arbido

2017/2 Tatorte

Grolimund Raphaël, Bibliothécaire-formateur

Milhit Igor, Spécialiste HES en information documentaire, RERO

Respecter la sphère privée des lecteurs en bibliothèque

La protection de la vie privée est un sujet qui a gagné en visibilité dernièrement et nous allons voir dans cet article en quoi cela concerne les bibliothèques. Entre considérations stratégiques, éthiques et techniques, le sujet est assez complexe et c'est ce qui le rend passionnant.

La loi fédérale sur la protection des données définit les données personnelles comme suit (LPD art. 3 al. a) :
On entend par:

> **a. données personnelles (données), toutes les informations qui se rapportent à une personne identifiée ou identifiable;**

La loi suisse ne donne pas une liste des données considérées comme personnelles. Mais si vous voulez plus d'informations à ce sujet, lisez le blog de François Charlet notamment (Charlet 2016a, 2016b, 2016c).

Non seulement il n'est pas facile de définir avec certitude si une donnée est personnelle ou non, mais en plus l'assemblage de données non personnelles est aussi à traiter avec le plus grand soin, car elles peuvent constituer un **profil de personnalité** (LPD art. 3 al. d) :

> **d. profil de la personnalité, un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique;**

De plus, il y a une sous-catégorie de données personnelles particulièrement sensibles qu'il faut traiter avec encore plus de soin: les **données sensibles**. La loi suisse les définit plus clairement que les données personnelles (LPD art. 3 al. c) :

1. **les opinions ou activités religieuses, philosophiques, politiques ou syndicales,**
2. **la santé, la sphère intime ou l'appartenance à une race,**
3. **des mesures d'aide sociale,**
4. **des poursuites ou sanctions pénales et administratives;**

Pas facile de définir ce qu'est une opinion philosophique, mais nous reviendrons sur ce point plus loin. En quoi est-ce que tout cela concerne les bibliothèques ? Elles n'ont pas de vocation commerciale et vendent encore moins les données de leurs utilisateurs ? En ce qui concerne les bibliothèques, non seulement il y a la loi à respecter, mais il y a aussi une éthique professionnelle.
En tant qu'institution traitant des données à caractère personnel, des obligations légales supplémentaires s'appliquent concernant la quantité de données récoltées, leur sécurité et

leur traitement par des tiers (LPD art. 4, 7 & 10).

Êtes-vous bien sûr que vous traitez les données de vos utilisateurs en respectant la loi ? Par ailleurs, au-delà des lois, soumises à des changements partout dans le monde en ce moment, les bibliothécaires ont aussi une déontologie à respecter. Le code d'éthique de BIS pour les bibliothécaires et les professionnels de l'information (BIS 2013) dicte au point 3 le comportement à avoir en matière de confidentialité : Les relations entre les usagers et les services documentaires demeurent confidentielles.

Les professionnels de l'information respectent la vie privée et garantissent la protection

des données personnelles qui, de fait, sont partagées entre les usagers et ces services.

Ils prennent les mesures appropriées pour garantir que les données ne soient pas utilisées

à d'autres fins que celles qui ont présidé à leur récolte.

Lorsque vous inscrivez un nouveau lecteur lui expliquez-vous clairement à quoi vont servir les données que vous lui demandez de vous fournir ? Il faudrait vous en assurer. Et si un pirate s'infiltre dans votre système ? Rappelez-vous qu'il ne pourra avoir accès qu'aux données que vous avez en votre possession. Il faudrait aussi vous poser la question si vous avez vraiment besoin de toutes les données que vous demandez à l'usager.

En plus de l'inscription, nombreuses sont les situations dans lesquelles les données des usagers peuvent être exposées à des personnes qui ne devraient pas y avoir accès. Il y a bien sûr les transactions au guichet, les échanges téléphoniques ou par e-mail, les animations, les formations, l'usage de la photocopieuse mise à disposition dans la bibliothèque, etc. Mais il ne faut pas oublier que l'usager peut interagir avec la bibliothèque sans qu'une intervention humaine ne soit nécessaire. Il peut interroger le catalogue, naviguer sur le site web de la bibliothèque et, ces dernières années, les réseaux sociaux sont venus s'ajouter à cette liste. Chacune de ces situations peut présenter des menaces dont le type et le degré de gravité diffèrent. Voyons un peu comment évaluer cela.

Modèle de menace

Selon le modèle de menace de l'Electronic Frontier Foundation (EFF), "il n'existe pas de solution unique afin de demeurer sécurisé en ligne. […] Les menaces varient en fonction de votre emplacement, de vos activités et des personnes avec lesquelles vous travaillez. En conséquence, afin de déterminer les solutions qui s'adapteront le mieux à vos besoins, vous devez effectuer une évaluation de votre modèle de menace." (EFF 2014)

Les cinq questions à vous poser pour évaluer votre modèle de menace sont (EFF 2014) :

1. Que souhaitez-vous protéger ?
2. Contre qui souhaitez-vous le protéger ?
3. Quelle est la probabilité que vous ayez besoin de le protéger ?
4. Quelles seraient les conséquences si vous échouiez ?
5. Quels désagréments êtes-vous disposé à affronter afin de vous en prémunir ? Comment

de résoudre ces problèmes ?

Comment de résoudre ces problèmes ?

Il ne faut pas céder à la tentation de se dire que tout est perdu, car s'il y a beaucoup de problèmes auxquels faire face, les solutions sont encore plus nombreuses. Le modèle de menace permet de choisir la solution la plus adaptée.
La toute première chose à faire est de réduire au strict minimum les données collectées sur les lecteurs. En listant les données actuellement demandées, on se rend compte qu'un certain nombre d'entre elles servent surtout à des fins statistiques. Si elles sont collectées, ne devraient-elles pas être anonymisées ? Et si oui, après combien de temps ?
Parmi les données collectées, l'historique de prêt revient souvent dans les discussions. Ce qu'un lecteur lit n'a-t-il pas trait à ses opinions religieuses, philosophiques, ou politiques ? Dans ce cas, ces informations sont des données personnelles sensibles (comme

nous l'avons vu plus haut) !

Nous allons passer en revue quelques choses simples qu'il est possible de changer afin de

protéger les données personnelles des lecteurs qui interagissent avec la bibliothèque. Il y

a évidemment bien d'autres situations dans lesquelles des mesures peuvent être prises, mais

nous n'avons pas assez de place pour toutes les traiter ici.
Lors des interactions au guichet, une distance de sécurité pourrait protéger les

informations des lecteurs des oreilles indiscrètes, si les locaux le permettent. De même,

les écrans sur le guichet dupliquant l'écran des bibliothécaires pour que le lecteur le

voit aussi exposent le compte du lecteur aux yeux de tous (y compris les données

personnelles). Sans parler du cas où les bibliothécaires partent aider un lecteur dans les

rayons sans verrouiller l'ordinateur…

Pour les animations, les participants doivent la plupart du temps s’inscrire. S’ils doivent remplir un formulaire, il est préférable que celui-ci se trouve sur le site web de la bibliothèque plutôt que d’avoir recourt à Google Form. S’ils doivent s’inscrire par e-mail, il convient d’utiliser une adresse hébergée par l’institution et non être une adresse fournie par une webmail commerciale. Le lieu où les messages sont stockés est important sur

le plan légal. Si une confirmation est envoyée aux participants, il est préférable de pas

utiliser un outil comme MailChimp et de tous les mettre en copie cachée. Il n’y a pas de

raison pour que quiconque ait accès aux adresses e-mail des participants. Les mêmes

considérations s’appliquent aux formations.

Si vous prenez des photos pendant l’animation, sachez qu’avoir le droit de prendre des

photos ne signifie pas avoir le droit de les partager. Il convient donc de prévoir un

formulaire de consentement à faire signer aux personnes présentes indiquant à quelles fins

les photos sont prises et comment elles seront utilisées. Elles doivent pouvoir refuser.

Ces images ne pourront être utilisées pour d’autres usages que ceux prévus et pour lesquels

les gens ont donné leur accord.

En ligne, une connexion sécurisée au site web et au catalogue est un prérequis

indispensable. Toutes les requêtes en HTTP doivent donc être redirigées vers une connexion

en HTTPS par défaut. Mais attention, certaines fonctionnalités des outils de découverte

désactivent la connexion sécurisée ! Il faut le savoir et en discuter avec le prestataire.

Il convient aussi de mettre dans la balance l’utilité de ladite fonctionnalité et le risque

encouru par le lecteur en utilisant le catalogue sans connexion sécurisée.
L'autre problème, ce sont les cookies. Ces petits fichiers texte stockent des informations dans le navigateur de l'internaute. Là encore, il s'agit de peser le pour et le contre des fonctionnalités basées sur ce mécanisme. Cela concerne notamment le partage sur les réseaux sociaux, l'affichage des couvertures de livres et la collecte de statistiques de consultation.

Avez-vous vraiment besoin de l'affichage des couvertures de livre dans le catalogue ? Sans doute. Mais doivent-elles forcément être fournies par Amazon ? Non. Avez-vous vraiment le choix ? À l'heure actuelle, pas vraiment…
Pour l'analyse de la consultation du site web, l'omniprésent Google Analytics peut facilement être remplacé par une alternative libre à héberger vous-mêmes (comme Piwik). Les données sont alors stockées chez vous et vous pouvez même les anonymiser afin d'éviter toute fuite de données personnelles.
Si vous mettez des postes informatiques à disposition dans votre bibliothèque, prévoyez une réinitialisation automatique des sessions chaque fois qu'un lecteur ferme le navigateur ou éteint l'ordinateur. Installez Firefox et configurez-le ! Définissez un moteur de recherche par défaut qui respecte la vie privée des internautes (ce n'est pas le choix qui manque), vérifiez les paramètres liés à la sécurité et la vie privée et ajoutez quelques modules complémentaires afin de garantir aux lecteurs qu'ils ne sont pas traqués, comme Privacy Badger pour bloquer les mouchards, Self-Destructing Cookies pour détruire les cookies des

onglets fermés et HTTPS Everywhere pour naviguer en HTTPS autant que possible. Vous pouvez

aussi activer la navigation privée par défaut. L'activation de certains de ces modules

peuvent rendre l'accès à certaines pages difficile, voire impossible. Oui, il existe des

pages qui ne se chargent pas si vous bloquez les pubs ! Faites des choix et informez les

utilisateurs !

Aller plus loin

Compte-tenu du rôle central des bibliothèques dans la société d'aujourd'hui, où les enjeux autour de l'information dépassent souvent ce que le grand public maîtrise, les bibliothèques ne pourraient-elles pas aller encore plus loin ? Nous pensons que oui.
Il y a déjà des formations sur la protection de la vie privée dispensées en bibliothèques (SJPL 2015; Fourmeux 2015). Pourquoi ne pas proposer un (méta)moteur de recherche basé sur searx (https://asciimoo.github.io/searx/), moteur libre et respectueux de la vie privée, et

de le configurer pour les besoins de votre communauté ? Et pourquoi ne pas aller jusqu'à

proposer aussi un nœud Tor (Library Freedom Project 2015), porte d'entrée et de sortie du

réseau d'anonymisation du même nom ?
Ce ne sont là que quelques propositions et elles ne vont pas sans une réflexion de fond.

Mais si ce sujet vous intéresse et que vous voulez aller plus loin, contactez Igor et

Raphaël. Ce sujet auquel ils s'intéressent depuis des années n'a pas fini de les

passionner. Vos questions et suggestions seront donc bienvenues !

Références

BIS, 2013. « Code d'éthique de BIS pour les bibliothécaires et professionnels de l'information » [en ligne]. 2013. http://www.bis.ch/fileadmin/re... (consulté le 30 mars 2017)
CHARLET, François, 2016a. « Initiation au GDPR (1)?: introduction et notion de donnée personnelle » [en ligne]. 1 novembre 2016. https://francoischarlet.ch/201...(consulté le 2 janvier 2017)
CHARLET, François, 2016b. « Initiation au GDPR (2)?: application territoriale » [en ligne]. 10 novembre 2016. https://francoischarlet.ch/201...(consulté le 2 janvier 2017)
CHARLET, François, 2016c. « Initiation au GDPR (3)?: consentement » [en ligne]. 8 décembre 2016. https://francoischarlet.ch/201... (consulté le 2 janvier 2017)
EFF, 2014. Une Introduction au Modèle de Menace. Autoprotection Digitale Contre la Surveillance [en ligne]. 1 août 2014. https://ssd.eff.org/fr/module/... (consulté le 18 avril 2017)
FOURMEUX, Thomas, 2015. « Kit pour protéger ses données personnelles en bibliothèque » [en ligne]. 1 décembre 2015. http://fr.slideshare.net/Bibli... (consulté le 4 décembre 2015)
LIBRARY FREEDOM PROJECT, 2015. « Tor exit relays in libraries » [en ligne]. novembre 2015. https://libraryfreedomproject....(consulté le 18 avril 2017)
SJPL, 2015. « Virtual Privacy Lab » [en ligne]. 1 octobre 2015. https://www.sjpl.org/privacy consulté le 18 avril 2017)

Raphaël Grolimund

Raphaël Grolimund est bibliothécaire-formateur à la Bibliothèque de l'EPFL et enseignant vacataire à la Haute école de gestion de Genève, filière information documentaire. Les logiciels libres et la protection de la vie privée sont intégrés dans la vie personnelle et dans ses formations depuis des années.

Igor Milhit

Igor Milhit est Spécialiste HES en information documentaire. Depuis novembre 2016, il est employé à la centrale RERO.

Abstract

Français

Le respect de la vie privée est un sujet délicat à prendre en main dans la vie de tous les jours. Ce n'est pas différent en bibliothèque. Aux contraintes légales et à la déontologie professionnelle s'ajoutent les obstacles techniques, ce qui rend les réflexions au sujet des menaces pesant sur la vie privée des lecteurs complexes et passionnantes. Malgré qu'il n'y a pas une solution à chaque problème, il est rassurant de constater qu'il y a bien plus de solutions que de problèmes. Et d'intéressantes perspectives d'avenir…

Deutsch

Das Respektieren der Privatsphäre ist ein heikles Thema, das jeden Tag wieder aufs Neue angegangen werden muss. Das ist in Bibliotheken nicht anders. Zu den rechtlichen Auflagen und den Fragen der beruflichen Ethik gesellen sich die technischen Barrieren, was die Überlegungen zur Wahrung der Privatsphäre der Benutzerinnen und Benutzer komplex aber auch spannend macht. Auch wenn es noch nicht für jedes Problem eine Lösung gibt, kann doch die beruhigende Feststellung gemacht werden, dass es bereits mehr Lösungen als Probleme gibt. Und es existieren auch interessante Perspektiven für die Zukunft…