Hadopi

BONNES PRATIQUES À METTRE EN ŒUVRE POUR LES STRUCTURES METTANT UNE CONNEXION À DISPOSITION D'UN PUBLIC

Dans le cadre des lois Hadopi, le titulaire d'un abonnement, qu'il soit une personne physique ou une personne morale, peut voir sa responsabilité engagée si sa connexion à internet est utilisée, par lui-même ou par un tiers, pour commettre des actes de contrefaçon d'œuvres protégées par le droit d'auteur (téléchargement ou mise à disposition sur les réseaux pair à pair).

Le présent document recense quelques bonnes pratiques qui permettent, si elles sont combinées et associées à des mesures d'information des utilisateurs de la connexion, de limiter les risques d'utilisation frauduleuse de la ligne internet d'une structure.

Les faits qui sont à l'origine de la réception d'une recommandation sont des mises à disposition, sur les réseaux pair à pair, d'œuvres protégées. Les logiciels ou applications pair à pair servent la plupart du temps au téléchargement d'une œuvre (afin de la consulter), mais aussi à sa mise à disposition pour d'autres internautes qui utilisent le même outil.

Si ce type de logiciel ou d'application est actif sur l'un des appareils connectés à un accès Internet (ordinateurs, smartphone, tablette), il peut mettre à disposition automatiquement des fichiers téléchargés et engager la responsabilité du titulaire de l'abonnement à internet sur le fondement de la contravention de négligence caractérisée.

Plusieurs moyens peuvent être mis en œuvre pour sécuriser la connexion et éviter renouvellement des faits.

I. LA SECURISATION DES ORDINATEURS

Plusieurs actions peuvent être entreprises dans le cas où des ordinateurs sont mis à disposition au sein de la structure :

❖ *Vérifier la présence de logiciels de pair à pair*

Un logiciel de type « BitTorrent », « uTorrent », « Azureus » ou « eMule » ou autre logiciel de pair à pair peut être actif sur un ou plusieurs ordinateurs de votre parc de postes informatiques. S'il n'est pas désactivé, ce type de logiciel peut mettre à disposition automatiquement des fichiers téléchargés.

Afin d'éviter la mise en partage automatique d'œuvres protégées par un droit d'auteur, et si un tel logiciel n'est utilisé que dans ce but, il est préférable de désinstaller le logiciel de partage. Pour vous aider, l'Hadopi vous propose une vidéo et une fiche pratique sur la désinstallation de ces logiciels, disponibles sur le site internet de l'Hadopi www.hadopi.fr.

❖ *Paramétrer des profils d'utilisateurs sur les ordinateurs (« administrateur » et « utilisateur »)*

Il est recommandé de créer des profils d'utilisateurs distincts sur les ordinateurs mis à disposition du public, et de réserver le profil « administrateur » au compte principal de l'ordinateur qui gère notamment l'installation des programmes et les opérations de maintenance de l'ordinateur.
Le compte « utilisateur » n'a dans ce cas que des possibilités limitées : Par exemple, il ne permet pas en général d'installer de nouveaux programmes, tels que les logiciels de partage.

II. LA SECURISATION DU RESEAU

Il n'existe pas aujourd'hui, de mesure de sécurisation infaillible. Seule une combinaison d'outils permet de limiter au maximum les risques d'utilisation frauduleuse de votre ligne internet. Il revient à chaque structure d'adapter et de combiner au mieux les mesures techniques à mettre en place, en fonction de ses moyens et de ses utilisateurs.

❖ *Application d'un filtrage par port*

Certains logiciels ou services de partage utilisent un port dont le numéro est défini par avance. Un filtrage peut être mis en place sur ce port afin que, l'application ou le service soient bloqués.

Les dispositifs de type pare-feu sont capables de filtrer les communications selon le port utilisé. Il peut être conseillé de bloquer tous les ports qui ne sont pas indispensables à la navigation internet et/ou aux services de messagerie (selon la politique de sécurité retenue de la structure).

❖ *Application d'un filtrage applicatif*

Le filtrage applicatif est une analyse des protocoles d'échange avec une recherche des contenus à travers un certain nombre de règles prédéfinies qui peut permettre, notamment, de filtrer les flux partagés *via* des logiciels pair à pair.

Le pare-feu applicatif permet de récupérer tous les paquets d'une connexion et d'en faire une analyse en profondeur. Le pare-feu peut être configuré pour reconnaître les protocoles et connexions légitimes. Le mécanisme de filtrage rejettera toutes les connexions qui ne sont pas conformes aux protocoles autorisés. Il consiste ainsi à repérer et bloquer tous les flux d'une certaine nature (par exemple bloquer le protocole « BitTorrent » empêche de télécharger des fichiers à travers ce type de logiciel pair à pair).

❖ *Filtrage de contenus et d'URLs*

Des solutions logicielles permettent de filtrer les types de contenus auxquels les utilisateurs pourraient avoir accès sur le web. Même si aucune ne peut être fiable à 100 %, il s'agit d'une mesure de précaution. Il est possible d'appliquer des limites horaires portant tout aussi bien sur l'utilisation de tel ou tel programme en particulier (navigateur internet, Skype, jeu vidéo, etc.) que sur celle de la connexion internet ou de l'ordinateur lui-même.

Ce type de logiciel fonctionne selon trois principes distincts :

- L'interdiction de mots ou formules clés établis dans une liste, tels que « sexe » par exemple. Cette méthode ne saurait néanmoins être totalement efficace, du fait, notamment, des sites en langue étrangère ou bien des cas où textes et visuels ne correspondent pas.
- La liste noire, qui consiste à mettre à jour à chaque connexion une liste de sites interdits par le logiciel. Là aussi l'efficacité n'est qu'approximative, car des sites sensibles sont lancés chaque jour sur le réseau Internet.
- La liste blanche est une solution plus sûre mais très restrictive, où seuls les sites autorisés seront accessibles. La liste de ces derniers peut être modifiée à votre gré.

Pour plus d'efficacité, il peut être intéressant d'utiliser une solution où sont combinées interdiction de termes clés et liste noire.

N.B. : Toutes ces recommandations seront efficaces si un bon paramétrage est opéré et mis à jour régulièrement et si une maintenance de sécurité est effectuée au quotidien.

De plus, ces bonnes pratiques seront d'autant plus efficaces si elles sont accompagnées d'une sensibilisation accrue des utilisateurs. Vous trouverez sur le site de l'Hadopi www.hadopi.fr, plusieurs fiches pratiques et documents de sensibilisation.