple de l'usage de ce logiciel pour télécharger un livre numérique. Le principe est de forcer l'utilisateur à utiliser des appareils et ou des logiciels permettant de contrôler les usages de copie. Ainsi il est impossible d'exercer le droit pourtant reconnu à la copie privé. Le

logiciel n'a donc pas « besoin » de savoir ce que l'utilisateur fait puisque le fichier est accédé dans un environnement contrôlé.

L'autre possibilité, utilisée par certains éditeurs mais qui tend à diminuer est l'usage des techniques de filigrane ou watermark. Elles sont décrites comme suit dans ce cours de culture numérique :
Le tatouage numérique, "Watermark" en anglais, est une technique qui permet d'intégrer des informations (auteur, licence , …) au sein d'une oeuvre numérique. Elle repose sur le principe de la sténographie [2]. Il existe deux types de tatouage numérique: le tatouage invisible et le tatouage visible. Le premier modifie l'oeuvre de manière imperceptible pour l'utilisateur. Dans le cadre d'oeuvres numériques, cela se traduit par la modification ou l'ajout de bits [3]. Quant au second type, il consiste à ajouter clairement une marque visible sur l'oeuvre, ce type de tatouage est principalement utilisé par les photographes.
Cette technologie présente toutefois quelques limites. En effet, le tatouage numérique n'est utilisable que sur des fichiers de types binaires (images, audio et vidéo). De plus, il permet simplement de protéger les oeuvres contre la copie, mais pas d'appliquer des limites d'utilisations sur l'oeuvre, contrairement au système de chiffrement.

Dans ce cas, c'est bien le fichier lui-même qui est verrouillé (dégradé) et pas les environnements logiciels.
Pour en savoir plus à propos des DRM et des droits des utilisateurs, nous vous recommandons enfin la lecture de ce Guide de la gestion des droits numériques à l'usage des consommateurs. Il nous semble très bien fait sur le sujet.
Nous avons trouvé des documents pour répondre à votre questions en formulant la requête suivante : *technique restriction de la copie « gestion numérique des droits » (les guillemets sont importants)* dans les moteurs de recherche suivants : google, google scholar, Isidore

Vous pouvez retrouver une synthèse des techniques de recherche documentaires que nous utilisons dans les Guides du Savoir Trouver du réseau Eurêkoi.

Cordialement,

Eurêkoi – Bibliothèque Publique d'Information
www.bpi.fr