Hadopi

BONNES PRATIQUES À L'EGARD DES PROFESSIONNELS METTANT LEUR CONNEXION À DISPOSITION D'UN PUBLIC

Dans le cadre des lois dites « Hadopi », un titulaire d'abonnement à Internet, qu'il soit une personne physique ou une personne morale (entreprise, association, collectivité…), peut recevoir des avertissements de l'Hadopi car il a l'obligation de veiller à ce que sa connexion ne soit pas utilisée pour télécharger ou mettre en partage sur internet des œuvres protégées par le droit d'auteur.

Un professionnel qui met sa connexion à disposition de ses salariés, de ses clients ou du public peut ainsi voir sa responsabilité engagée, car c'est lui le titulaire de l'abonnement.

Afin d'accompagner les professionnels dans les mesures à prendre pour sécuriser leur connexion, et ainsi éviter de faire l'objet d'une procédure de réponse graduée, l'Hadopi propose des outils pratiques à mettre en œuvre sur le plan technique.

1. Les bons réflexes avant de partager sa connexion

Avant de mettre un accès internet à disposition de plusieurs utilisateurs, il faut se poser les bonnes questions, à savoir :

- ❑ Qui sont les utilisateurs autorisés à se connecter à mon réseau Internet ?
- ❑ Comment les utilisateurs se connectent-ils à mon réseau (Wi-Fi, Filaire) ?
- ❑ Quelles mesures ont été mises en place pour limiter la connexion à mon accès aux seuls utilisateurs autorisés ?
- ❑ Quelles mesures ont été mises en place pour prévenir l'utilisation de mon accès à internet à des fins de contrefaçon ?
- ❑ Ai-je sensibilisé mes utilisateurs sur la bonne manière d'utiliser la connexion à internet que je mets à leur disposition ?
- ❑ Quelles solutions, et quels outils sont à ma disposition pour prévenir de nouveaux manquements ?

2. Les bonnes pratiques pour sécuriser sa connexion

Après avoir répondu à ces questions, il convient de trouver les mesures les plus appropriées à la situation du professionnel.

1/ La sécurisation des ordinateurs

❖ *Vérifier la présence de logiciels pair à pair et les désinstaller*

Les faits qui sont à l'origine de l'avertissement sont des mises à disposition, sur les réseaux pair à pair d'œuvres protégées (film, musique, série télévisée) par le biais d'un logiciel ou d'une application, par l'intermédiaire d'un logiciel ou d'une application pair à pair.

Ces outils (« uTorrent », « BitTorrent », « Azureus », etc.) peuvent être actifs sur un ordinateur de votre structure, mis à disposition des salariés ou du public. Ils sont paramétrés pour mettre à disposition automatiquement, dès que l'ordinateur se connecte à internet, des fichiers précédemment téléchargés.

En effet, un logiciel de pair à pair est utilisé, le plus souvent, à la fois pour le téléchargement d'un fichier (enregistrement), mais il met aussi à disposition le fichier pour d'autres internautes qui utilisent le même logiciel (mise à disposition). Ces deux actes sont potentiellement des atteintes au droit des auteurs lorsque le fichier en question est une œuvre protégée.

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 ce type de logiciel des ordinateurs mis à disposition des utilisateurs et / ou d'inviter les utilisateurs de votre connexion de les désactiver ou désinstaller de leur ordinateur avant de se connecter à votre réseau.

Le site Internet de l'Hadopi www.hadopi.fr vous accompagne avec des fiches pratiques et des vidéos sur la désinstallation de ces logiciels à la rubrique « Réagir à la réception d'une lettre de recommandation » / « Désinstaller un logiciel pair à pair ».

❖ *Paramétrer les ordinateurs avec les fonctionnalités « 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 des programmes.

(Pour plus d'informations, voir la fiche pratique *Mon ordinateur, quelle maintenance et quelle sécurité ?* à la rubrique « Ressources et Données » / « Sensibilisation » / « Les fiches pratiques » du site Internet de l'Hadopi).

2/ Le paramétrage de la « Box »

En tant que professionnel il se peut que vous partagiez votre réseau avec un public en communiquant le mot de passe wifi de votre boîtier de connexion (box) à des locataires, des adhérents d'une association ou des salariés par exemple. Il est alors possible de prendre des mesures pour contrôler l'utilisation de la box mise à disposition de tiers en la paramétrant via l'interface de celle-ci. Vous pouvez notamment désactiver le Wi-Fi communautaire, masquer le réseau Wi-Fi pour des utilisateurs externes (c'est-à-dire autres que les personnes à qui vous avez autorisé la connexion) ou encore définir des plages horaires pendant lesquelles le Wi-Fi du boitier de connexion sera activé.

(Pour plus d'informations sur ces possibilités de paramétrages, voir la rubrique dédiée sur le site Internet de l'Hadopi « Réagir à la réception d'une lettre de recommandation », menu de droite « Paramétrer sa box »).

3/ La sécurisation du réseau

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.

❖ *Appliquer 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).

❖ *Appliquer un filtrage applicatif*

Le filtrage applicatif est une analyse protocolaire qui peut permettre, notamment, de filtrer le partage *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).

❖ *Appliquer un 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 logiciels 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.
- 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 combinés 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 qu'une maintenance sécurité est effectuée au quotidien (voir à ce sujet la fiche pratique fiche pratique *Mon ordinateur, quelle maintenance et quelle sécurité ?* à la rubrique « Ressources et Données » / « Sensibilisation » / « Les fiches pratiques » du site Internet de l'Hadopi).

Ces bonnes pratiques seront d'autant plus efficaces si elles sont accompagnées d'une sensibilisation accrue des utilisateurs. Des outils et documents de sensibilisation sont disponibles sur le site Internet de l'Hadopi.

Pour plus d'informations, rendez-vous sur www.hadopi.fr à la rubrique dédiée aux professionnels.