Quelles obligations pour les bibliothèques qui souhaitent offrir un accès à internet ?

Johanna Carvais
jcarvais@cnil.fr

Pascal Palut
ppalut@cnil.fr

Commission nationale de l'informatique et des libertés (Cnil)

Juriste au sein du service des affaires juridiques de la Cnil, **Johanna Carvais** *fait partie du pôle « nouvelles technologies ». Titulaire d'un troisième cycle de droit public des technologies de l'information et de la communication et major de sa promotion, elle a d'abord travaillé dans un cabinet d'avocats. Elle donne régulièrement des cours à l'Institut supérieur d'électronique de Paris et participe à des formations délivrées par l'École nationale des ponts et chaussées (aujourd'hui dénommée École des ponts ParisTech).*

Pascal Palut *occupe les fonctions de juriste-documentaliste au sein de la direction des études, de l'innovation et de la prospective de la Cnil. Il est titulaire d'un DESS en droit des nouvelles technologies de Paris 1 – Panthéon Sorbonne. Rattaché au service de l'information et de la documentation, il s'occupe notamment des problématiques liées à la gestion des connaissances.*

L'impact des attentats du 11 Septembre sur la conservation des données de trafic sur internet

Dans un contexte général tendu, lié aux attentats du 11 septembre 2001, le monde entier entreprend des développements législatifs importants en matière de lutte contre le terrorisme, à commencer par les États-Unis qui adoptent, dès le 24 octobre 2001, leur Patriot Act[1]. Cet acte autorise le FBI à exiger de toute personne physique ou morale qu'elle lui produise « toute chose tangible » dès lors qu'il lui est précisé que cet ordre est pris dans le cadre d'une enquête de lutte contre le terrorisme international ou des activités d'espionnage. Pour ce faire, le FBI n'a pas besoin de démontrer qu'il existe une « cause probable » de croire que la personne sur laquelle sont effectuées des recherches a commis un acte ou a exercé des activités répréhensibles. Fin novembre 2003, avec le Domestic Security Enhancement Act[2] (appelé Patriot Act II), le Congrès a encore accru les pouvoirs du FBI en diminuant d'autant le contrôle judiciaire. Pour rappel, l'homme clé des attentats du World Trade Center, Mohamed Atta, se prépara depuis Hambourg, où, étudiant boursier en architecture du gouvernement allemand, il obtint de son université l'ouverture d'une salle de prière. Cette dernière, équipée d'une liaison internet, lui permit de correspondre avec toutes les autres personnes impliquées dans ce complot.

C'est dans ce mouvement de renforcement du pouvoir des forces de l'ordre face au risque terroriste que les directives européennes du 12 juillet 2002[3] et du 15 mars 2006[4] ont voulu améliorer l'utilisation des données par les autorités judiciaires en imposant aux opérateurs de communications électroniques la conservation de certaines données techniques sur une longue période, qu'elles soient utiles ou non à la facturation.

La France a, de son côté, initié dès 1999 une réflexion concernant la conservation des données de trafic qui a abouti à l'introduction en droit français du principe de rétention des données prévu par la loi sur la sécurité quotidienne du 15 novembre 2001, puisque l'exploitation des données techniques générées par l'utilisation d'un service de communications élec-

1. Voir : Philippe Cantié, « USA Patriot Act », *BBF*, 2006, n° 5, p. 64-71. En ligne : http://bbf.enssib.fr/consulter/bbf-2006-05-0064-001

2. Loi sur le renforcement de la sécurité intérieure.

3. Directive 2002/58 CE du Parlement européen et du Conseil européen du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

4. Directive 2006/24 CE du Parlement européen et du Conseil européen du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002-58/CE.

troniques est devenue un élément indispensable de toute enquête judiciaire. En même temps qu'elle prévoit un principe général d'effacement ou d'anonymisation de toute donnée relative au trafic, cette loi distingue parmi ces données celles qui peuvent être conservées à des fins de facturation, celles qui peuvent être conservées à des fins de sécurité du réseau des opérateurs, et enfin celles qui doivent être conservées aux fins exclusives d'enquêtes judiciaires. Cette loi est codifiée notamment à l'article L. 34-1 du *Code des postes et des communications électroniques* (CPCE).

Sur ce dernier point, on note une ambiguïté dans le texte de l'article L. 34-1 du CPCE entre « pouvoir » et « devoir ». L'article dispose en réalité que, « *pour les besoins de la recherche, de la constatation et de la poursuite des infractions* [...], *il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonyme certaines catégories de données techniques* ». Or, l'article L. 39-3 du CPCE sanctionne d'un an d'emprisonnement et de 75 000 euros d'amende la non-conservation des données pendant un an pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales : il s'agit bien d'une obligation, et non d'une possibilité[5].

La loi n° 2006-64 relative à la lutte contre le terrorisme du 23 janvier 2006[6] et ses décrets d'application sont venus élargir l'exploitation de ces données, dont la conservation est obligatoire depuis la loi de 2001. Avec tous ces textes qui encadrent le contrôle de l'accès à internet en France, les organismes, publics ou privés, finissent par se perdre. Quelles obligations pour l'organisme qui souhaite offrir au public un accès à internet ?

L'obligation de conservation de l'article L. 34-1 CPCE

Qui doit conserver ?

Les dispositions de l'article L. 34-1 s'appliquent aux opérateurs de communications électroniques (téléphone fixe, téléphone mobile et internet). Font partie des opérateurs « *les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne* », c'est-à-dire « *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* ». Mais de qui s'agit-il en réalité ?

La notion d'« établissements recevant du public » est définie par le *Code de la construction et de l'habitation*. Son article R. 123-2 précise d'ailleurs que « *sont considérées comme faisant partie du public toutes les personnes admises dans l'établissement à quelque titre que ce soit en plus du personnel* ». La loi de lutte contre le terrorisme a élargi la définition d'« opérateur de communication en ligne » afin de soumettre à l'obligation de conservation les opérateurs « classiques » bien sûr, mais aussi les cybercafés, restaurants, hôtels, aéroports et mairies offrant des « hot spots ». Au vu de ce qui précède, il est donc logique d'exclure les entreprises ou administrations de cette obligation, puisqu'elles assurent un accès au réseau à leurs seuls salariés ou agents, et non pas « au public ». En revanche, à la question : « les bibliothèques et les universités sont-elles des opérateurs de communications électroniques ? », il convient de répondre que les débats parlementaires n'ont pas exclu cette possibilité dès lors qu'elles offrent au public un accès à internet. La définition de la loi est – faut-il encore le rappeler – volontairement large : en clair, une bibliothèque qui offre au public un accès à internet est soumise à cette obligation.

Cette obligation de conservation pour les opérateurs de communications électroniques est à distinguer de celle incombant aux hébergeurs et fournisseurs d'accès à internet prévue à l'article 6-4 de la loi pour la confiance dans l'économie numérique du 21 juin 2004, notamment celle relative aux catégories de données conservées[7].

La Cnil

La Commission nationale de l'informatique et des libertés (Cnil) est une autorité administrative indépendante, créée en 1978, qui se compose d'un collège pluraliste de 17 membres. Son président est élu par ses pairs. La Commission est dotée, depuis 2004, d'un pouvoir de contrôle et de sanction renforcé sur l'ensemble des traitements de données personnelles. Jouant aussi un rôle d'alerte et de conseil, la Cnil a fondamentalement pour mission de veiller à ce que le développement des nouvelles technologies ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.
www.cnil.fr

Quelles données doivent être conservées ?

Les « données relatives au trafic »

L'article L. 34-1 du CPCE prévoit une obligation de conservation des « données relatives au trafic », sans plus de précision sur leur définition. Il énonce, en effet, que les catégories de données de trafic soumises à l'obligation de conservation sont déterminées par décret en conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés (Cnil). Il est prévu[8], pour l'application des alinéas II et III de l'article L. 34-1 du CPCE, que les données relatives au trafic s'entendent « *des informations rendues disponibles par les procédés de communication, susceptibles d'être enre-*

5. D'ailleurs les travaux préparatoires de la loi n° 2006-64 relative à la lutte contre le terrorisme du 23 janvier 2006 lèvent cette ambiguïté et sont clairs quant à l'obligation.

6. En ligne : www.legifrance.gouv.fr

7. Cf. le décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. En ligne : www.legifrance.gouv.fr

8. Décret n° 2006-358 du 24 mars 2006. En ligne : www.legifrance.gouv.fr

gistrées par l'opérateur à l'occasion des communications électroniques dont il assure la transmission ». Ces données de trafic sont exclusivement des données techniques, précisent les articles L. 34-1 et L. 34-1-1 du CPCE.

Parmi ces données techniques de connexion, l'article R. 10-13 du CPCE[9] liste de manière limitative les catégories de données concernées :

- les informations permettant d'identifier l'utilisateur ;
- les données relatives aux équipements terminaux de communication utilisés ;
- les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
- les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
- les données permettant d'identifier le ou les destinataires de la communication.

La Cnil, dans son avis du 10 novembre 2005, considère que le décret d'application, adopté le 24 mars 2006, en se contentant d'énumérer cinq catégories génériques de données, ne permet pas aux opérateurs de mesurer précisément l'obligation qui leur est faite de conserver certaines données.

Ce qui est clair, c'est que toutes les données couvertes par cette obligation sont des données techniques de connexion. Dès lors, les informations permettant d'identifier l'utilisateur doivent s'entendre comme des données techniques d'identification telles que l'adresse IP. Il n'existe pas en revanche d'obligation pour les opérateurs de communications électroniques d'identifier leurs clients par leur nom ou leur prénom. D'ailleurs, ils n'ont aucune assermentation leur permettant d'exiger la présentation de pièces d'identité.

Les données d'identification

Par ailleurs, l'obligation de transmettre les données d'identification, issue du décret n° 2010-236 du 5 mars 2010 (décret d'application de la loi dite Hadopi I) concerne le fournisseur d'accès à internet, qui a l'obligation de transmettre les données d'identification du titulaire de l'abonnement (et non de l'utilisateur) au service internet. En d'autres termes, ni le *Code des postes et des communications électroniques*, ni la loi Hadopi I n'imposent une identification des utilisateurs du réseau internet des bibliothèques.

Les données de trafic, puisqu'elles sont engendrées par les communications, sont de nature à révéler un éventail de détails concernant la façon dont les personnes mènent leur vie quotidienne. Or, les informations conservées « *ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications* », c'est-à-dire et par exemple le contenu des SMS ou même les adresses URL des sites internet visités. En effet, les adresses URL sont susceptibles de révéler les intérêts personnels d'une personne, par exemple des indications relatives aux opinions religieuses, aux opinions politiques, à la santé ou à la vie sexuelle – mais l'article 226-15 du *Code pénal* sanctionne d'un an d'emprisonnement et de 45 000 euros d'amende le fait d'ouvrir ou de prendre frauduleusement connaissance des correspondances arrivées ou non à destination et adressées à des tiers.

Néanmoins, il peut être fait obligation aux fournisseurs de détenir ces informations dans les hypothèses suivantes :

- S'agissant des sites web consultés, l'article 60-1 du *Code de procédure pénale* prévoit que seul l'officier de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir du fournisseur d'accès à internet « *de prendre sans délai toutes les mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs* ».
- S'agissant du contenu des échanges sur internet, il peut être procédé à des interceptions des communications par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunications.

Combien de temps sont conservées les données ?

Dans son avis du 9 décembre 2003, la Cnil avait estimé, en ce qui concerne la durée de conservation des données devant être conservées au titre de la recherche, de la constatation et de la poursuite des infractions pénales, qu'« *une durée de conservation limitée à trois mois par les opérateurs de télécommunications serait de nature à réduire les risques induits par un dispositif qui déroge aux règles applicables à la protection des données à caractère personnel, tout en permettant aux autorités judiciaires d'exercer leurs activités dans des conditions acceptables, étant entendu qu'elles peuvent toujours, dans le cadre d'une enquête, obtenir la préservation de certaines données*[10] ». Mais dans son avis du 10 novembre 2005, la Cnil a relevé que les nécessités des enquêtes concernant les infractions pénales les plus graves peuvent justifier un accès à des données de trafic remontant à une période supérieure à trois mois et que, dès lors, la durée de conservation d'un an prévue par le projet de décret n'appelait pas d'opposition de sa part.

L'harmonisation européenne fixe aux États membres une durée minimale de conservation de six mois et maximale de deux ans à compter de la date de la communication, ce qui leur laisse une large marge de manœuvre. Enfin, le décret d'application du 24 mars 2006 relatif à la conservation des données fixe dans l'article L. 34-1 du CPCE une durée de conservation d'un an.

Qui accède aux données ?

Les données de trafic ne sont conservées que pour les « *besoins de la recherche, de la constatation, de la poursuite d'infractions pénales* ». Dès lors,

9. Cet article est issu du décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données de communications électroniques.

10. En ligne : www.legifrance.gouv.fr

© Cnil

outre les services internes qui, en raison de leur fonction, sont chargés de traiter les données, seules les autorités légalement habilitées à avoir communication de ces données, à savoir les « tiers autorisés », pourront y accéder. On compte notamment, parmi les tiers autorisés, les autorités judiciaires, dans le cadre défini par le *Code de procédure pénale*.

L'article L. 34-1-1 permet, hors contrôle de l'autorité judiciaire, l'accès par des agents individuellement habilités des services de police et gendarmerie nationales en charge de la lutte contre le terrorisme aux données techniques conservées par les opérateurs de communications électroniques. Cet accès est encadré par la loi : les demandes devront être motivées, centralisées et soumises à la décision d'une personne qualifiée, désignée par la Commission nationale de contrôle des interceptions de sécurité sur proposition du ministre de l'Intérieur. Sur ce point, la Cnil a préconisé une amélioration de la procédure de contrôle de l'accès aux données techniques, et le Conseil constitutionnel, dans sa décision du 19 janvier 2006[11], estime que l'accès aux données de connexion par les services de police est assorti de limitations et précautions propres à assurer la conciliation entre le respect de la vie privée et la prévention des actes de terrorisme.

En outre, les autorités administratives ont besoin d'avoir parfois accès à ces informations pour connaître des infractions qui ne relèvent pas forcément du pénal, mais du fiscal. Pour remédier aux dispositions de l'article L. 34-1, plusieurs textes (l'article 65 du *Code des douanes*, l'article L. 83 du *Livre des procédures fiscales* et l'article L. 621-10 du *Code monétaire et financier*) prévoient explicitement que les services des douanes, les services des impôts et l'Autorité des marchés financiers pourront avoir accès aux données de connexion conservées par les opérateurs de communications électroniques.

Le 12 juin 2009, la loi favorisant la diffusion et la protection de la création sur internet, dite loi Hadopi I[12], instaure la conservation des données relatives au trafic pour les besoins de la recherche, de la constatation, et de la poursuite d'un manquement à l'obligation définie à l'article L. 336-3 du *Code de la propriété intellectuelle*, c'est-à-dire un manquement à son obligation de sécurisation de la connexion. Cette conservation a pour but la mise à disposition de ces données à la Haute autorité pour la diffusion des œuvres et la protection des droits sur internet (Hadopi)[13]. Enfin, les personnes concernées peuvent bien sûr accéder à leurs données en vertu des dispositions de la loi « Informatique et libertés »[14].

11. En ligne : www.conseil-constitutionnel.fr

12. Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet. En ligne : www.legifrance.com

13. www.hadopi.fr

14. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée en 2004.

Les obligations issues de la loi « Informatique et libertés »

L'obligation de conservation des données de trafic de l'article L. 34-1 du CPCE induit une obligation de collecte. Or, la collecte et la conservation constituent des « traitements » au sens de l'article 2 de la loi du 6 janvier 1978 modifiée en août 2004.

Parmi les données couvertes par cette obligation, on retrouve des données techniques d'identification, telles que l'adresse IP. Bien que la jurisprudence ne tende pas vers cette acception, la Cnil a toujours maintenu qu'une adresse IP permettait dans certains cas d'identifier un abonné – personne physique – qui se connecterait au réseau d'un opérateur de communication électronique (d'une bibliothèque par exemple). Le CPCE parle d'ailleurs de « données d'identification », ce qui induit la possibilité d'identifier une personne. Dès lors, la conservation et a fortiori la collecte des données de trafic, parmi lesquelles figurent des données qui identifient, de manière directe ou indirecte, une personne physique, constituent des traitements de données à caractère personnel soumis à la loi « Informatique et libertés ».

De fait, le G29 – organisation de toutes les Cnil européennes –, qui a déjà eu à se prononcer sur le sujet, est plutôt sceptique sur la nécessité d'une telle obligation. Adopté le 9 novembre 2004, l'avis du G29 relatif au projet de décision-cadre sur la conservation de données traitées et stockées en relation avec la mise à disposition de services de communications électroniques disponibles publiquement ou de données sur les réseaux de communications publiques vient tempérer l'utilité de l'obligation de conservation [15]. L'avis rappelle que la décision-cadre ne fournit pas d'éléments de nature à persuader que la conservation à grande échelle des données de trafic constitue l'unique option pour lutter contre la criminalité. Imposer aux opérateurs de conserver des données de trafic dont il n'a pas besoin à des fins propres est une dérogation au principe de finalité issu de la directive sur la protection des données du 24 octobre 1995 [16].

À l'obligation de conservation viennent s'ajouter les obligations issues de la loi française de protection des données du 6 janvier 1978 modifiée, qui reprend les principes fixés par la directive de 1995. Ces obligations s'imposent aux responsables de traitements, à savoir en l'espèce aux opérateurs de communications électroniques.

Une obligation d'effectuer des formalités

L'article 22 de la loi « Informatique et libertés » prévoit que les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Cnil. Cette déclaration doit être préalable à la mise en place du traitement, et fait l'objet d'un récépissé de déclaration. Ce récépissé ne vaut pas contrôle de légalité, il s'agit en quelque sorte d'un accusé de réception des formalités administratives. Tout manquement à cette obligation de déclaration est sanctionné par le *Code pénal* de cinq ans d'emprisonnement et de 300 000 euros d'amende pour le responsable de traitement (article 226-16).

Même si de telles sanctions sont rarement appliquées, la Cnil veille, notamment au travers de ses contrôles, au respect de cette disposition. Elle a, d'ailleurs, déjà mis en demeure en 2009 une médiathèque, notamment pour défaut de formalité auprès de la Cnil dans le cadre d'un traitement de conservation des données de trafic.

Il appartient aux opérateurs de communications électroniques (et donc aux bibliothèques offrant au public un accès à internet) de procéder à une déclaration. Cette démarche peut s'effectuer, aujourd'hui, directement en ligne depuis le site de la Cnil. La Commission délivre désormais le récépissé en moyenne sous quatre jours.

Une durée de conservation limitée des données

L'article 6-5 de la loi du 6 janvier 1978 modifiée prévoit un principe de durée limitée de conservation des données. Il dispose que les données doivent être conservées sous une forme permettant l'identification des personnes concernées « *pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées* ». À cet égard, la Cnil analyse la durée de conservation de chaque traitement, puisqu'elle est garante du droit à l'oubli. Dans la mesure où il existe un texte spécifique (l'article L. 34-1 du CPCE), et en application du principe de droit « *generalia specialibus non derogant* » (les lois de portée générale ne dérogent pas aux lois spéciales), la durée de conservation adéquate pour un tel fichier est d'un an.

Une obligation d'information des personnes

La loi « Informatique et libertés » impose la délivrance d'une information à la charge du responsable de traitement. Son article 32 prévoit une obligation d'informer les personnes concernées par le traitement : de la finalité, de l'identité du responsable de traitement, des destinataires, des droits des personnes et le cas échéant d'un transfert de données hors Union européenne. Le défaut d'information est également sanctionné par le *Code pénal* d'une contravention de cinquième classe.

En pratique, dans les bibliothèques, cette information peut se faire par voie d'affichage dans les locaux, par la remise d'un document, au travers du règlement intérieur, d'une charte ou encore de la notice d'utilisation des postes informatiques. Des modèles de mentions types sont disponibles sur le site de la Cnil dans la rubrique « vos responsabilités ».

15. En ligne : www.legifrance.gouv.fr

16. Directive 95/46 CE du Parlement européen et du Conseil européen du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Une obligation de sécurité

L'article 34 de la loi du 6 janvier 1978 prévoit également une obligation en termes de sécurité. Le responsable de traitement est tenu de « *prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données, et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ». Cette obligation de moyen – et non de résultat – suppose que les opérateurs de communications électroniques mettent en place des mesures de sécurité physiques (ordinateurs dans des locaux fermés à clé par exemple) et logiques (identifiants et mots de passe de connexion, politiques de renouvellement des mots de passe, mots de passe alphanumériques d'au moins six caractères...).

Dans le cas où l'opérateur de communication électronique fait appel à un sous-traitant, il est important de savoir que l'article 35 de la loi précise que « *le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données* ». Là encore, le site de la Cnil met à disposition un modèle de clause de confidentialité pouvant être utilisé en cas de sous-traitance[17]. Pour autant, il convient de faire attention, le contrat ne suffit pas, et cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect des mesures de sécurité et de confidentialité. Concrètement, il faudra procéder, par exemple, à des audits réguliers auprès de la société sous-traitante.

Conclusion

Les obligations issues du *Code des postes et des communications électroniques* et de la loi « Informatique et libertés » engagent la responsabilité des organismes mettant à disposition du public un accès à internet. La loi Hadopi I engage également la responsabilité des titulaires des abonnements internet – en l'occurrence les bibliothèques – en cas de téléchargement illicite d'œuvres protégées à partir du réseau mis à la disposition du public, uniquement si cet accès n'a pas été sécurisé.

Cette obligation de sécuriser les accès à internet se retrouve au travers de la protection des mineurs face aux contenus à caractère violent, pornographique ou portant atteinte à la dignité humaine. L'article 227-24 du *Code pénal* vient sanctionner de 75 000 euros d'amende et de trois ans d'emprisonnement le fait de permettre à un mineur de voir ou de percevoir les contenus susvisés. Pour limiter cette responsabilité, les opérateurs vont chercher des solutions au travers de mécanismes de contrôle. Sans être obligatoires, ces solutions sont laissées à la discrétion des bibliothèques qui offrent un accès à internet : mettre en place un filtrage de l'accès (une liste blanche de sites internet accessibles[18] ou une liste noire de sites dont l'accès serait bloqué), limiter les temps de connexion ou neutraliser certaines fonctionnalités pour éviter le téléchargement, demander aux utilisateurs de s'identifier ; on peut aussi préconiser l'affichage d'une charte expliquant que chacun est responsable de ses accès à internet[19], ou la mise à disposition du règlement intérieur précisant les droits et obligations qui régissent l'espace de l'accès à internet – voire la signature de contrats d'adhésion.

Ces solutions ne doivent toutefois pas contrevenir aux libertés des usagers, et en l'occurrence elles ne doivent pas restreindre la liberté d'accès à internet, reconnue à valeur constitutionnelle depuis 2009[20]. Dans la balance, entre liberté d'accès à internet et contrôle des bibliothèques, un juste équilibre reste encore à trouver... ●

Mars 2011

17. Dans la rubrique « En savoir plus », fiches pratiques.

18. Lors des débats parlementaires sur la loi Hadopi, le « filtrage blanc » avait été, à un moment, évoqué pour brider volontairement les accès publics Wifi gratuits. Vivement critiqué pour son atteinte majeure à la liberté d'accès à l'information, il a finalement été abandonné.

19. TA de Pau, 2e chambre, nos 0502107 et 0601289, 18 septembre 2007. La responsabilité de la médiathèque de Pau n'avait pas été engagée au motif qu'elle avait expressément prévu dans son règlement intérieur l'interdiction de se connecter à certains sites.

20. Décision n° 2009-580 du Conseil constitutionnel du 10 juin 2009. En ligne : www.conseil-constitutionnel.fr