HADOPI = BIG BROWSER EN BIBLIOTHÈQUE !

LE 4 JANVIER 2011 ***LIONEL MAUREL (CALIMAQ)***

Par le moyen détourné du concept de négligence caractérisée prévu dans le cadre de la loi hadopi, les bilbiothécaires sont en passe de devoir jouer les petits soldats de la surveillance généralisée des internautes.

En septembre 2009, j'avais écrit **un billet** pour évaluer les risques que la loi Hadopi ne s'applique aux bibliothèques, avec de graves conséquences sur leur capacité à offrir un accès internet à leurs usagers. Une semaine après la parution du **décret relatif à la labellisation des moyens de sécurisation**, il est certain à présent que le mécanisme de riposte graduée va avoir des répercussions sur les bibliothèques, et plus largement sur tous les lieux d'accès publics à Internet.

Pire que la coupure d'accès…

Jusqu'à présent, ce qui était certain, c'est que les personnes morales (entreprises, associations, administrations, etc) entraient bien dans le champ d'application de la loi Hadopi. Des amendements avaient été **proposés au Sénat** pour exclure ces dernières de la riposte graduée, mais ils avaient été repoussés **à l'initiative du gouvernement**. Telle qu'elle a été votée, la loi Hadopi s'applique à tous les titulaires d'une adresse IP, qu'il s'agisse de particuliers ou d'organisations (elle vise exactement les ***« personnes titulaires de l'accès à des services de communication en ligne au public »*** , sans autre précision).

Plusieurs analyses ont été produites cette année pour tenter d'évaluer comment la riposte pourrait s'appliquer **dans le cadre des entreprises**, au cas où des salariés utiliseraient les accès internet pour télécharger illégalement. Peu nombreux en revanche ont été ceux qui se sont penchés sur les conséquences possibles de la loi Hadopi sur les espaces qui fournissent un accès public à Internet, par le biais de postes Internet ou de connexions Wifi (comme les cybercafés, hôtels, hôpitaux, aéroports, EPN, parcs, universités, bibliothèques, etc).

Il peut paraître **assez improbable à première vue** que ces entités subissent une coupure d'accès à internet, suite à des téléchargements opérés par des usagers. **La loi Hadopi 2** indique ceci :

> ***Pour prononcer la peine de suspension [...] et en déterminer la durée, la juridiction prend en compte les circonstances et la gravité de l'infraction ainsi que la personnalité de son auteur, et notamment***

> ***l'activité professionnelle ou sociale de celui-ci, ainsi que sa situation socio-économique.***

Si rien n'empêche en théorie le juge de couper l'accès à une personne morale, on peut penser que cette rédaction de la loi lui permettra de moduler sa décision de façon à éviter les conséquences catastrophiques, liées à la coupure d'une entreprise ou d'une administration.

Mais la coupure d'accès n'est pas le seul risque que fait courir la loi Hadopi aux personnes morales et à mon sens, ce n'est pas le péril principal. La pression exercée pour recourir à des moyens de sécurisation labellisés risque en effet d'avoir des conséquences bien plus graves sur l'accès public à Internet. C'est la conséquence du fait que la riposte graduée s'articule non directement autour du délit de contrefaçon, mais autour de la notion de **négligence caractérisée** dans la sécurisation de son accès à Internet.

Négligence caractérisée + moyens de sécurisation = surveillance volontaire

Un autre décret, paru en juin dernier, a défini ce que l'on doit entendre par ce terme :

> ***Constitue une négligence caractérisée [...], le fait, sans motif légitime, pour la personne titulaire d'un accès à des services de communication au public en ligne, lorsque se trouvent réunies les conditions prévues au II :***
>
> ***1° Soit de ne pas avoir mis en place un moyen de sécurisation de cet accès ;***
>
> ***2° Soit d'avoir manqué de diligence dans la mise en œuvre de ce moyen.***

Dans le dispositif de la riposte graduée, l'Hadopi repère les téléchargements illégaux commis depuis certaines adresses IP, à partir des relevés que lui transmet **l'entreprise privée TMG**, agissant pour le compte des ayants droit. L'Hadopi envoie un mail d'avertissement aux titulaires de l'adresse IP, qui vise précisément à vérifier s'ils ont bien pris la précaution de sécuriser leur connexion Internet et pour leur enjoindre de le faire si ce n'est pas le cas.

Pour ce faire, les titulaires doivent apporter la preuve qu'ils ont installé un moyen de sécurisation, sous la forme d'un logiciel bloquant l'accès aux sites permettant le téléchargement illégal. Ces logiciels de sécurisation peuvent ou non avoir été homologués par l'Hadopi, par rapport à une liste de spécifications fonctionnelles. Si c'est un logiciel homologué qui a été choisi par le titulaire, le cas de l'internaute « **sera examiné avec une attention bienveillante** « , selon les mots de la présidente de l'Hadopi.

C'est l'objet du **décret paru la semaine dernière** de préciser la procédure par laquelle ces moyens de sécurisation seront labellisés. Un document préparatoire au développement des spécifications fonctionnelles donne par ailleurs des indications sur la forme que ces moyens de sécurisation pourront prendre et c'est là que l'on se rend compte comment ils pourront affecter les lieux d'accès public à Internet.

Ce document indique ceci (p.9) :

> ***Les cibles d'utilisateurs des dispositifs de sécurité peuvent être classées en 2 grandes classes : les entreprises, institutions,***

associations, d'une part et les particuliers, le grand public, d'autre part.

Pour les organisations, il y a encore deux sous-catégories : les organisations qui ont du personnel permanent, identifié et les organisations comme les hôtels, les cybercafés, les sites Wi-Fi ouverts (aéroports, etc.) où les utilisateurs sont de passage.

Les bibliothèques ne sont pas directement citées, mais il est évident que nous rentrons dans les deux sous-catégories, à la fois pour le personnel permanent et pour les utilisateurs de passage. Pour se mettre en conformité avec les attentes de l'Hadopi, il faudra donc installer ces moyens de sécurisation sur tous les postes munis d'une connexion internet, qu'ils soient mis à disposition du personnel ou des usagers, ainsi que des accès wifi.

Toujours d'après ce document, ces logiciels analysent la navigation à partir d'un système de listes noires, grises et blanches (p. 21) :

Le module de traitement utilise plusieurs sortes de triplets de listes :

Les listes noires : entités interdites (par exemple, la liste des sites web interdits par décision de justice) ;
Les listes grises : entités qui peuvent présenter des risques en matière de contrefaçon et qui nécessiteront une action de l'utilisateur pour outrepasser la notification du risque ; par exemple la liste grise des applications suspectes, la liste grise de plages de ports ou d'adresses qui rentrent en jeu dans certains protocoles ou certaines applications ;
Les listes blanches : entités autorisées, par exemple la liste blanche de l'offre légale.

Par ailleurs, le logiciel garde en mémoire toutes les opérations effectuées à partir d'un poste, ce que le document désigne par le terme de « journalisation », **analysée ci-après par Marc Rees** de *PC-Inpact* :

[...] cette journalisation est propre au moyen de sécurisation labellisé. Elle trace l'historique complet de tous les événements significatifs de l'ordinateur (ex : éléments de la vie interne du moyen de sécurisation : démarrage, arrêt, activation, désactivation, modification des profils de sécurité, etc.).

Dans le document préparatoire précité, on parle de « journaux sécurisés [qui] doivent être archivés et conservés par le titulaire de l'abonnement pendant la période d'une année, période où le titulaire pourrait demander à une tierce partie de confiance, un déchiffrement des journaux correspondant à des dates fixées et une copie certifiée conforme du déchiffrement de ces journaux ». Comme indiqué, plus l'abonné aura le sentiment d'être sécurisé face au risque Hadopi, plus il sera surveillé, traqué, examiné, observé.

Bienvenue dans l'Hadopithèque…

Vous vous demandez peut-être comment tout ceci peut se traduire dans une bibliothèque ?

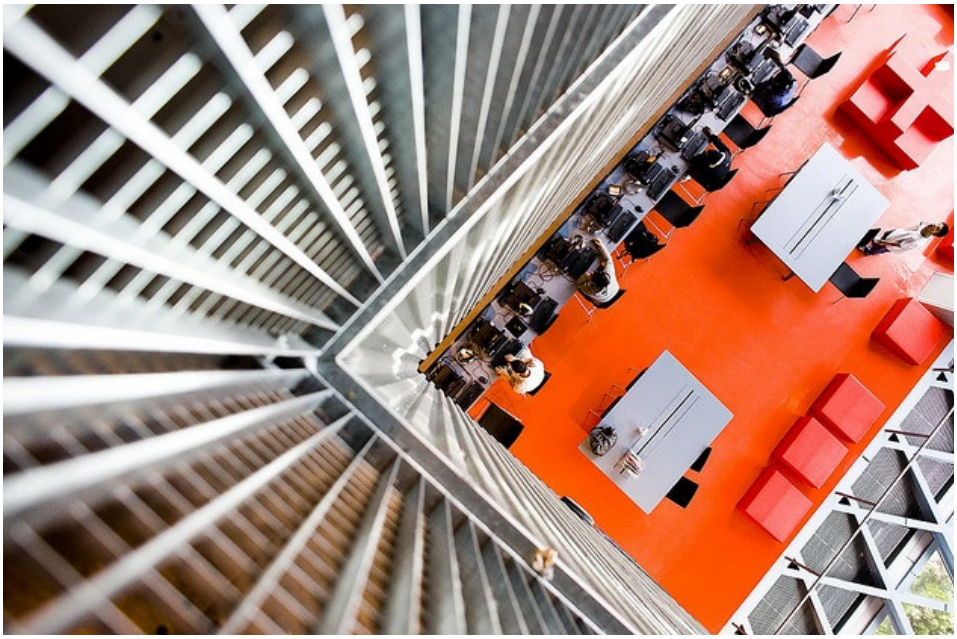
Essayons de combiner tous ces éléments et de voir ce qui risque de se passer dans les nouvelles “Hadopithèques”.

Chers bibliothécaires, sachez que vous êtes responsables, de plein fouet, pour tout ce que vos usagers (mais aussi vos collègues…) peuvent commettre à partir des connexions internet que vous mettez à leur disposition. Pour ne pas être accusés par l’Hadopi de négligence caractérisée, vous allez devoir installer des logiciels de sécurisation, et tant qu’à faire des systèmes labellisés, lorsqu’ils auront été homologués. Ces systèmes vont restreindre l’accès à Internet à partir de listes pré-établies. Ils vont en outre enregistrer tout ce que vos usagers feront à partir des postes. Si l’Hadopi vient à flasher une de vos adresses IP et à vous adresser un courrier d’avertissement, vous devrez lui apporter la preuve que vous aurez sécurisé vos accès et lui fournir les enregistrements opérés par le logiciel.

N’est-ce pas déjà une charmante façon de concevoir le métier de bibliothécaire ? Mais ce n’est pas tout. Imaginons que vous décidiez de modifier les paramètres du logiciel pour ouvrir l’accès à certains sites. Ce sera enregistré par le système de journalisation et retenu contre vous par l’Hadopi. Attention donc à ne pas être trop libéral. Mieux vaut peut-être même bloquer davantage de sites que ce que le logiciel propose par défaut…

Et si par malheur une faille quelconque se produit et qu’un de vos usagers arrive à commettre un acte illicite ? Ne vous en faites pas, vous êtes toujours responsable, **comme l’explique Maître Eolas** :

> ***On constate que votre abonnement a servi à télécharger illégalement, et que s’il a pu servir à cela, c’est qu’il n’était pas assez sécurisé. Si vous apportez la preuve de sa sécurisation absolue ou presque, vous apportez la preuve que c’est vous qui avez téléchargé. Dans les deux cas, vous pouvez être sanctionné. Pervers, n’est-ce pas ?***



The Librarian is watching you !

Nous étions déjà hélas **habitués en bibliothèque à subir les désagréments des Proxinators**, mis en place par des DSI souvent portées à faire du zèle en matière de sécurité informatique, bien au-delà des exigences posées par la loi. Nous savons bien combien il peut être difficile d’exercer le métier de bibliothécaire, et surtout le travail de médiation numérique, dans un environnement cadenassé. Voilà que la loi Hadopi vient à présent donner des arguments massues pour verrouiller et sur-verrouiller les accès à Internet dans nos établissements. Bien plus que la coupure d’accès, somme toute assez hypothétique, c’est d’emblée la « négligence caractérisée » qui risque de faire peur à nos

tutelles et les pousser à mettre en place de manière préventive les moyens de sécurisation.

En 2009 lors du débat sur la loi Hadopi, le gouvernement avait déjà avancé l'idée de mettre en place **un système de « portail blanc »** pour les accès publics à Internet, limité à un « internet citoyen » correspondant à une liste finie de sites considérés comme sans danger. Ce projet avait suscité **une vive réaction de la part de l'IABD** (Interassociation Archives, Bibliothèques, Documentation), au nom de la défense du droit d'accès à l'information, et il avait été finalement abandonné. Mais la réapparition de « listes blanches » dans les spécifications fonctionnelles des moyens de sécurisation me fait craindre qu'on ne s'achemine tout droit vers un retour à cette réduction de l'internet public à la portion congrue.

Si mes craintes se confirment, on assisterait à un durcissement radical des conditions d'accès à internet en bibliothèque. L'IABD, **dans une mise au point de cet été**, avait tenu à rappeler que rien dans le cadre légal actuel ne nous oblige à filtrer a priori l'accès à internet, ni à identifier nos usagers. La CNIL, **dans une fiche pratique sur son site**, confirme cette analyse.

Tout cet équilibre pourrait être mis à bas par la loi Hadopi et modifier les relations entre les bibliothèques et les usagers en les plaçant sous le signe de la surveillance et de la suspicion. **Marc Rees de *PC-Inpact*** arrive à cette conclusion en ce qui concerne les foyers privés :

> ***[...]l'abonné est responsable des mauvais usages qui seraient commis par des tiers (membre de sa famille, voisins, étrangers). Qu'il se reproche quelque chose ou non n'a pas d'emprise. Au contraire, le texte injecte un climat de suspicion et de défiance dans l'entourage proche.***

Cette défiance sera nécessairement encore plus forte dans les lieux d'accès public à Internet. Bien sûr – et c'est là le plus pervers – rien n'empêche le bibliothécaire de ne pas mettre en place le dispositif de sécurisation, jugeant que sa mission implique avant tout de donner accès à l'information de manière neutre et de respecter la *privacy* de ses usagers (**comme disent nos confrères américains**). Mais combien voudront – pourront – faire ce choix qui les expose de plein fouet à la mise en cause de leur responsabilité ? Comment défendre cette option devant sa tutelle en ayant seulement une chance de se faire entendre ?

Alors que **plus de 30% des foyers français** n'ont pas de connexions à internet à domicile, on s'achemine vers un accès public verrouillé, cadenassé, surveillé et appauvri. L'accès à Internet devient une composante fondamentale des services offerts en bibliothèque (**voyez ici à la BU d'Angers**, où elle tend même à s'imposer comme le service essentiel en fonction duquel l'espace est reconfiguré). Qu'en sera-t-il une fois que la loi Hadopi aura produit tous ses effets ?

Mais il y a pire à mes yeux. Le dispositif de la négligence caractérisée a cette perversité qu'il fera du bibliothécaire un des maillons actifs du dispositif de surveillance, poussé par la force des choses à installer des mouchards dans son parc informatique, sans que le texte de la loi ne le lui impose formellement. Il fera de nous des complices, tout simplement.

Bibliothécaires, avez-vous vraiment envie de devenir les « Grands Frères » de vos usagers ? Il n'est peut-être pas encore trop tard pour dire NON à ce qui se prépare.

– — –

Article initialement publié sur le blog **:: S.I. Lex ::**

>> Photos flickr CC **Mosman Library** ; **Thomas Hawk** (**bis**)

BERTRAND DUNOGIER
le 4 janvier 2011 - 10:00 • SIGNALER UN ABUS - PERMALINK

Effectivement, cette question est une réalité pour de nombreux établissements, surtout au vu de la floraison massive des cafés proposant un accès wifi.

Ma femme travaille justement dans un lieu (privé) qui propose à ses clients un accès wifi, avec ou sans prêt d'ordinateur. Je serais très très surpris que personne n'ait téléchargé depuis cet endroit de fichiers illégaux depuis la mise en place de HADOPI. Que faire pour eux en l'absence de réel technicien sur place et de "logiciels de sécurisation" valables ?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

WWW
le 4 janvier 2011 - 11:40 • SIGNALER UN ABUS - PERMALINK

Cette loi risque en effet d'enrayer l'évolution des accès internet gratuit wifi ou non.

Aujourd'hui la plupart des "box" possède un accès wifi publique en plus de l'accès privé.
Cet accès publique est authentifié et il est nécessaire d'appartenir au même fournisseur d'accès que le propriétaire de la box.

J'ai bien peur que l'initiative ultime pour ne plus être responsable de sa ligne en tant que service ""gratuit"", soit d'être sponsorisé par un fournisseur d'accès afin de mettre en place ce type de solution.

Donc plus d'accès gratuit et malheureusement même un service réduit a un prix.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

ADÈLE GROS-ROUGE
le 4 janvier 2011 - 12:30 • SIGNALER UN ABUS - PERMALINK

Je suis victime à mon boulot d'un "Proxinator" installé par ma collectivité, très con dans ses critères comme tous les proxinators (je n'ai pas été associée à la définition de ces critères, établis par des gens qui ignorent que mon métier consiste à trouver de l'information par tous les moyens, où qu'elle soit, sans la trier à priori et à la CRITIQUER avant d'en faire usage ou pas)
Le proxinator m'interdit par exemple de préparer une vente aux enchères, alors que les libraires sont définitivement passés au catalogue et à la gestion de la vente électronique ….

Alors, je lève le pied : si on m'infantilise, je REFUSE DE TRAVAILLER ET DE COOPERER et je ne me sers pas non plus de ma connexion personnelle pour contourner le proxinator (je ne suis pas payée pour bosser chez moi).

Je n'ai jamais rien téléchargé d'illégal (rien d'assez intéressant) et j'ai toujours payé tous les produits électronique que j'utilisais. Désormais, je n'en achète plus du tout et je ne suis pas disposée à vivre ainsi, "watchée" de toutes parts.

J'ai donc supprimé tout accès wifi chez moi et je refuse d'en installer ou de donner le moindre accès internet à quiconque à mon boulot. J'ai aussi supprimé le GSM et tous ces gadgets de traçage. Bef, j'ACHETE PAS.

Pas joignable ? Tant pis. Prenez rendez vous et venez me voir, A L'ANCIENNE.

Ringarde ? RIEN-A-FOUTRE.

Du repos pour la tête et pour le porte-feuille. Et dans ma famille, ON EST TOUS COMME CA ….. On a même des COPAINS PAREILS …..

Joyeuses Pâques !

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

BERTRAND DUNOGIER
le 4 janvier 2011 - 14:28 • SIGNALER UN ABUS - PERMALINK

Précision au sujet des accès FreeWifi, SFR Wifi, etc. Ceux-ci sont effectivement différents des accès WiFi personnels de la box, et peuvent être activés indépendamment. Leur usage nécessite un identifiant propre au FAI, toujours obtenu & fourni aux abonnés.

La très grosse nuance, critique ici, est que lorsque l'on utilise un tel accès, l'adresse IP utilisée n'est PAS celle de la connection ADSL de la box utilisée (on ne la connait en

général pas), mais celle correspondant aux identifiants wifi !

On a vu récemment un cas d'avertissement HADOPI envoyé à une personne qui n'avait pourtant rien téléchargé. En fait, celui-ci avait gracieusement donné ses identifiants FreeWifi à un ami, qui à son tour avait téléchargé. Le téléchargement a donc été identifié comme effectué depuis la connection ADSL du prêteur des identifiants, et non celle du propriétaire de la box.

Soyez donc TRES prudents si vous prêtez ces identifiants !

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

1 ping

« La loi Hadopi menace-t-elle l'accès à Internet des bibliothèques ? « Veille documentaire le 26 mai 2011 - 15:19

[...] → OWNI : « Hadopi = Big Browser en bibliothèque ! » (4 janvier 2011) [...]