Documentation et bibliothèques

Les données personnelles des usagers en bibliothèque : de beaux défis de gestion en perspective

The Personal Data of Library Users: Managing the Issues

Estelle Beck

Volume 64, numéro 1, janvier–mars 2018

Survivre à la gestion ?

URI : https://id.erudit.org/iderudit/1043719ar
DOI : https://doi.org/10.7202/1043719ar

Aller au sommaire du numéro

Éditeur(s)

Association pour l'avancement des sciences et des techniques de la documentation (ASTED)

ISSN

0315-2340 (imprimé)
2291-8949 (numérique)

Découvrir la revue

Citer cet article

Beck, E. (2018). Les données personnelles des usagers en bibliothèque : de beaux défis de gestion en perspective. *Documentation et bibliothèques*, *64*(1), 16–27. https://doi.org/10.7202/1043719ar

Résumé de l'article

Les données sont devenues un élément central de nos sociétés de plus en plus basées sur les nouvelles technologies et les services personnalisés. Les bibliothèques ne sont pas épargnées par cette tendance. Gérer les renseignements personnels des usagers fait donc dorénavant partie intégrante de leurs tâches et des services rendus. Pour cerner cette thématique et les enjeux la concernant, le présent article traite du cadre légal de la gestion des données au Canada et aux États-Unis, ainsi que des aspects déontologiques qui en découlent. Les différentes étapes relatives à un processus global de gestion des données sont ensuite présentées, ainsi que les solutions technologiques de nature à assurer la protection des données personnelles auprès des usagers des bibliothèques.

LES DONNÉES PERSONNELLES DES USAGERS EN BIBLIOTHÈQUE : DE BEAUX DÉFIS DE GESTION EN PERSPECTIVE

Estelle BECK
Bibliothécaire-documentaliste, Chambre des députés, Grand-Duché du Luxembourg
Présidente de l'Association luxembourgeoise des bibliothécaires, archivistes et documentalistes (ALBAD)
beckestelle@ymail.com

RÉSUMÉ | ABSTRACT

Les données sont devenues un élément central de nos sociétés de plus en plus basées sur les nouvelles technologies et les services personnalisés. Les bibliothèques ne sont pas épargnées par cette tendance. Gérer les renseignements personnels des usagers fait donc dorénavant partie intégrante de leurs tâches et des services rendus. Pour cerner cette thématique et les enjeux la concernant, le présent article traite du cadre légal de la gestion des données au Canada et aux États-Unis, ainsi que des aspects déontologiques qui en découlent. Les différentes étapes relatives à un processus global de gestion des données sont ensuite présentées, ainsi que les solutions technologiques de nature à assurer la protection des données personnelles auprès des usagers des bibliothèques.

The Personal Data of Library Users: Managing the Issues

Data have become a central element of our societies and are increasingly dependent on new technologies and personalized services. Libraries are not immune to this trend. Managing users' personal information has become an integral part of a library's activities and services. To fully grasp this challenge and the related issues, this article outlines the legal framework for data management in Canada and the United States, as well as the inherent ethical aspects. The different stages of a global data management process are presented as well as technological solutions that ensure the protection of the personal data of library users.

Introduction

Big Brother, *big data*, publicités sur mesure… les données et leurs exploitations sont devenues un élément central de notre société largement dominée par les nouvelles technologies et les services personnalisés qui y sont assujettis.

Les données personnelles des usagers, que ce soit les renseignements concernant l'adresse personnelle, les données de prêt, les données de connexion aux postes informatiques, les recherches effectuées dans les bases de données, les données de lecture des livres numériques[1], etc. font donc partie d'une information de grande valeur, qu'il importe aux bibliothèques de gérer avec soin.

Dans la littérature scientifique, les avis divergent sur la meilleure manière de gérer les données des usagers. Certains militent pour une gestion tournée uniquement vers la protection des données, tandis que d'autres pensent qu'il est bénéfique d'exploiter cette information pour évaluer les services proposés, les améliorer ou développer de nouveaux services personnalisés (Varnum 2015). Parmi ces derniers, il y a l'exemple de la New York Public Library qui a développé une application mobile demandant aux usagers de révéler leur localisation dans la ville pour pouvoir mieux les servir en leur proposant de l'information à valeur ajoutée, comme les horaires d'ouverture de la bibliothèque la plus proche (Brantley 2015). Afin de protéger ses usagers face à l'infobésité, l'American Philosophical Society Library a récemment lancé un nouvel outil de recommandations pour archives et manuscrits. Ces recommandations, proposées sur la base des données de prêt et de celles fournies par les usagers, spécifiant leurs intérêts, ont pour but de préfiltrer les résultats de recherche selon un modèle basé sur les préférences des usagers (Pekala 2017).

La gestion des données des usagers, faite de plusieurs éléments façonnables en fonction des besoins et des convictions de chaque institution, permet pourtant de combiner les deux aspects (protection et exploitation des données). Par conséquent, les bibliothèques peuvent, d'une part, offrir des services personnalisés, comme le fait toute entreprise commerciale, et d'autre part, protéger les données des usagers de manière exemplaire et respectueuse de la vie privée,

1. Cf. Beck, Estelle. La protection des données de lecture des livres numériques aux États-Unis et en France. *I2D* 53 (3) : 84

de la législation en vigueur et des principes éthiques de la profession. Cet article traite de ces différents éléments, afin de donner aux bibliothèques des ressources et des moyens adaptés à leur environnement et à leur communauté.

Quelles lois s'appliquent lorsqu'il est question de gestion et de protection des données personnelles des utilisateurs ? Quelles règles déontologiques et morales font référence dans ce domaine ? Quelles sont les étapes à respecter lors de la mise en place d'une politique globale de gestion des données au sein des bibliothèques, avec quels moyens, quels outils ? Ce sont ces différentes questions relatives à la gestion des données personnelles des usagers qui seront abordées ici.

Au Canada, la protection des données personnelles et le droit à la vie privée sont régis par un ensemble complexe de lois qui s'appliquent au secteur privé, au secteur public (dont les bibliothèques).

Les cadres législatifs en vigueur, ainsi que les aspects déontologiques et éthiques seront tout d'abord présentés. Les défis relatifs à la gestion des données personnelles, ainsi que les différentes étapes propres au traitement des données personnelles seront ensuite énoncés. Enfin, certains aspects relatifs à la gestion des données des usagers, comme les solutions techniques, la formation des usagers et la codification de politiques de confidentialité seront davantage détaillées.

Cadre légal au Canada

Au Canada, la protection des données personnelles et le droit à la vie privée sont régis par un ensemble complexe de lois qui s'appliquent au secteur privé, au secteur public (dont les bibliothèques), au secteur de la santé et à des secteurs particuliers, telles les banques.

Le Canada ayant adopté la *Déclaration universelle des droits de l'homme*[2], les citoyens canadiens sont protégés par son article 12, stipulant que « [n]ul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes[3]. »

À l'échelle fédérale, le Canada comporte deux lois majeures sur la protection des données. La première est la *Loi révisée du Canada 1985*, ch. P-21 sur la protection des renseignements personnels[4], dernièrement modifiée le 5 avril 2016. Cette loi a pour but de réglementer la protection des renseignements personnels et le droit d'accès des individus aux données les concernant. Elle ne s'applique qu'aux données traitées par les institutions gouvernementales fédérales énumérées dans la Loi.

La seconde loi sur la protection des données est la *Loi du Canada 2000*, ch. 5 qui porte sur la protection des renseignements personnels et les documents électroniques[5]. Elle a été sanctionnée le 13 avril 2000 et modifiée pour la dernière fois le 23 juin 2015 par la *Loi du Canada 2015*, ch. 32, portant sur la protection des renseignements personnels numériques[6]. Elle a pour objectif de faciliter et promouvoir le commerce électronique tout en protégeant les données et renseignements personnels collectés, exploités ou communiqués dans le cadre d'activités économiques. Cette loi s'applique donc aux fournisseurs tiers susceptibles de proposer leurs services aux bibliothèques.

Selon le *Rapport annuel au Parlement 2015-2016* du Commissariat à la protection de la vie privée du Canada[7], ces deux textes sont pourtant inadaptés aux technologies et aux comportements numériques du XXIe siècle et nécessiteraient donc une refonte en profondeur. En effet, la *Loi sur la protection des renseignements personnels* a été adoptée alors qu'Internet n'existait pas encore et la *Loi sur la protection des renseignements personnels et les documents électroniques* a été promulguée lorsque les réseaux sociaux étaient encore inexistants.

Par ailleurs, ce cadre législatif a été sérieusement menacé par le dépôt du projet de loi C-51, *Loi antiterroriste 2015*[8], qui a soulevé un débat national, mettant en évidence l'ampleur des préoccupations de la population canadienne vis-à-vis des nouveaux pouvoirs élargis de collecte et de communication de l'information, conférés aux ministères et organismes gouvernementaux. Inquiète, l'Association canadienne des bibliothèques a réagi en publiant un énoncé de positions concernant ce projet de loi[9]. Tout en étant

2. Le Canada vote pour la *Déclaration* lors de son adoption le 10 décembre 1948. Le Canada affirme ensuite son engagement envers la *Déclaration* lors de la ratification, en 1976, du *Pacte international relatif aux droits civils et politiques* et du *Pacte international relatif aux droits économiques, sociaux et culturels*.
3. <www.un.org/fr/universal-declaration-human-rights/index.html>. (Consulté le 17 octobre 2017)
4. <laws-lois.justice.gc.ca/fra/lois/p-21/index.html>. (Consulté le 17 octobre 2017)
5. <laws-lois.justice.gc.ca/fra/lois/P-8.6/>. (Consulté le 17 octobre 2017)
6. <laws-lois.justice.gc.ca/fra/loisAnnuelles/2015_32/index.html>. (Consulté le 17 octobre 2017)
7. *Le temps est venu de moderniser les outils du XXe siècle : rapport annuel au parlement 2015-2016 concernant la* Loi sur la protection des renseignements personnels et les documents électroniques *et la* Loi sur la protection des renseignements personnels. <www.priv.gc.ca/media/4161/ar_201516_fra.pdf>. (Consulté le 29 novembre 2017)
8. *Loi du Canada 2015*, ch. 20, sanctionnée le 18 juin 2015 <laws-lois.justice.gc.ca/fra/LoisAnnuelles/2015_20/>. (Consulté le 29 novembre 2017)
9. CLA Statement on Bill C-51, *The Anti-Terrorism Act, 2015*. 13 mars 2015. <cla.ca/wp-content/uploads/CLA_Stmt_C51_anti_terrorism_13mar2015_final_ltrhd-1.pdf>. (Consulté le 29 novembre 2017)

compréhensive sur les besoins accrus concernant la sécurité intérieure, l'association souligne ses préoccupations relatives aux risques que cette loi représente pour la vie privée des citoyens canadiens et pour leur liberté d'expression, ces deux notions étant essentielles au respect d'une société libre et démocratique. Malgré ces inquiétudes, également formulées par le Commissaire à la protection de la vie privée[10] Daniel Therrien, sur l'incidence de certaines dispositions du projet de loi sur la protection de la vie privée, ce projet a été adopté sans amendements.

Au Québec, la loi applicable aux traitements de données personnelles effectués par les entreprises, en remplacement[11] de la *Loi du Canada 2000*, ch. 5, est la *Loi sur la protection des renseignements personnels dans le secteur privé*[12], chapitre P-39.1. Elle est entrée en vigueur le 1er janvier 1994 et dernièrement modifiée en 2017. Par ailleurs, le chapitre troisième du *Code civil* québécois[13] est relatif au respect de la réputation et de la vie privée. Est notamment considérée comme une atteinte à la vie privée la « surveillance de la vie privée par quelque moyen que ce soit ». À l'article 35, le consentement est explicitement évoqué par les termes : « Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci y consente ou sans que la loi l'autorise. »

Les bibliothèques québécoises, qu'elles soient financées en totalité ou en partie par le gouvernement du Québec, selon leur rattachement administratif, sont, quant à elles, régies par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[14] (entrée en vigueur le 1er octobre 1982, dernièrement modifiée en 2017). Cette loi s'applique à tous les renseignements détenus par un organisme public dans l'exercice de ses fonctions, que leur conservation soit assurée par l'organisme public lui-même ou par un tiers. La forme des renseignements n'est ici pas pertinente puisque la Loi s'applique aux données écrites, graphiques, sonores, visuelles, informatisées ou autres.

En son Chapitre III, Section I, cette loi dispose que les renseignements personnels sont considérés comme confidentiels, sauf lorsque la personne concernée consent à leur divulgation. De même, la Section II (article 63.1) indique qu'un « organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support ».

Ainsi, la protection de la vie privée et des données personnelles des usagers de bibliothèques est solidement inscrite dans la législation canadienne, ce aussi bien au fédéral que dans la province de Québec. Néanmoins, les principes protégés par ce cadre législatif sont rudement mis à l'épreuve par l'environnement numérique actuel, les stratégies marketing de plus en plus agressives et les exigences de sécurité intérieure.

Cadre légal aux États-Unis

Comme c'est le cas au Canada, l'article 12 de la *Déclaration universelle des droits de l'homme* s'applique également aux États-Unis. Par ailleurs, dans la constitution[15], il existe deux principes majeurs s'apparentant à la protection de la vie privée des citoyens, considérés par les bibliothèques comme les fondements de leur mission. En effet, le premier amendement garantit la liberté d'expression et la liberté de la presse[16] et le quatrième amendement protège les citoyens de toute intrusion excessive dans leur vie privée, leurs documents ou leurs habitations[17]. Dans la *common law*, il existe également un principe de responsabilité civile pour atteinte à la vie privée, rendant responsable des dommages causés

10. Comparution devant le Comité sénatorial permanent de la sécurité nationale et de la défense au sujet du projet de loi C-51, *Loi antiterroriste 2015*, 23 avril 2015, déclaration prononcée par Daniel Therrien <www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/conseils-au-parlement/2015/parl_20150423/>. (Consulté le 29 novembre 2017)

11. Le décret d'exclusion visant des organisations de la province de Québec (DORS/2003-374) dispose dans son article 1 que : « Toute organisation, autre qu'une entreprise fédérale, qui exploite une entreprise au sens de l'article 1525 du *Code civil du Québec* et qui est assujettie à la *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., ch. P-39.1, est exclue de l'application de la partie 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* à l'égard de la collecte, de l'utilisation et de la communication de renseignements personnels qui s'effectuent à l'intérieur de la province de Québec. » <laws-lois.justice.gc.ca/fra/reglements/DORS-2003-374/page-1.html>. (Consulté le 28 novembre 2017)

12. <www.legisquebec.gouv.qc.ca/fr/showdoc/cs/P-39.1>. (Consulté le 17 octobre 2017)

13. <legisquebec.gouv.qc.ca/fr/showdoc/cs/CCQ-1991>. (Consulté le 17 octobre 2017)

14. <www.legisquebec.gouv.qc.ca/fr/ShowDoc/cs/A-2.1>. (Consulté le 30 novembre 2017)

15. Constitution of the United States. <www.senate.gov/civics/constitution_item/constitution.htm>. (Consulté le 17 octobre 2017)

16. *« Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof ; or abridging the freedom of speech, or of the press ; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances. »* Source : <www.law.cornell.edu/constitution/first_amendment>.

17. *« The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. »* Source : <www.law.cornell.edu/constitution/fourth_amendment>.

par son fait toute personne s'ingérant dans la vie privée d'autrui (Le Métayer 2010).

Parallèlement, le *Privacy Act*[18], instauré en 1974, oblige les autorités publiques à ne stocker que les données personnelles pertinentes et nécessaires à l'accomplissement de leurs fonctions. Ce *Privacy Act* est intéressant pour les bibliothèques, puisqu'il a été voté au fédéral et conçu pour contrôler les collectes, utilisations et diffusions faites des données personnelles sensibles des citoyens par le gouvernement et les agences gouvernementales. Pourtant, il n'existe aucune autorité spécifiquement dédiée à la protection des données personnelles et à la surveillance des traitements de données aux États-Unis, rendant ainsi tout contrôle de l'application de cette loi peu probable. Cet acte législatif a également le désavantage d'avoir, depuis son adoption, été décrédibilisé par le vote d'autres réglementations plus permissives.

La protection de la vie privée des usagers de bibliothèques reste finalement un droit non absolu et partiellement dépendant des décisions des tribunaux, puisque la majorité de ces textes législatifs permet l'accès aux données de prêt lors de la présentation d'un ordre de perquisition ou d'une assignation.

Parmi celles-ci, le *USA PATRIOT Act*[19], voté en 2001, a été particulièrement décrié par les professionnels de l'information, même si ces derniers reconnaissent la nécessité d'assurer la sécurité nationale. Adoptée à la suite des attentats du 11 septembre 2001, cette réglementation a été reconduite en 2006, malgré les protestations des bibliothécaires. De fait, cet acte a largement étendu le champ des investigations possibles par le Federal Bureau of Investigation (FBI) puisque la section 215 y inclut toute chose tangible, comme les livres, documents, enregistrements, etc.[20]. Sans directement mentionner les bibliothèques, ni les données de prêt et les données relatives aux connexions Internet, les termes retenus sont néanmoins assez larges pour les y englober. Un document de l'American Library Association (ALA) mentionne d'ailleurs explicitement que la section 215 du *USA PATRIOT Act* permet au FBI d'avoir accès aux données des bibliothèques, y compris aux données numériques et aux communications électroniques enregistrées[21]. Par ailleurs, le *USA PATRIOT Act* affaiblit les contraintes légales devant être respectées par le FBI lors de ses investigations, permettant aux agents gouvernementaux d'obtenir plus facilement les données, en indiquant par exemple qu'elles sont nécessaires pour leurs recherches concernant le terrorisme international. Quiconque est sollicité par le FBI à ce sujet n'a toutefois pas le droit d'informer des tiers de la visite des agents fédéraux. Ainsi, cet acte législatif oblige les bibliothèques à coopérer, sur demande, avec le FBI, en leur transmettant les données relatives aux ressources que certains usagers ont consultées, recherchées ou empruntées.

En parallèle à ces réglementations fédérales, il existe des lois sectorielles qui encadrent l'exploitation des données personnelles dans certains secteurs spécifiques, mais celles-ci restent assez parcellaires (Le Métayer 2010). Cette situation crée un environnement légal complexe et déconcertant. Ainsi, pour les bibliothèques, il existe un patchwork de 48 réglementations étatiques[22], ainsi que celle du District of Colombia, protégeant l'anonymat des usagers de bibliothèques et la non-divulgation des données de prêt des ouvrages imprimés. Parmi ces différents textes, certains mentionnent même que les données de prêt collectées dans les bibliothèques doivent être considérées comme de l'information confidentielle (Proia 2013). Malgré le fait que la grande majorité de ces réglementations ait été adoptée en réaction au Library Awareness Program des années 1970 et suivantes, lorsque le FBI s'est adressé aux bibliothèques pour identifier les espions potentiels de la guerre froide, les termes de ces lois diffèrent d'un État à l'autre. Par ailleurs, peu d'entre elles ont été mises à l'épreuve par un tribunal, ce qui aurait pourtant permis d'identifier l'étendue de la protection accordée, le type de recours possible et la responsabilité des bibliothécaires en cas de violation de la loi.

La protection de la vie privée des usagers de bibliothèques reste finalement un droit non absolu et partiellement dépendant des décisions des tribunaux, puisque la majorité de ces textes législatifs permet l'accès aux données de prêt lors de la présentation d'un ordre de perquisition ou d'une assignation. En sus, la plupart des lois autorisent explicitement l'échange de données protégées lorsque l'usager concerné en donne l'autorisation préalable ou y consent en

18. *Privacy Act of 1974*, 5 U.S.C. § 552a. <www.justice.gov/opcl/privacy-act-1974>. (Consulté le 28 novembre 2017)

19. *Public Law 107-56*, Oct. 26, 2001. <www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>. (Consulté le 28 novembre 2017)

20. *« The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution. »* Source : <www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>.

21. American Library Association, *The USA PATRIOT Act in the Library*. Source : <www.ala.org/Template.cfm?Section=ifissues&Template=/ContentManagement/ContentDisplay.cfm&ContentID=32307>.

22. Liste des réglementations étatiques établie par l'ALA : <www.ala.org/advocacy/privacy/statelaws>. (Consulté le 17 octobre 2017)

aval, tandis qu'aucune notion d'intention n'est exprimée. Un bibliothécaire divulguant les données de lecture d'un usager par inadvertance est alors tout aussi coupable qu'un tiers l'ayant effectué volontairement. Les termes de ces actes législatifs ont également le désavantage d'être trop spécifiquement tournés vers les bibliothèques et par conséquent, dans le cadre de la protection des données de lecture, de ne pas s'appliquer aux entreprises privées ni aux fournisseurs de contenus numériques. Ces derniers peuvent donc facilement être perquisitionnés par les agences gouvernementales, la plupart du temps en violation du quatrième amendement de la constitution, rendant la notion du « droit d'être seul » d'un individu quasi inexistante (Proia 2013).

Aspects déontologiques

Perçues comme des institutions garantes de la démocratie, les bibliothèques ont vocation à s'engager en défaveur de la censure, ainsi que pour la protection de la liberté d'expression et de la liberté intellectuelle. Conséquemment, la protection des données personnelles et de la vie privée des usagers est un sujet essentiel pour les professionnels des bibliothèques qui sont particulièrement attachés à ces deux notions, en reconnaissance de leur importante connexion avec la liberté intellectuelle. La confidentialité des transactions entre les lecteurs et les bibliothèques est donc explicitement défendue dans la majorité des codes déontologiques et textes éthiques de la profession, que ce soit à l'échelle internationale, aux États-Unis ou au Canada.

Ainsi, la Fédération internationale des associations et institutions de bibliothèques (IFLA) consacre tout le troisième chapitre de son code de déontologie à la protection de la vie privée des usagers, au secret professionnel et aux questions de transparence dans les termes suivants :

> *Librarians and other information workers respect personal privacy, and the protection of personal data, necessarily shared between individuals and institutions.*
>
> *The relationship between the library and the user is one of confidentiality and librarians and other information workers will take appropriate measures to ensure that user data is not shared beyond the original transaction*[23].

Par ailleurs, l'American Library Association, dans son code de déontologie[24] adopté dès 1939, souligne le rôle des bibliothèques en faveur de la protection des données des usagers en mentionnant explicitement que « *we protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted* ». Le *Library Bill of Rights* déclare également que la vie privée des lecteurs doit être protégée par les bibliothèques, en dépit de quoi les usagers risquent de perdre leur liberté de recherche et d'information[25]. Ces deux textes confèrent donc un rayonnement national à cette mission de protection des données et de la vie privée des lecteurs. Cependant, ils ont originellement été développés avant la croissance fulgurante d'Internet et la transformation de la notion de vie privée dans tous les domaines de la société. Afin d'étudier la question de la protection des données des usagers à la suite de l'avènement du numérique, l'ALA avait mandaté un groupe de travail, dont le rapport n'a toutefois pas entièrement été pris en considération. De fait, en lieu et place de retravailler ses politiques et règles de conduite professionnelle relatives à cette thématique, l'ALA a simplement rédigé une interprétation du *Library Bill of Rights*[26], complétée par une foire aux questions[27]. Par ailleurs, elle a développé un *Privacy Toolkit*[28] à destination des bibliothécaires, incluant des recommandations pour la mise en place d'une politique de confidentialité et la conduite d'un audit relatif à la protection de la vie privée au sein de leurs établissements.

Du côté canadien, le code de déontologie de l'Association canadienne des bibliothèques[29], approuvé en juin 1976, dispose en son quatrième point (§4) que les membres de la Fédération ont la responsabilité de « protéger la vie privée et la dignité des usagers des bibliothèques et de leur personnel ». Ce document ayant également été rédigé bien avant la rapide évolution du monde numérique, ce principe a été souligné dans un énoncé de position, approuvé en 1994 et dernièrement modifié en 2012, relatif à l'accès à la technologie de l'information et des communications[30]. Dans ce document, la confidentialité occupe tout un chapitre (point 5) et indique, entre autres énoncés, que

> […] *il y devrait y avoir une déclaration écrite exposant le but pour lequel des données personnelles sont recueillies.*

23. <www.ifla.org/publications/node/11092>. (Consulté le 19 octobre 2017)

24. <www.ala.org/tools/ethics>. (Consulté le 18 octobre 2017)

25. *Library Bill of Rights*, adopté en 1939 et dernièrement amendé le 23 janvier 1996 : *« Libraries should challenge censorship in the fulfilment of their responsibility to provide information and enlightenment. »* <www.ala.org/advocacy/intfreedom/librarybill>. (Consulté le 29 septembre 2017)

26. *Privacy : An interpretation of the Library Bill of Rights*, texte dernièrement amendé le 1er juillet 2014. <www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy>. (Consulté le 29 novembre 2017)

27. *Questions and answers on privacy and confidentiality*, texte dernièrement modifié le 1er juillet 2014. <www.ala.org/advocacy/intfreedom/librarybill/interpretations/qa-privacy>. (Consulté le 29 novembre 2017)

28. *Privacy Tool Kit.* <www.ala.org/advocacy/privacyconfidentiality/toolkitsprivacy/privacy>. (Consulté le 29 novembre 2017)

29. <cfla-fcab.ca/fr/lignes-directrices-et-exposes-de-position/code-de-deontologie/>. (Consulté le 28 novembre 2017)

30. <cfla-fcab.ca/fr/lignes-directrices-et-exposes-de-position/acces-a-la-technologie-de-linformation-et-des-communications/>. (Consulté le 28 novembre 2017)

La collecte de renseignements personnels devrait être limitée à ce qui est nécessaire aux fins de l'objet déterminé par l'organisme. Le consentement devrait être requis pour la collecte de renseignements personnels, ainsi que pour l'utilisation ou la divulgation ultérieure de ces renseignements.

En juin 2013, L'Association canadienne des bibliothèques s'est dite d'ailleurs préoccupée, dans un énoncé de position sur la confidentialité des télécommunications[31], du non-respect de ce principe par les organismes gouvernementaux au Canada et aux États-Unis, ainsi que par les sociétés de télécommunications et s'inquiètait de la « possible collecte illicite de renseignements privés sur le public canadien, dont le possible accès illégal aux relevés confidentiels de compte, d'emprunt et de recherche des utilisateurs de bibliothèques dans tous les secteurs des services bibliothécaires au Canada [...] ».

Au Québec, le code de déontologie de la Corporation des bibliothécaires professionnels du Québec[32] dispose également, dans ses articles 33 à 36 relatifs au secret professionnel, que le bibliothécaire doit respecter le secret « de toute information de nature confidentielle obtenue dans l'exercice de sa profession », que ce soit dans le cadre général des activités de la bibliothèque, d'une recherche confidentielle, ou au cours d'une communication documentaire, d'une entrevue ou d'une bibliothérapie[33].

Enfin, le règlement relatif au Code d'éthique des employés de Bibliothèques et Archives nationales du Québec[34] se montre encore plus directif, indiquant que les employés concernés doivent connaître la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et doivent en respecter les dispositions, de même qu'ils doivent respecter les politiques en matière de sécurité de l'information. L'article 15 mentionne également la question de la confidentialité des données en stipulant que « l'employé de BAnQ est tenu à la discrétion sur ce dont il a connaissance dans l'exercice ou à l'occasion de l'exercice de ses fonctions et il est également tenu, à tout moment, au respect du caractère confidentiel de l'information ainsi reçue ».

Lorsqu'il est question de gérer les données personnelles des usagers, toutes les recommandations déontologiques soulignent donc l'importance de protéger les données de prêts, de recherche et de toutes autres communications effectuées via Internet, ainsi que de respecter la confidentialité des échanges entre utilisateurs et professionnels.

Gestion des données des usagers

La gestion des données des usagers est composée de différentes facettes en fonction de l'objectif. Les trois principales sont : la gestion aux fins de la protection et de la sauvegarde de la confidentialité des renseignements personnels, la gestion aux fins d'analyses statistiques d'utilisation des services offerts par l'institution, et la gestion en vue d'une exploitation pour le développement et l'amélioration consécutive de nouveaux services personnalisés. Ces différents modes de gestion peuvent bien sûr être combinés. Ainsi, certaines données peu utiles pour une analyse statistique des usages, par exemple l'adresse, le numéro de téléphone ou l'adresse électronique d'un lecteur, peuvent être traitées aux fins uniques de leur protection. D'autres, telles les données relatives aux prêts, au nombre de téléchargements effectués, etc., peuvent être utilisées en tant que données statistiques pour, par exemple, continuellement réadapter la politique d'acquisition de l'institution aux besoins réels et constatés des utilisateurs. Enfin, d'autres données peuvent être exploitées dans le but de développer de nouveaux services personnalisés. De l'information détaillée sur les centres d'intérêt des utilisateurs permet, par exemple, de mettre en place un service de recommandations personnalisées, comme le montre l'expérience de la Lawrence (Kans.) Public Library[35]. Un service similaire serait, grâce à une liste précise des titres empruntés par un usager, de proposer un service semblable à celui d'Amazon — « Si vous aimez ça, vous pourriez également apprécier… » —, suggestions qui peuvent être imprimées sur les bordereaux de

Lorsqu'il est question de gérer les données personnelles des usagers, toutes les recommandations déontologiques soulignent donc l'importance de protéger les données de prêts, de recherche et de toutes autres communications effectuées via Internet, ainsi que de respecter la confidentialité des échanges entre utilisateurs et professionnels.

31. <cfla-fcab.ca/fr/lignes-directrices-et-exposes-de-position/enonce-de-position-sur-la-confidentialite-des-telecommunications/>. (Consulté le 29 novembre 2017)

32. <cbpq.qc.ca/node/479>. (Consulté le 18 octobre 2017)

33. Selon le Grand dictionnaire terminologique, la bibliothérapie est définie comme une « thérapie fondée sur la lecture pour favoriser la guérison. La bibliothérapie est utilisée pour traiter des problèmes autant émotifs que physiques. Les ouvrages utilisés pour ce faire peuvent être de nature diverse, tels des romans ou des ouvrages spécialisés ». <www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=18940028>. (Consulté le 17 octobre 2017)

34. <www.banq.qc.ca/a_propos_banq/mission_lois_reglements/lois_reglements_politiques/codes/>. (Consulté le 18 octobre 2017)

35. <americanlibrariesmagazine.org/2016/09/01/recommended-reading-readers-advisory/>. (Consulté le 5 décembre 2017).

D'autres bibliothèques ont également mis ce service en place comme, par exemple, la Kansas City Public Library <www.kclibrary.org/readers-services/personalized-reading-profile> et la St Charles Public Library <www.scpld.org/personalized-reading-list-adult>.

prêt ou envoyées par courriel lors de l'envoi d'un rappel d'échéance.

Au sein d'un même système, les données sont donc susceptibles d'être traitées différemment selon leur sensibilité et les besoins analytiques de la bibliothèque. Néanmoins, quels que soient les types de gestion envisagés, plusieurs étapes préliminaires doivent être respectées, dont :

- Inventaire des données collectées par l'institution :
  Précisément connaître quelles sont les données déjà collectées par l'institution, leur mode de stockage, leur accessibilité (qui a le droit d'accès, sous quelles conditions) et leur exploitabilité, est la première étape de toute mise en place d'une gestion globale des données des usagers.
- Identification des données collectées par les fournisseurs tiers :
  « *Libraries have to work quite hard to even know how much personally identifiable information is transmitted from the services they deliver to third parties.* » (Breeding 2016b, 6) En effet, de nombreux services proposés aux usagers sont en réalité fournis par des tiers, sur lesquels les bibliothèques n'ont que peu de contrôle (Brantley 2015). Savoir quelles données sont collectées, par quel fournisseur, comment, pour quelle finalité et dans quelles conditions de stockage, fait donc partie intégrante de l'inventaire des données des usagers indirectement collectées par la bibliothèque (Pekala 2017). Certaines données pourront d'ailleurs éventuellement se révéler utiles pour des besoins analytiques ou de développement. Les données relatives aux emprunts, collectées par l'application MeeScan proposée par Bintec Library Services[36], en sont un exemple. Ce système permet aux usagers d'emprunter les ouvrages avec leur téléphone mobile, quel que soit le lieu où ils se trouvent dans la bibliothèque, et enregistre ainsi les données de prêt qui seront ensuite utile à l'institution pour l'analyse statistique d'utilisation du fonds.
- Le cas échéant, examen des besoins analytiques précis de la bibliothèque :
  Il est important de définir clairement les résultats escomptés d'une exploitation de données. Cette définition explicite de la question ou du problème à résoudre permet alors de répertorier les données utiles pour y apporter des réponses et clairement déterminer le traitement qui sera effectué sur ces données et les conséquences pratiques correspondantes. Quelles données exactes devront être collectées/exploitées pour atteindre le but souhaité ? Qui aura accès à ces données ? Quand et comment cette information sera-t-elle utilisée ? Quel contrôle sera mis en place pour prévenir tout abus et utilisation non relative au projet initial ? Quand et comment les données seront-elles supprimées ? (Kim 2016) En effet, « *it is important that we start this process now and change our blunt practices into more strategic data collection and analysis* » (Varnum 2015, 3).
- Définition du mode de gestion à appliquer à chaque type de données inventoriées :
  Conséquemment aux étapes précédentes, une réelle politique de gestion des données peut être mise en place en fonction des objectifs à atteindre et du type de données collectées. L'idéal est de développer cette politique à partir d'un véritable cadre collaboratif pour que tous les membres de l'institution puissent faire valoir leurs intérêts et mettre en perspective leurs enjeux respectifs. Leur implication lors de la rédaction de ce document permet également d'aborder et de respecter les aspects concernant l'éthique professionnelle vis-à-vis de la protection de la vie privée, mais aussi de parler des aspects avantageux de l'exploitation des données pour le développement de services à valeur ajoutée. Ainsi, lorsque les avantages et les inconvénients auront collectivement été évalués, la confiance du personnel dans les pratiques d'exploitation des données sera plus facilement renforcée. Par ailleurs, participer à l'élaboration de la politique de gestion des données permet également, par la suite, de mieux représenter et soutenir la position de la bibliothèque face aux questions et aux préoccupations des différentes catégories d'usagers.

Ces prérequis définis, il sera alors possible de se pencher sur les étapes du processus de gestion des données personnelles.

Collecte

Face aux entreprises commerciales, très portées à exploiter les données personnelles et offrant, en contrepartie, des services hautement personnalisés, les consommateurs sont de plus en plus à l'aise avec la collecte de renseignements personnels. Cependant, il n'en demeure pas moins que cette collecte, selon la législation québécoise en vigueur, doit être effectuée avec le consentement des personnes concernées. Ce principe de consentement n'étant pas nouveau, les plateformes commerciales le sollicitent, généralement via leurs conditions générales d'utilisation et dans une terminologie teintée d'un discours hermétique difficilement compréhensible pour l'utilisateur. Ceci mène à un biais du consentement, les internautes n'étant pas nécessairement conscients de toutes les autorisations

36. <americanlibrariesmagazine.org/2017/07/19/save-staff-time/>. (Consulté le 5 décembre 2017)

effectivement octroyées concernant leurs données lorsqu'ils acceptent ces conditions générales, d'ailleurs très rarement lues. De plus, la collecte de données personnelles se fait généralement par défaut et ne laisse aux internautes que le choix, après coup, de ne plus faire partie de la liste de collecte (principe de l'*opt out*).

Pour contrer ces pratiques plus ou moins déloyales voire confuses, les bibliothèques doivent inverser la tendance et demander le consentement des usagers en amont, avant tout processus de collecte, de manière à leur permettre alors de choisir à quelles données ils souhaitent autoriser l'accès et d'en connaître leurs finalités (principe de l'*opt in*). De cette manière, c'est l'usager lui-même qui décidera dans quelles mesures il accepte la personnalisation des services assujettis à ses données personnelles et s'il en autorise la collecte à des fins clairement définies. Pour ce faire, il doit être entièrement conscient des conséquences que ce traitement aura sur ses données et, du coup, sur sa vie privée. La terminologie explicative utilisée doit donc être claire, précise et facilement compréhensible pour tout un chacun. Les termes concernant la collecte de données doivent indiquer quelles seront exactement les données collectées, dans quel but, sous quelles conditions (cryptage, anonymisation, droits d'accès, etc.), ainsi que ce qu'il adviendra des données ensuite. Par ailleurs, lors de l'utilisation d'un service personnalisé, il est important de signaler quelles sont les données minimales nécessaires et les conditions de protection des données garanties, tout en mentionnant les avantages que ce service peut apporter (Brantley 2015).

[I]l est primordial que les renseignements collectés soient automatiquement anonymisés, afin que seule l'information pouvant être analysée aux fins statistiques ou exploitée pour le bon fonctionnement de services personnalisés soit conservée.

Tout en indiquant aux usagers les services supplémentaires qui peuvent leur être proposés s'ils acceptent de fournir d'autres données personnelles (Brantley 2015), il est absolument indispensable de ne pas léser les lecteurs qui ne souhaitent pas se soumettre à ces pratiques de collecte. Ainsi les personnes non désireuses de fournir leurs données en échange de services personnalisés ne doivent pas voir pour autant leurs chances d'obtenir des services de moindre qualité. Des offres de service pleinement respectueuses de la vie privée doivent donc également être maintenues et offertes sans aucune discrimination à l'égard des pratiques d'acceptabilité.

La question se pose également sur la confiance que l'on porte aux fournisseurs de services externes, y compris ceux utilisés pour analyser l'utilisation du site Web de la bibliothèque. Google Analytics, par exemple, est particulièrement controversé, car son implémentation sur un site lui permet de collecter une image très complète du comportement de recherche d'un usager sur l'intégralité du Web. Il ne permet en effet pas seulement de savoir ce que les usagers recherchent dans le catalogue ou dans une base de données de la bibliothèque, mais aussi sur toutes les autres activités de recherche en ligne, les sites visités, les vidéos regardées, les achats effectués, etc. (Dowling 2017) Dans une optique de cohérence entre les différents services proposés par la bibliothèque, il est donc primordial d'inclure et de faire en sorte que les fournisseurs tiers, concernés par la même stratégie de collecte des données, proposent également un libre choix d'options (*opt in*) aux usagers (Ayala 2017). Selon Jessamyn West, si les fournisseurs tiers refusent de s'adapter aux exigences des bibliothèques en matière de collecte et de protection des données, ils devraient faire face aux enjeux suivants : « [They] *should not be getting their contracts renewed if they don't fix this. It's just a highlight of how little we understand what we should ask for. You'd never buy a car without seat belts, so why are these companies still in business ?* » (West 2016, 25)

Néanmoins, la collecte de données personnelles n'est pas nécessairement tout ou rien. Il peut y avoir une ouverture du côté des possibilités disponibles pour les usagers. Il est donc requis d'avoir un système restrictif par défaut, en fonction des cadres législatifs évoqués précédemment, et d'ensuite, par libre choix (*opt in*), laisser les usagers accepter la collecte et l'exploitation de certaines de leurs données en fonction de leurs besoins, leur permettant d'accéder à des services plus personnalisés. Ainsi la bibliothèque pourra mieux gérer les données personnelles en fonction des différents taux d'acceptation des usagers concernés (Breeding 2016a).

Anonymisation

« *That portion of library user data that includes personally identifiable information should be retained in that form only as long as absolutely necessary for operational purposes.* » (NISO 2015, 3)

Ainsi, il est primordial que les renseignements collectés soient automatiquement anonymisés, afin que seule l'information pouvant être analysée aux fins statistiques ou exploitée pour le bon fonctionnement de services personnalisés soit conservée. Bien sûr, l'exploitation nécessite parfois de conserver des données sensibles, comme le nom et le numéro de téléphone d'un usager lors d'un prêt. Ces données doivent être traitées avec la plus haute attention et doivent toujours être transmises cryptées. Par ailleurs, dès que leur exploitation ne nécessite plus de les garder en clair, ces renseignements doivent également être anonymisés (Breeding 2016a).

Pour une protection des données optimale, une anonymisation minutieuse est idéale. Cela signifie que non seulement les renseignements personnels concernant le prêt et les connexions doivent être anonymisés, mais également toute l'information qui permettrait une reconstitution de ces actions : le journal des transactions elles-mêmes (*log files*) et tous les renseignements personnels sauvegardés via les différentes copies de sauvegarde du système informatique, qu'ils concernent le prêt ou la transaction du prêt (Breeding 2016b). En effet, si l'anonymisation n'est pas faite intégralement, ou si seuls les noms sont supprimés, il subsiste des risques d'identification. Des pratiques commerciales d'exploration de données démontrent que quelques données anonymisées mises bout à bout peuvent aisément permettre d'identifier un individu (Dowling 2017). Il est par exemple très aisé pour Google de « réidentifier » un internaute dont les données auraient préalablement été anonymisées, ce grâce au recoupement d'information telle que l'historique des recherches et les données de géolocalisation de la personne.

Par ailleurs, les renseignements transmis via Internet et reflétant les comportements des usagers sur la Toile devraient également être minutieusement anonymisés. Comme pour la collecte, la proactivité est donc de mise pour assurer une cohérence entre le traitement interne global exprimé via la politique de confidentialité et le traitement des données relatives aux comportements numériques. Il est donc important de s'assurer que les journaux des transactions sauvegardés sur le serveur, qui contiennent généralement l'historique de toutes les recherches effectuées ainsi que les adresses IP correspondantes, soient aussi anonymisés et cryptés. Si aucun besoin analytique des données concernant le comportement numérique n'existe, cette information peut tout bonnement être supprimée des serveurs. Ce traitement doit être appliqué à tous les services électroniques proposés (catalogue, bases de données, autres interfaces de recherche, etc.), le cas échéant avec le soutien des fournisseurs externes et des institutions de tutelle (université, municipalités, etc.) concernés (Breeding 2016b).

Exploitation

Cet article n'étant pas destiné à décrire les différentes méthodes d'exploitation des données (*big data*, exploration de données, visualisation de données, etc.), seul le principe du respect de la finalité et du consentement des usagers sera évoqué ici.

En effet, lors de la collecte de données personnelles, le consentement des usagers a été accordé dans un but bien établi ou dans le cadre d'un projet précis, comme la participation à une enquête de satisfaction ou l'enregistrement de la localisation pour un service personnalisé lié au lieu où se trouve le lecteur. Cela est par exemple le cas de l'application mobile proposée par la New York Public Library depuis le 4 mai 2016 qui permet, grâce aux données de géolocalisation, de découvrir la ville de New York telle qu'elle était entre 1870 et 1970 via plus de 40 000 photos et dessins conservés dans la collection Milstein de la bibliothèque[37].

Lors de l'exploitation des données, il est extrêmement important, afin d'honorer le consentement donné et de garder la confiance des usagers, de respecter la finalité annoncée dans le cadre du protocole de collecte des données personnelles. Même s'il est parfois attrayant de se dire qu'il est possible d'exploiter certains renseignements de manière plus poussée ou dans d'autres buts que ce qui avait été annoncé lors de la collecte, ce sont des pratiques qu'il faut éviter. Lorsqu'un autre projet ou un autre service personnalisé sont en cours de développement, il est nécessaire de reformuler une demande de consentement auprès des lecteurs, adaptée à cette nouvelle finalité, toujours dans le respect d'un cadre ou d'un protocole éthique établi.

Il est également important de préciser ici que la quantité des renseignements exploités doit être proportionnelle à la finalité visée. Par conséquent, il faut restreindre l'utilisation des données, et donc en amont la collecte, à la seule information qui est fondamentalement utile pour atteindre l'objectif défini. À nouveau, cela est une marque de respect vis-à-vis du consentement des usagers et des cadres législatifs établis. De même, éviter de collecter et conserver des données inutiles pour l'exploitation permet de réduire la quantité de renseignements à gérer et, de facto, susceptibles d'enfreindre les cadres législatifs établis.

Stockage

La gestion des données des usagers ne s'arrête pas aux données « en mouvement » (celles collectées pour le prêt, nécessaires à la consultation de ressources électroniques ou exploitées aux fins statistiques). En effet, leurs conditions de stockage définitif font partie intégrante d'une politique globale de gestion des données. Pour assurer une protection constante et durable, crypter les renseignements stockés sur les différentes plateformes de sauvegarde, y compris celles de secours, doit donc d'être envisagé (Breeding 2016b).

Par ailleurs, pour éviter toute exploitation ou tout accès indu, il est primordial de formaliser les autorisations et les conditions d'accès — sur les serveurs stockant les renseignements personnels des lecteurs — allouées aux personnes en fonction de leur catégorie d'usages. Tout le personnel de la bibliothèque ne doit pas pouvoir avoir accès à toutes les données conservées.

37. <www.club-innovation-culture.fr/application-mobile-flashback-numerique-new-york/>. (Consulté le 5 décembre 2017)

Quant aux usagers, ils doivent pouvoir, en tout temps et dans la mesure du possible, avoir accès aux données personnelles sauvegardées les concernant, afin de pouvoir demander leur correction ou leur suppression (NISO 2015).

Autres aspects relatifs à la gestion des données des usagers

Les bibliothèques ont la responsabilité légale et éthique de protéger les données des usagers, puisque « *without privacy, we don't actually have free speech : you can't read, write, research, or talk freely if your every move is being monitored* » (Macrina 2016, 38). Ainsi, la protection des données fait partie intégrante de leur gestion, pour laquelle il existe de nombreuses recommandations, aussi bien techniques qu'informatives.

Aspects techniques de protection des données

Notons tout d'abord que le meilleur moyen de protéger les données des lecteurs est d'éviter au maximum de les collecter et de les sauvegarder. Ainsi, conscientes de leur responsabilité vis-à-vis des données des usagers, la plupart des bibliothèques ne conservent l'information de prêt que jusqu'au retour de l'ouvrage. Dès que la fin de la transaction de prêt est enregistrée, la ligne correspondante est alors effacée du serveur. Actuellement, cette opération n'est généralement effectuée que sur les données de prêt physiques et non pas sur ce qui touche aux ressources électroniques, alors que les bibliothèques devraient, en réalité, traiter les transactions numériques de la même manière que les transactions de prêts classiques (Pekala 2017). Bien sûr, cela vient également du fait que la plupart des transactions numériques transitent par les plateformes des vendeurs tiers et ne peuvent donc pas réellement être administrées dans le respect des politiques locales ou propres à chaque établissement.

Par conséquent, pour sécuriser les données des usagers pouvant être collectées lors de leur navigation en ligne, le protocole HTTPS est une solution idéale à implémenter à toutes les connexions Internet proposées au sein de l'établissement, y compris aux réseaux sans fil mis à disposition des usagers. Le site Web de l'institution doit également être certifié HTTPS (Dowling 2017). Ce format assure en effet la confidentialité de toutes les transactions effectuées via un navigateur, l'authenticité du site visité et l'intégrité des données échangées. Le protocole HTTPS empêche également les attaques informatiques pouvant avoir lieu intempestivement lors d'une connexion (Macrina 2016). En effet, l'information reste inintelligible pour les personnes qui n'ont pas la clé permettant de décrypter les informations et il devient alors impossible d'intercepter, de lire ou de s'insérer dans des communications électroniques. Lors de l'utilisation du protocole HTTPS, il est important de s'assurer que les techniques de cryptage à l'œuvre sont les plus récentes, car, dans le cas contraire, cette mesure s'avère moins efficace et des fuites d'information peuvent être à déplorer (Breeding 2016b).

D'autre part, il est possible de proposer, sur les bornes de consultation Internet, une navigation anonymisée grâce au navigateur Tor[38]. Cette option étant assez restrictive, il n'est pas nécessaire de la proposer par défaut, mais plutôt de la mettre à disposition sur les postes Internet pour que les usagers les plus concernés par leur vie privée puissent l'exploiter (Macrina 2016). Munir les ordinateurs offerts en libre-service à la bibliothèque d'adresses IP dynamiques, donc très difficilement traçables, est aussi une solution technique intéressante (Breeding 2016b). Une autre possibilité est de transformer toutes les adresses IP uniques en une seule adresse IP, communes à tous les postes informatiques disponibles à la bibliothèque, ce afin d'anonymiser les connexions et les comportements de chacun (Brandt 2016).

L'utilisation d'un réseau VPN, pour lequel une connexion préalable avec identifiant et mot de passe est nécessaire, est également possible. Ce système permet aux usagers de bénéficier de la protection d'un réseau fiable et crypté, quel que soit le réseau réel (éventuellement public et sans fil) depuis lequel il accède aux ressources électroniques (Dowling 2017).

Rédaction d'une politique de confidentialité

Une des actions les plus importantes lorsqu'il s'agit de protéger les données des usagers est de le formaliser et de le faire connaître auprès des usagers grâce au développement d'une politique de confidentialité ou d'un code de conduite. Ce document doit être clair et accompagné d'information facilement accessible aux usagers, leur indiquant comment ils peuvent obtenir, consulter ou modifier leurs données et les conseillant sur la meilleure manière de se protéger.

Tous les éléments propres au respect de la confidentialité des données et mis en place au sein de la bibliothèque doivent être inclus dans ce document : niveau de protection des clients Web, information sur les témoins de connexion (*cookies*), utilisation d'un mode de cryptage, conditions de stockage de l'information, limitation de l'accès aux données par les employés, procédures de sécurité informatique mises en place, normes utilisées, etc. Il peut aussi être

38. Développé en 2008 par The Tor Project, le navigateur Tor est un logiciel libre basé sur Mozilla Firefox et destiné à naviguer anonymement. Il permet d'accéder au réseau Tor et Internet de manière techniquement sécurisée, car il bloque par défaut les extensions telles que Flash et Javascript. Grâce à une extension intégrée nommée HTTPS Everywhere, il permet également de privilégier les connexions sécurisées via le protocole HTTPS. Tor est un acronyme de The Onion Router (routeur organisé en couches différentes, comme les oignons) et permet l'anonymat des internautes en reposant sur des serveurs spécifiques appelés « nœuds ».

pertinent d'ajouter une mention précisant que, bien entendu, les données collectées ne seront pas revendues, commercialisées ou louées à des tiers.

Cette politique peut également inclure des mentions spécifiques, en prévision d'une éventuelle demande de divulgation, comme une indication sur le fait que les données personnelles identifiables ne seront révélées que sur présentation d'une assignation, d'un ordre de perquisition ou d'un autre document légal, et seulement après révision de ces documents par un conseiller juridique.

Lors du processus de rédaction de la politique de confidentialité, l'idéal est d'organiser des tables rondes et des entretiens qualitatifs avec les usagers, afin de mieux cerner l'opinion du public desservi sur les questions relatives à la gestion de leurs données. Il est alors intéressant de s'enquérir sur ce qui, selon eux, doit être protégé, tout en précisant ce que la bibliothèque peut ou ne peut pas faire. À partir de là, et dans la mesure du possible, la politique de confidentialité peut être adaptée aux exigences des lecteurs. Lors de la phase de rédaction, une relecture devrait être demandée à un échantillon de personnes afin de déterminer si le texte est compréhensible et clair pour une majorité de la population (Mayer-Schönberger 2014).

Par ailleurs, de même que pour la collecte et l'anonymisation des données, rédiger de fortes politiques de confidentialité pour nos bibliothèques doit aussi signifier exiger des fournisseurs tiers des politiques de confidentialité acceptables. En tant que partenaires de nos institutions, ils doivent accepter d'indiquer publiquement quelles données ils collectent, comment ils les sécurisent, avec qui ils les partagent et combien de temps ils les conservent. Ces politiques de confidentialité devraient être disponibles en ligne pour que la bibliothèque puisse les mentionner et pour que les usagers puissent facilement les consulter (Dowling 2017).

Lors du processus de rédaction de la politique de confidentialité, l'idéal est d'organiser des tables rondes et des entretiens qualitatifs avec les usagers, afin de mieux cerner l'opinion du public desservi sur les questions relatives à la gestion de leurs données.

Formation

La formation aux usagers est un aspect crucial lorsqu'il est question de gestion et de confidentialité des données. En effet, même si une institution peut se montrer exemplaire, il est impossible d'intégralement contrôler les données traitées par les fournisseurs tiers. Il s'agit donc davantage d'informer les lecteurs au sujet des données qui sont transmises aux tiers ou qui sont collectées pour les besoins de fonctionnement des services, d'identifier les facteurs de risque et de connaître les conséquences potentielles de cette gestion (Brantley 2015).

Côté professionnel, « *our privacy policies mean little if we do not train staff to use them appropriately* » (Dowling 2017, 35). Ainsi, former le personnel de la bibliothèque sur les questions générales de gestion et de protection des données des usagers fait partie intégrante d'une politique de gestion globale. De manière générale, il serait judicieux d'envisager l'ajout de ces thématiques dans les cursus universitaires en bibliothéconomie, ou via des formations continues (Pekala 2017).

Conclusion

Les lecteurs veulent consulter l'historique de leurs recherches ou de leurs prêts, souhaitent sauvegarder et retrouver les documents sélectionnés et partager ces résultats. Les données sont donc omniprésentes dans toutes les transactions qu'un usager effectue lors de l'utilisation d'un service proposé par la bibliothèque. Pourtant, collecter, gérer et exploiter les données des usagers ne signifie pas nécessairement violer leur vie privée si ces pratiques sont faites de manière transparente et cohérente.

Développer une politique globale de gestion des données signifie aussi bien porter la responsabilité de leur confidentialité que respecter la confiance des lecteurs vis-à-vis des utilisations faites avec leurs données. Les bibliothèques doivent donc démontrer qu'elles protègent les données autant que possible tout en les exploitant de manière raisonnée et anonyme. Il est également important d'informer les lecteurs sur toutes les étapes de la gestion de leurs données et sur ce qu'il est susceptible de se produire avec leurs données en cas de problèmes ou de malversations.

En définitive, même si la protection des données des usagers est un élément essentiel de l'éthique et des pratiques des bibliothécaires, il est nécessaire, si les bibliothèques souhaitent continuer à concurrencer les plateformes commerciales riches en services personnalisés, de développer et de proposer des services similaires, tout aussi fluides et intuitifs. Pour atteindre cet objectif, les bibliothécaires, dans leur politique de gestion des données, doivent savoir faire un choix équilibré entre sécurité et exploitation des renseignements personnels des usagers pour leur fournir la valeur ajoutée escomptée. La clé est de donner aux usagers et à la communauté toute l'information et les options technologiques leur permettant de décider eux-mêmes, et en connaissance de cause, du sort de leurs données.

SOURCES CONSULTÉES

Ayala, Daniel. 2017. Security and privacy for libraries in 2017. *Online Searcher* 41 (3) : 48–52.

Brandt, Peter. 2016. A better browser experience : UX meets patron security and confidentiality. *Computers in Libraries* 36 (8) : 4–7.

Brantley, Peter. 2015. Books and browsers : Privacy for digital library patrons. *Publishers Weekly* 262 (1) : 20–21.

Breeding, Marshall. 2016a. High security and flexible privacy for library services. *Computers in Libraries* 36 (5) : 12–15.

Breeding, Marshall. 2016b. Issues and technologies related to privacy and security. *Library Technology Reports* 52 (4) : 5–12.

Dowling, Thomas. 2017. Paths to protecting patron privacy. *International Information & Library Review* 49 (1) : 31–36.

Kim, Bohyun. 2016. Cybersecurity and digital surveillance versus usability and privacy : Why libraries need to advocate for online privacy. *College & Research Libraries News* 77 (9) : 442–451.

Le Métayer, Daniel & Guillaume Piolle. 2010. Droits et obligations à l'ère numérique : protection de la vie privée. In *L'usager numérique : Séminaire INRIA, 27 septembre — 1er octobre 2010.* Paris : ADBS Éditions, 63–88.

Macrina, Alison. 2016. Protection patron privacy. *Library Journal* 141 (12) : 38–39.

Mayer-Schönberger, Viktor & Kenneth Cukier. 2014. *Big data : la révolution des données est en marche.* Paris : Robert Laffont.

NISO. 2015. *NISO Consensus Principles on Users' Digital Privacy in Library, Publisher, and Software Provider Systems (NISO Privacy Principles)*. Consulté le : 20 octobre 2017. <www.niso.org/apps/group_public/download.php/15863/NISO%20Consensus%20Principles%20Users%20Digital%20Privacy.pdf>.

Pekala, Shayna. 2017. Privacy and user experience in 21st century library discovery. *Information Technology and Libraries* 36 (2) : 48–58.

Proia, Andrew A. 2013. A new approach to digital reader privacy : Tate regulations and their protection of digital book data. *Indiana Law Journal* 88 (4) : 1593–1618.

Varnum, Ken. 2015. Editorial board thoughts : Library analytics and patron privacy. *Information Technology and Libraries* 34 (4) : 2–4.

West, Jessamyn. 2016. Cybersecurity as an extension of privacy in libraries. *Computers in Libraries* 36 (5) : 24–25.