Point législatif : l'accès internet en bibliothèque

- directives européennes du 12 juillet 2002 et du 15 mars 2006 :

Dans le but d'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.

- loi sur la sécurité quotidienne du 15 novembre 2001

Introduction en droit français du principe de rétention des données (l'exploitation des données techniques générées par l'utilisation d'un service de communications électroniques étant un élément indispensable de toute enquête judiciaire.) + Principe général d'effacement ou d'anonymisation de toute donnée relative au trafic

Distinction entre les données 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.

- Obligation de conservation de l'article L. 34-1 du Code des postes et des communications électroniques (CPCE)

Qui conserve ?

Une bibliothèque qui offre au public un accès à internet est soumise à cette obligation.

Quoi ?

Les « données relatives au trafic » (données techniques exclusivement)

- 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.

Les données couvertes par cette obligation sont des **données techniques de connexion** (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 :

-décret n°2010-236 du 5 mars 2010 (décret d'application de la loi dite Hadopi I)

Obligation concernant le fournisseur d'accès à internet : transmettre les données d'identification du titulaire de l'abonnement (et non de l'utilisateur) au service internet.

> aucune législation n'impose une identification des utilisateurs du réseau internet des bibliothèques.

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* », comme le contenu des SMS ou même les adresses URL des sites internet visités. (**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)

• 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 ?
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.
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 ?

Sont habilitées à avoir communication de ces données, les **autorités judiciaires**, dans le cadre défini par le **Code de procédure pénale**. (Les données de trafic ne sont conservées que pour les « besoins de la recherche, de la constatation, de la poursuite d'infractions pénales ».)

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.

Les autorités administratives ont besoin d'avoir accès à ces informations pour connaître des infractions relevant non pas du pénal mais du fiscal. 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.

La loi n°2009-669 du 12 juin 2009, favorisant la diffusion et la protection de la création sur internet, dite loi Hadopi I, 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)

Les personnes concernées peuvent accéder à leurs données en vertu des dispositions de la loi « Informatique et libertés ».

- Obligations issues de la loi « Informatique et libertés »

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 ».

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).
> Il appartient 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.
La durée de conservation de ces données est de un an.

L'article 32 de la loi « Informatique et libertés » prévoit une obligation d'informer les personnes concernées par le traitement.
> 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 ».

En conclusion :

> Les obligations issues du CPCE et de la loi « informatiques et libertés » engagent la responsabilité des bibliothèques .
> La loi Hadopi I engage la responsabilité des titulaires des 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.
> L'obligation de sécuriser les accès à Internet est laissée à discrétion des bibliothèques :
- mettre en place un filtrage de l'accès (une liste blanche de sites internet accessibles 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
- préconiser l'affichage d'une charte expliquant que chacun est responsable de ses accès à internet
- mise à disposition du règlement intérieur précisant les droits et obligations qui régissent l'espace de l'accès à internet
- la signature de contrats d'adhésion.

Source : bbf-2011-03-0053-011 :
Quelles obligations pour les bibliothèques qui souhaitent offrir un accès à internet ?
Johanna Carvais, Pascal Palut (Cnil)