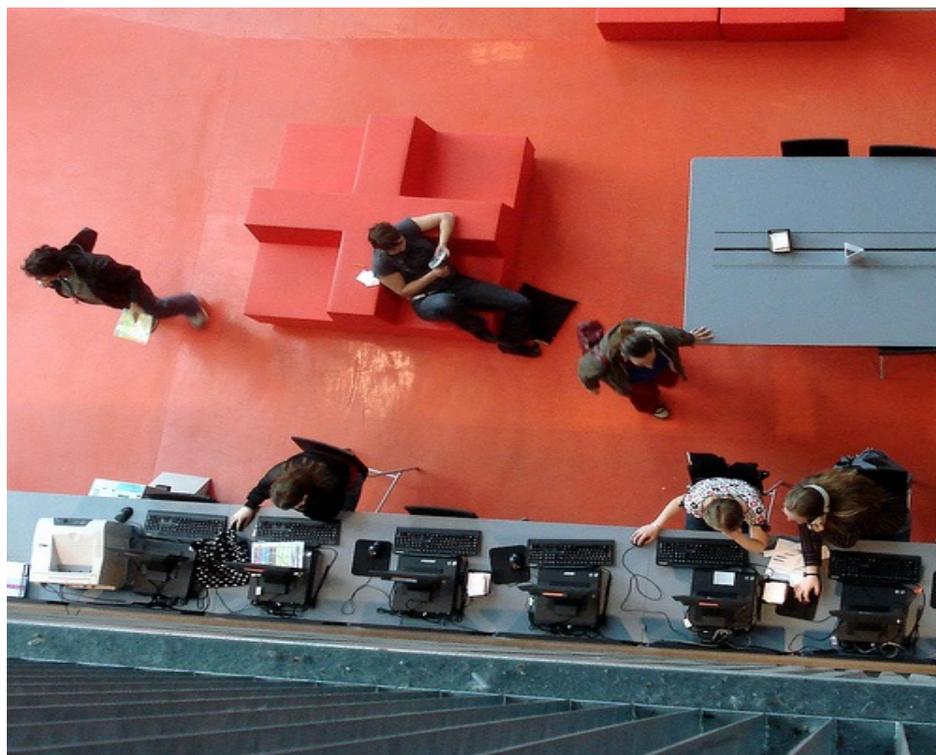


ACCÈS INTERNET EN BIBLIOTHÈQUE : CE QU'EXIGE VRAIMENT LA LOI

LE 26 MARS 2010 LIONEL MAUREL (CALIMAQ)

Si donner accès à Internet est une des missions importantes des services d'archives, de bibliothèques et de documentation, elle peut aussi engager leur responsabilité, en cas d'agissement délictueux des usagers. Quel équilibre trouver pour préserver la liberté de ces derniers en respectant la législation ?



Si donner accès à Internet est une des missions importantes des services d'archives, de bibliothèques et de documentation, elle peut aussi engager leur responsabilité, en cas d'agissement délictueux des usagers. Quel équilibre trouver pour préserver la liberté de ces derniers en respectant la législation ?

L'IABD (**Interassociation Archives Bibliothèques Documentation**) publie aujourd'hui **une mise au point**, concernant la teneur et l'étendue des obligations légales qui pèsent sur les services d'archives, de bibliothèques et de documentation lorsqu'ils offrent sur place des accès Internet à leurs usagers. L'information a été relayée sur **Bibliobsession** et **Paralipomènes**.

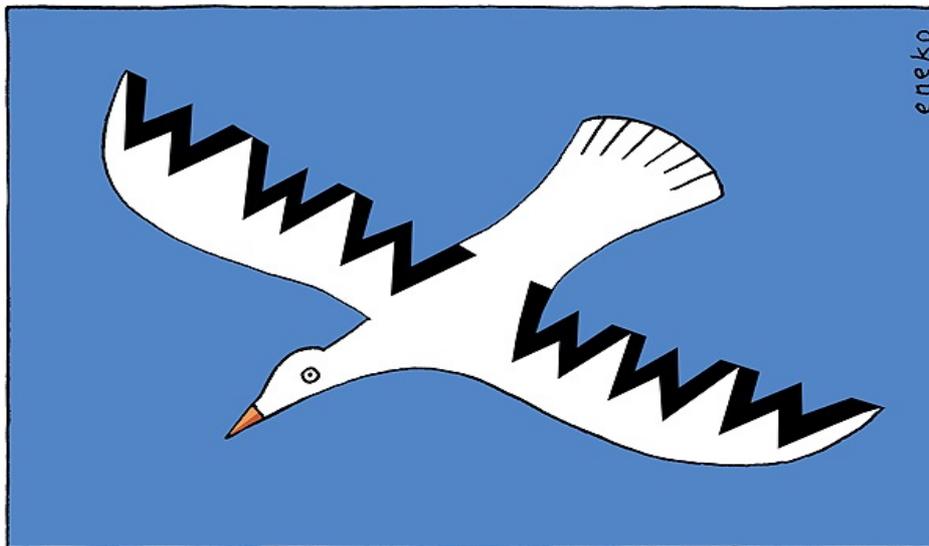
Le sujet est complexe et sensible, car il confronte les professionnels de l'information à un choix difficile. Donner accès à Internet constitue aujourd'hui pour les services d'archives, de bibliothèques et de documentation un aspect essentiel de leurs missions ; mais leur responsabilité est susceptible, à divers degrés, d'être engagée du fait d'agissements délictueux qui seraient commis à partir de ces connexions par leurs usagers.

Entre la liberté de l'utilisateur et la responsabilité de l'établissement, il faut trouver un équilibre, qui est d'autant plus difficile à déterminer que **les textes applicables sont nombreux** (Code des Postes et Communications Électroniques, Loi LCEN de 2004, loi anti-terroriste de 2006, loi Hadopi de 2009, etc) et leurs dispositions délicates à interpréter. Demander aux utilisateurs de s'identifier lorsqu'ils se connectent à Internet ; mettre en place des filtres pour bloquer l'accès à certains sites ; neutraliser certaines fonctionnalités comme le téléchargement ou l'usage des clés USB : autant de pratiques qui ont cours dans nos établissements, sans que l'on sache si elles sont réellement exigées par les textes de loi.

La question est d'autant plus importante que depuis l'été 2009, l'accès à Internet n'est pas seulement un service rendu à l'utilisateur, mais l'exercice d'une liberté fondamentale,

explicitement consacrée par le Conseil Constitutionnel à l'occasion de sa censure de la première loi Hadopi :

« [...] aux termes de l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 : « La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi » ; qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services. »



Il peut être tentant pour les bibliothèques, archives et centres de documentation de mettre en place des mécanismes de contrôle qui leur permettront de limiter les risques de voir leur responsabilité engagée. Mais il faut bien avoir conscience que si ces dispositifs vont au-delà de ce que la loi exige, ils auront pour effet de restreindre volontairement l'exercice d'une liberté fondamentale des citoyens, constitutionnellement consacrée.

La mise au point de l'IABD passe en revue les textes pour délimiter avec précision le champ de ces obligations légales. Il ressort de l'analyse que si les bibliothèques, archives et centres de documentation sont bien obligés de conserver pendant un an les données de connexion (loi anti-terroriste de 2006), il n'est nullement exigé, ni de recueillir l'identité des personnes qui accèdent à Internet, ni de mettre en place des moyens de sécurisation des connexions tels que des systèmes de filtrage.

Les textes préservent donc le droit des usagers à utiliser Internet librement, sans avoir à donner leur identité et à conserver leur anonymat lors de leur usage des connexions.

L'accès public à Internet est une liberté consacrée, mais hélas menacée. Lors du débat de la loi Hadopi, il avait été un temps proposé par le ministère de la Culture de **mettre en place un « portail blanc » pour brider les accès publics wifi** et les restreindre à une liste prédéterminée de sites « propres ». Un tel système aurait pu être appliqué dans les parcs ou les mairies, mais aussi dans les bibliothèques et autres services similaires offrant des accès wifi à leurs usagers. Face à cette menace d'atteinte à la liberté d'accès à l'information, l'IABD avait déjà réagi **par le biais d'une déclaration**. Le projet de portail blanc a finalement été abandonné lors de l'examen au Parlement de la loi, mais j'ai eu l'occasion d'essayer de montrer dans un billet précédent comment **la loi Hadopi était susceptible d'aggraver la responsabilité pesant sur les bibliothèques** du fait de l'usage des connexions Internet qu'elles offrent à leurs usagers.

Lors du dernier congrès de l'ABF, un atelier avait été organisée sur le thème « **L'autonomie**

de l'utilisateur versus la responsabilité du bibliothécaire » auquel j'avais participé. Il en était ressorti que plus qu'une question légale, les modalités de l'accès à Internet relèvent d'un choix professionnel qui revêt une forte dimension éthique. Pour que la liberté de l'utilisateur puisse exister, le bibliothécaire doit nécessairement accepter d'assumer une part incompressible de responsabilité.

Aux États-Unis, les bibliothécaires ont subi (**et subissent encore**) les conséquences du **Patriot Act**, qui les obligent à communiquer aux autorités des données personnelles sensibles de leurs usagers.

Il n'y a pas (encore) de Patriot Act en France, mais bien souvent, il reste plus facile de se connecter à Internet depuis un Mac Do qu'à partir de la bibliothèque de son quartier.

Si les services de bibliothèques, d'archives et de documentation veulent pleinement jouer un rôle d'espace public dans la cité, ils doivent aborder de front ces questions.

Ci-dessous le texte complet de la mise au point de l'IABD.

Offrir un accès à l'internet dans une bibliothèque, un service d'archives ou d'information : Les conditions juridiques

Entre les missions des bibliothèques, des services d'archives et d'information, et les obligations légales, quelle est la frontière entre un service ouvert à tous et le respect de la loi ? Comment interpréter les mesures préconisées ou imposées par le législateur, et les concilier avec la tradition d'un accès le plus large possible à l'information et à la connaissance ? Y a-t-il un espace d'interprétation propice à la sauvegarde des libertés ? Partageons-nous une posture professionnelle respectueuse du droit mais aussi des intérêts des usagers ?

QUELLES OBLIGATIONS LÉGALES ?

· Conserver les logs de connexion ?

Internet peut être libre et gratuit pour le public ; les établissements ne sont pas tenus de recueillir l'identité des personnes à qui ils proposent un accès à l'internet ; l'utilisateur peut même utiliser un pseudo pour se connecter et avoir accès à ses espaces personnels. En revanche, on doit pouvoir identifier l'ordinateur à l'origine de l'usage illicite par une adresse IP fixe.

La seule obligation qui s'impose aux bibliothèques, aux services d'archives et d'information (ou aux organismes dont ils relèvent) est de remettre, lors d'une réquisition judiciaire ou administrative, selon les cas, les logs de connexion (note 1) et toutes les informations qu'ils détiennent (note 2). Ces informations seront recoupées par les services chargés de l'enquête pour retrouver la personne à l'origine de l'infraction. L'antériorité exigible pour les données est d'un an.

· SÉCURISER LES POSTES ?

La loi n'impose pas que l'on filtre les accès à l'internet des ordinateurs mis à la disposition du public (note 3). Installer des filtres pour bloquer certains sites susceptibles d'être pénalement répréhensibles ne permettrait que de limiter sa responsabilité en cas de réquisition judiciaire, c'est-à-dire seulement après avoir reçu une lettre recommandée enjoignant l'abonné de sécuriser son poste.

En revanche, le fait de munir de filtres les ordinateurs proposés au public limite de manière arbitraire l'accès à l'internet, alors que cet accès constitue une liberté publique consacrée par le Conseil constitutionnel [5].

· Remettre des informations nominatives ?

C'est une obligation qui ne s'impose, au titre de la loi Hadopi, qu'aux organisations qui opèrent en tant que FAI (les services informatiques des universités, par exemple). Il incombe, en effet, aux FAI de fournir aux personnes chargées de l'enquête les informations détaillées dans le décret du 5 mars 2010, dont certaines sont nominatives (note 4).

LE POIDS DE CHARTES ET DES RÈGLEMENTS

Chartes et règlements intérieurs permettent d'informer le public des bibliothèques sur les usages interdits, sur la surveillance dont ils peuvent faire l'objet et sur l'existence éventuelle

de filtres.

D'autres documents destinés aux bibliothécaires leur rappellent le contrôle qu'il convient d'exercer et leur obligation de mettre fin à tout usage de l'internet qui serait manifestement illicite (contrefaçon, cyberpédopornographie, activités terroristes, etc.). L'enquête permettra d'évaluer, en fonction d'un contexte, la diligence du personnel.

Nulle obligation d'identifier les personnes ni même de filtrer les accès à l'internet

En cas de réquisition, les bibliothèques, les services d'archives et d'information abonnés à des FAI doivent remettre aux enquêteurs les logs de connexion et toute autre information habituellement recueillie. Il leur est recommandé de remettre aussi les chartes communiquées aux usagers et les informations destinées aux personnels.

QUE DISENT LES TEXTES ?

La loi anti-terroriste

L'obligation de conserver pendant un an les données de connexion, imposée aux fournisseurs d'accès Internet (FAI) par la loi anti-terroriste du 23 janvier 2006 [1], est étendue à tous ceux qui offrent un accès à l'internet à leur public.

Comme l'indique le Forum des droits sur l'internet [7], la conservation des logs peut se faire de trois manières différentes :

- en utilisant localement des unités de stockage dédiées associées à un routeur mis en place pour assurer la répartition du trafic interne entre les différents postes ;
- en confiant cette obligation au FAI auprès duquel on a acheté des abonnements à plusieurs adresses IP publiques correspondant au nombre de postes ;
- en confiant l'enregistrement à un tiers prestataire de services.

La loi Hadopi

La loi dite Hadopi [3] dissocie les obligations des FAI de celles des titulaires d'un abonnement à l'internet. La responsabilité d'une bibliothèque, d'un service d'archives ou d'information titulaire de plusieurs abonnements auprès d'un FAI n'est engagée pour les usages illicites réalisés à partir des ordinateurs connectés au réseau mis à la disposition du public que si les postes n'ont pas été sécurisés, après en avoir reçu l'injonction écrite de la Haute Autorité pour la diffusion des œuvres et la protection des droits d'auteur sur Internet (Hadopi).

Qu'en conclure ?

Ni la loi anti-terroriste, ni la loi Hadopi n'obligent ces établissements à identifier les utilisateurs des ordinateurs mis à leur disposition, ni à conserver des informations nominatives pour les remettre lors d'une enquête diligentée par un juge au titre de la loi Hadopi, ou d'une personnalité qualifiée placée auprès du ministre de l'Intérieur au titre de la loi anti-terroriste, ni même à filtrer à titre préventif les accès à l'internet.

Le respect des usages traditionnellement admis dans les bibliothèques, services d'archives et d'information reste compatible avec les obligations juridiques qui leur sont imposées, dès lors que les professionnels appliquent la loi, toute la loi, rien que la loi.

Textes

1. Loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers. **Sur le site Légifrance.**
2. Décret 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques. **Sur le site Légifrance.**
3. Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet. **Sur le site Légifrance.**
4. Décret n° 2010-236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet ». **Sur le site Légifrance.**
5. Décision n° 2009-590 DC du 22 octobre 2009. Loi relative à la protection pénale de la propriété littéraire et artistique sur internet. **Sur le site du Conseil constitutionnel.**

Recommandations – Déclarations

6. Offrir un accès public à l'internet : Des responsabilités aux multiples implications.

Déclaration de l'IABD, 10 mars 2009. **Sur le site de l'IABD.**

7. Les lieux d'accès public à l'internet. Recommandation du Forum des droits sur l'internet,

28 décembre 2007. **Sur le site du Forum des droits sur l'internet.**

8. Non au portail blanc. Déclaration de l'IABD du 6 mars 2009. **Sur le site de l'IABD.**

Notes

(1) Logs de connexion

Les données relatives au trafic s'entendent des informations rendues disponibles par les procédés de communication électronique, susceptibles d'être enregistrées par l'opérateur à l'occasion des communications électroniques dont il assure la transmission et qui sont pertinentes au regard des finalités poursuivies par la loi.

Cette obligation s'impose à toutes « les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit », une définition qui concerne les cybercafés mais également les bibliothèques. Il incombe aux opérateurs de communications électroniques de conserver pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales : a) Les informations permettant d'identifier l'utilisateur ; [c'est-à-dire celles qui sont enregistrées par lors des communications] b) Les données relatives aux équipements terminaux de communication utilisés ;

c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ; d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ; e) Les données permettant d'identifier le ou les destinataires de la communication.

(2) Les données nominatives seront remises uniquement si celles-ci sont déjà recueillies habituellement.

(3) Selon l'article 25 de la loi sur le droit d'auteur et les droits voisins dans la société de l'information (Dadvsi), le titulaire d'un accès à des services en ligne de communication au public en ligne doit veiller à ce que cet accès ne soit pas utilisé à des fins de contrefaçon, en mettant en œuvre les moyens de sécurisation qui lui sont proposés par le fournisseur de cet accès en application de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. N'étant pas assortie de sanction, cette disposition ne peut pas être mise en œuvre.

(4) Loi Hadopi. Décret du 5 mars 2010 Les données conservées par les agents assermentés travaillant pour les ayants droit : date et heure des faits ; adresse IP des abonnés concernés ; protocole pair à pair utilisé ; pseudonyme utilisé par l'abonné ; informations relatives aux œuvres ou objets protégés concernés par les faits ; le nom du fichier présent sur le poste de l'abonné (le cas échéant) ; le nom de son fournisseur d'accès à internet. Les données à fournir à la Hadopi par les FAI : noms et prénoms de l'abonné, son adresse postale et son adresse électronique ; ses coordonnées téléphoniques et son adresse d'installation téléphonique.

(5) La bibliothèque titulaire d'un abonnement encourt des sanctions pénales : une contravention de 5ème catégorie (amende de 1500€), une coupure de l'accès à Internet d'un mois et une obligation de mettre en œuvre un « moyen de sécurisation » labellisé par la Hadopi.

25 mars 2010

IABD (Interassociation archives-bibliothèques-documentation) – <http://www.iabd.fr>

Secrétariat : ABF – 31, rue de Chabrol – 75010 Paris – 01 55 33 10 30 – abf@abf.asso.fr



Billet initialement publié sur :: S.I.Lex ::



2 pings

Les tweets qui mentionnent owni] Accès Internet en bibliothèque : ce qu'exige vraiment la loi -- Topsy.com le 27 mars 2010 - 17:11

[...] Ce billet était mentionné sur Twitter par Aurélien Fache, Owni, Christophe Goddon, Alexandre Ultré, cyberanimateur et des autres. cyberanimateur a dit: Accès Internet en bibliothèque : ce qu'exige vraiment la loi <http://bit.ly/cZ0uZz> via @AddToAny [...]

[WORDPRESS HASHCASH] The comment's actual post text did not contain your blog url (<http://owni.fr/2010/03/26/acces-internet-en-bibliotheque-ce-qu%e2%80%99exige-vraiment-la-loi>) and so is spam.

Sécurité Anti Terroriste du 26/03/210 | Archives de Sécurité Tube le 27 mars 2010 - 20:50

[...] Accès Internet en bibliothèque : ce qu'exige vraiment la loi | Owni.fr [...]

[WORDPRESS HASHCASH] The comment's actual post text did not contain your blog url (<http://owni.fr/2010/03/26/acces-internet-en-bibliotheque-ce-qu%e2%80%99exige-vraiment-la-loi>) and so is spam.