UNIVERSITÉ DE LYON

Diplôme de conservateur de bibliothèque

Mémoire d'étude / mars 2019

La protection de la vie privée des lecteurs par les bibliothécaires français

Marion CHOVET

Sous la direction de Damien Belvèze
Chargé de la formation des usagers– Service commun de documentation – Université Rennes 1

enssib

Remerciements

Je tiens d'abord à remercier Damien Belvèze, mon directeur de mémoire, pour sa très grande réactivité, ses conseils précieux, ses relectures attentives et son accompagnement tout au long de ce travail.

Je remercie l'ensemble des personnes qui ont contribué à ce travail, et notamment aux très nombreux collègues qui ont répondu à l'enquête et qui l'ont partagée, mais également Vincent Boulet Estelle Graf, Jérôme Kalfon, Corine de Munain, Claire N'Guyen, Isabelle Ressouche pour avoir répondu à mes sollicitations et m'avoir accordé du temps lors d'entretien mais également partagé des documents internes.

Je remercie Sylvie Chevillotte et Catherine Renard pour leurs encouragements et leur veille attentive.

Enfin, mes remerciements à mes collègues de la promotion Benoîte Groult pour leur bonne humeur, et leur bienveillance.

Résumé :

40 ans après la Loi Informatiques et Liberté, l'entrée en vigueur du Règlement européen pour la protection des données à caractère personnel en mai 2018, a été de l'occasion de se demander, à nouveau, quelle était la responsabilité des bibliothécaires vis-à-vis de la vie privée de leurs usagers. Cette étude vise à présenter les grands principes juridiques, mais également déontologiques qui permettent aux professionnels d'assurer la protection de la vie privée des lecteurs. Il s'agit également d'étudier comment assurer cette protection à l'heure du numérique, et comment les bibliothécaires peuvent se positionner sur le sujet, notamment en opérant des choix en faveur d'outils et services protecteurs de la vie privée. Nous verrons enfin comment les bibliothèques peuvent former et communiquer avec leurs pairs et leurs usagers sur ce droit fondamental.

Descripteurs : Droit à la vie privée

Fonctionnaires – Déontologie

Identité numérique

Informatique et liberté

Internet – Droit européen

Protection de l'information (informatique)

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Traces numériques

Abstract :

40 years after the Data Protection Act and the entry into force of the European Regulation for the Protection of Personal Data in May 2018, was the appropriate moment to ask again, what the responsibility of librarians is regarding the privacy of their users. This study aims to present the main legal principles, but also ethical principles that allow librarians to protect the privacy of readers. It also aims to discuss how this protection can be ensured in the digital age, and how librarians can position themselves on the subject, in particular by making use of privacy

protection tools and services. Finally we discuss how libraries can communicate with and train their peers and their users on this basic right.

Keywords :

Right to privacy, Officials – Ethics, Numeric identity, Internet and freedom, Internet - European Law

Information Protection (IT)

Regulation (EU). 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Droits d'auteurs

Sommaire

Sigles et abréviations

ABES : Agence bibliographique de l'enseignement supérieur
ABF : Association des Bibliothécaires de France
ALA : American Library Association
ANSSI : Agence nationale de la sécurité des systèmes d'information
BIS : Bibliothèque interuniversitaire de la Sorbonne
BIU : Bibliothèque interuniversitaire
BIUS : Bibliothèque interuniversitaire de santé
BnF : Bibliothèque nationale de France
BNU : Bibliothèque nationale et universitaire de Strasbourg
CDFUE : Charte des droits fondamentaux de l'Union européenne
CEDH : Cour européenne des droits de l'homme
CEDH : Convention européenne des droits de l'homme
CIL : Correspondant informatique et liberté
CJUE : Cour de Justice de l'Union Européenne
CNIL : Commission nationale de l'informatique et des libertés
CNRS : Centre national de la recherche scientifique
COMUE : Communauté d'universités et établissements
CPU : Conférence des présidents d'université
DANE : Délégation académique au numérique éducatif
DPD : Délégué à la protection des données
DPO : Data protection officer
DRM : Digital rights management
DSI : Direction des systèmes d'information
GAFAM : Google Apple Facebook Amazon Microsoft
HATVP : Haute Autorité pour la Transparence de la Vie publique
IFLA : International Federation of Library Associations and Institutions
IP : Internet protocol
ISNI : International standard name identifier
LQDN : La Quadrature du net
MOOC : Massive open online course
OCLC : Online Computer Library Center
ORCID : Open researcher and contributor ID
RGPD : Règlement général pour la protection des données
RSSI : Responsable de la sécurité des systèmes d'information
SCD : Service commun de documentation
VIAF : Virtual international authority file

INTRODUCTION

La confidentialité, la vie privée des usagers en bibliothèques est une question déjà ancienne, avant même l'existence du numérique. Ainsi dans *L'homme sans qualité*[1], le bibliothécaire apporte au Général Stumm les livres de la femme qu'il aime sans l'accord de celle-ci et dévoilant ainsi ce qu'on peut considérer comme une part de sa vie privée. Les bibliothécaires n'ont pas toujours été les chantres de la liberté, que certains vantent aujourd'hui. Les registres de lecture (ou emprunts sur place) n'avaient manifestement pas de caractère confidentiel au XIXe siècle. Et à la fin du XXe siècle les bibliothécaires au départ ont été relativement frileux dans le fait de proposer internet à leurs usagers et ont défini des usages légitimes qui n'ont cessé de s'élargir. Il y a peu, nous étions censés rappeler aux étudiants que les ordinateurs étaient réservés à la recherche documentaire et non pas pour surfer sur les réseaux sociaux. Aujourd'hui, Twitter sert de média à la communication scientifique et il ne viendrait à l'idée de personne de limiter l'accès aux réseaux sociaux.

En 1974, un projet gouvernemental visant à identifier chaque citoyen par un numéro et d'interconnecter, via ce numéro, tous les fichiers de l'administration et qui créa une vive émotion dans l'opinion publique. Une commission Informatique et Libertés fut alors créée et celle-ci proposa de créer une autorité administrative indépendante. En 1978, la première loi sur les questions liées à l'informatique[2], au numérique a été votée. Le législateur a eu pour objectif de protéger les individus face aux dérives potentielles du numérique. La Loi Informatique et Libertés de 1978 a permis la création d'une autorité administrative indépendante : la Commission nationale de l'informatique et des libertés (CNIL). Initialement la CNIL régissait essentiellement la confidentialité du contenu des registres des lecteurs et de leurs emprunts.

Avec l'apparition d'internet, du web 2.0, la dématérialisation des procédures de service public, les big data, la question de la confiance face aux usages du numérique est au cœur des préoccupations des citoyens. Une conciliation plus exigeante doit être opérée entre liberté d'expression et sauvegarde de l'ordre public, liberté d'information et protection de la vie privée, sûreté et lutte contre la criminalité.

Le droit à la protection des données personnelles est né en réponse aux questions posées par l'essor du numérique. S'il est souvent présenté comme se rattachant à la vie privée, ses enjeux sont plus larges, et peut être considéré comme un droit fondamental.[3] L'évolution des comportements à l'égard de la vie privée, notamment sur internet, est parfois comparée la révolution sexuelle des années 60. Une certaine

---

[1] N'empêche, mon ami, lui dis-je, qu'il n'est pas commode de vous expliquer ce que je cherche à lire !"« Et que penses-tu qu'il m'ait répondu ? Il me regarde avec modestie, hoche la tête et dit : "Avec votre permission, mon général, cela peut arriver. Il n'y a pas si longtemps, une dame me parlait qui m'a dit exactement la même chose ; peut-être la connaissez-vous, mon général, cette dame est la femme de M. le sous-secrétaire Tuzzi, du Ministère des Affaires étrangères."« Hein, qu'est-ce que tu en dis ? Je te promets que j'ai accusé le coup ! Et comme le vieux s'en aperçoit, ne faut-il pas qu'il m'amène tous les livres que Diotime se fait réserver là-bas ! Maintenant, quand je vais à la Bibliothèque, c'est positivement comme un mariage spirituel clandestin : ici ou là, prudemment, je note un signe ou un mot au crayon dans la marge, sachant qu'elle le trouvera un jour prochain sans soupçonner le moins du monde qui s'est ainsi glissé dans ses pensées au moment où elle se demande ce que cela peut vouloir dire ! ». MUSIL. R. L'homme sans qualité. Editions du Seuil, 2004. Tome 1, page 519.

[2] FRANCE. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Journal officiel de la République française. [en ligne]. Disponible à l'adresse : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460

[3] CONSEIL D'ETAT. *Etude annuelle 2014, le numérique et les droits fondamentaux*. La documentation française, 2014, p.5

désinhibition des jeunes générations devra les obliger maitriser les risques engendrés par cette liberté. Les bénéfices de cette liberté sont ressentis comme dépassant ses inconvénients.

L'entrée en vigueur du Règlement général pour la protection des données (RGPD) en mai 2018 a donné l'occasion aux professionnels des bibliothèques de réévaluer l'importance du respect des données personnelles de leurs lecteurs dans le champ de leurs pratiques et préoccupations professionnelles. Selon l'enquête menée dans le cadre de ce travail, on note un très bon niveau de première information des bibliothécaires sur le RGPD, parmi les répondants à notre enquête, plus de 94% des conservateurs ont été informés sur le RGPD, 100% des bibliothécaires, 90% des catégories B, et 100% des catégories C.

La technologie étant en constante évolution, souvent complexe, les technologies numériques sont souvent non (ou mal) maîtrisées par les acteurs du monde des bibliothèques, mais aussi par leurs publics. Un outil n'est jamais neutre, il faut autant que possible connaître son fonctionnement, avoir accès à sa structure, afin de connaître les impacts politiques et sociétaux au moment du choix. Comme le préconise le rapport de Terra Nova « L'école sous algorithme », il s'agit

> *d'inviter les acteurs publics à chercher les moyens de reprendre la main sur les choix stratégiques à faire en matière de numérique éducatif, à la fois au niveau pédagogique (moteurs de recherche, ressources en ligne, applications d'adaptive learning) et administratif (logiciels d'affectation type Affelnet ou APB, logiciels d'emploi du temps, espaces numériques de travail)*[4].

Ces préconisations peuvent être appliquées au monde des bibliothèques (qui est un des acteurs du monde pédagogique), les enjeux étant très proches.

Il s'agit donc d'étudier quelle est la responsabilité des bibliothécaires français vis-à-vis de la protection de la vie privée de leurs usagers. Quelle place les bibliothécaires français accordent-ils au respect de la vie privée des usagers de bibliothèques dans la déontologie ? Quelles actions sont mises en œuvre par les bibliothèques pour prévenir les fuites de données personnelles ou prendre les mesures pour rendre les usagers autonomes dans la gestion en ligne de ces données?

Avec l'entrée en vigueur du RGPD, la question de la marchandisation des données personnelle a été souvent abordée. Nous avons choisi de ne pas traiter ce sujet dans ce mémoire, s'agissant d'une réflexion plus économiste et fiscaliste que bibliothéconomique. Il faut néanmoins garder à l'esprit, que selon une étude menée en 2013 par le cabinet de conseil McKinsey en 2013[5], l'exploitation des données des étudiants (pour la mise en place d'algorithmes censés faciliter l'apprentissage - *Learning Analytics*- et orienter les étudiants et finalement les rendre plus employables à l'issue de leurs études) pourrait générer de 849 à 1 133 milliards d'euros de bénéfice à l'échelle planétaire.

Compte tenu de l'actualité du sujet avec l'entrée en vigueur du RGPD, et la diversité des bibliothèques (pour ne pas dire la totalité) ayant à traiter de la question de la vie privée, nous avons fait le choix de mener une enquête auprès des

[4] AGACINSKI, D ; BRUN, F, ISART, C, JAMES, M. L'école sous algorithmes. Terra Nova, [en ligne. 10 mars 2016. Disponible à l'adresse : http://tnova.fr/etudes/l-ecole-sous-algorithmes

[5] https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information

professionnels des bibliothèques. Cette enquête nous a permis de récolter de très nombreuses données, par type d'établissement mais également sur l'appréhension de la question selon les catégories de personnel ou bien leurs fonctions au sein des établissements.

730 personnes ont répondu à l'enquête, mais nous avons pris le parti de n'exploiter que les questionnaires complets soit 60,14% (439 réponses complètes) de l'ensemble. Les répondants avaient la possibilité de s'exprimer librement à la suite de certaines questions, ce qui nous a permis de recueillir quelques retours qualitatifs, questionnements ou retour d'expérience.

Pour compléter cette enquête, nous avons sollicité quelques rares entretiens auprès de personnels de bibliothèques ayant à traiter de la question des données personnelles dans des domaines soit plus techniques (par exemple les fichiers d'autorités, ou les ressources électroniques) ou bien ayant une vision d'ensemble de la question au sein d'un établissement (comme la DPO – Data Protection Officer de la Bibliothèque nationale de France).

Nous avons également étudié la littérature professionnelle, les ressources disponibles sur les sites internet d'institutions officielles comme la CNIL, d'associations (comme La Quadrature du Net). S'agissant des débats, sur le rôle du bibliothécaire en matière de protection de la vie privée, soulevés (ou bien réactivés) au sein de la profession par l'entrée en vigueur du RGPD, nous avons consulté les listes de diffusion d'échanges entre professionnels (comme les listes ADBU ou Couperin) mais également les prises de position de bibliothécaires sur des forums (comme Agorabib), sur leurs blogs personnels ou via les réseaux sociaux. Enfin, lors de nos recherches nous avons également pu récolter des informations par sérendipité.

Nous verrons donc dans un premier temps le cadre juridique et déontologique dans lequel les bibliothécaires doivent s'inscrire, et dans un second temps comment les professionnels peuvent assurer une protection de la vie privée des lecteurs. Enfin nous étudierons comment les bibliothécaires devront opérer des choix, et enfin communiquer sur leurs actions, leurs politiques, leurs offres de formations.

CADRE JURIDIQUE ET DEONTOLOGIQUE

Depuis Aristote la vie privée est définie comme la survie, le règne de la nécessité à laquelle il faut pourvoir, tandis que la vraie vie, celle qui nous définit, en tant qu'animaux politiques, est la vie politique. La philosophie parle de la personne et de la manière dont elle se constitue à partir de son intimité qu'elle doit à ce titre préserver. Du point de vue philosophique, le droit à la vie privée est sans limite extrinsèque. Seul le sujet est en mesure d'assigner des limites à son droit à la vie privée dans la mesure où il en a besoin pour entrer en contact avec les autres.

Comme l'indique Jean-Louis Halpérin, dans son article « Protection de la vie privée et privacy : deux traditions juridiques différentes ? », la notion de vie privée apparaît en France lors de débats sur la presse dans le projet de Constitution en 1791 :

> *Dans un climat de suspicion à l'égard de la presse la plus révolutionnaire, accusée par de nombreux Constituants d'appeler à la désobéissance aux lois, fut voté un article (inséré dans le chapitre V, titre III, article 17 de la Constitution de 1791) qui limitait les délits de presse à la provocation aux crimes et délits, à la calomnie volontaire contre les fonctionnaires publics et aux « calomnies et injures contre quelques personnes que ce soit relatives aux actions de leur vie privée »*

Aux Etats-Unis, en 1890, est publié dans *Harvard Law review* « The right to privacy »[6], une première définition moderne de la vie privée. Selon les auteurs, S. Warren et L Brandeis, la vie privée est constituée de trois éléments : le secret, la quiétude et l'autonomie.

Par ailleurs, on distingue différents types d'intimité (privacy).

- Physical/ accessibility privacy : intimité physique ou droit d'être laissé seul dans un espace physique donné
- Psychological/mental privacy : intimité psychologique ou droit d'être indemne de l'influence d'autrui dans la construction de sa pensée
- Decisional privacy : intimité dans la prise de position ou droit d'être indemne de l'influence d'autrui pour faire des choix
- Informational privacy : droit d'être indemne des intrusions d'autrui en préservant dans le secret un ensemble de faits à propos de la personne

Comme l'analyse Martin Untersinger[7], ces trois éléments peuvent se transposer dans la sphère numérique. Selon lui, le secret serait « la capacité d'un individu à contrôler la collecte et l'utilisation de ses données personnelles ou la possibilité de choisir quand ses attitudes, croyances et comportements et opinions doivent être partagés avec ou cachés des autres ». Se ménager une zone de quiétude consiste à pouvoir s'isoler de la société et ne pas subir une intrusion des autres ; c'est non seulement une question d'espace mais également de communication. Enfin l'autonomie c'est la possibilité de se définir, son identité, ses opinions, sa manière de vie.

[6] WARREN, Samuel D, BRANDEIS, Louis D. « The Right to Privacy » *Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220. Disponible à l'adresse : https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

[7] UNTERSINGER, M. Anonymat sur Internet. Eyrolles, 2ème ed. 2014 ; p.4

Avec le numérique, certains sont partisans d'un dépassement de l'aspiration à la vie privée, en faveur d'un mouvement de « publicisation de soi », et d'autres soutiennent, comme Antonio Casilli[8] que cette aspiration n'a pas disparu mais a seulement changé de contenu ; il ne s'agit plus seulement d'être dans une zone de quiétude, à l'abri des intrusions, mais aussi de maîtrise son image, sa réputation.

L'investissement affectif de la vie privée est un phénomène moderne qui a connu des éclipses malheureuses. Selon Hannah Arendt le but du totalitarisme est le suivant : « la domination permanente de chaque individu dans chaque sphère de sa vie ». Il s'agit donc de régenter tous les aspects de vie individuelle, sa vie publique aussi bien que sa vie privée. D'où les dystopies modernes qui conjuguent totalitarisme plus ou moins fort et disparition de la vie privée comme dans l'ouvrage « The Circle » de Dave Eggers paru en 2012 et dans lequel les employés d'une firme, géante du Web, doivent partager la totalité de leurs données personnelles. Il s'agit donc là d'un totalitarisme digital.

Cette sphère a vocation à rester à l'abri des regards d'autrui. Le droit au respect de la vie privée est protégé au titre des droits de la personnalité. Plusieurs textes, nationaux et internationaux définissent le champ de protection de la sphère privée.

LA VIE PRIVEE DANS LES TEXTES DE LOI

Inconnue sous l'Ancien Régime, la notion de vie privée est apparue de façon très éphémère au 19ème siècle et dans le cadre de législations et jurisprudence relatives à la presse, et la diffamation. Le droit au respect de la vie privée a été introduit dans le droit français par la loi n° 70-643 du 17 juillet 1970. L'article 9, alinéa 1er, du code civil dispose que « chacun a droit au respect de sa vie privée ».

La notion de vie privée figure également à l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentale. Cet article renvoie plus largement à la « vie privée et familiale », et aux notions de protection de « domicile » et de « correspondances »

Le droit au respect de la vie privée a également valeur constitutionnelle. En effet, c'est un droit subjectif que le Conseil constitutionnel a fait entrer dans le bloc de constitutionnalité en le rattachant à l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 (Cons. const. 23 juill. 1999)[9].

Définition

La vie privée est la sphère d'intimité de la personne. Elle se définit par opposition à la vie publique.

Cette sphère a vocation à rester à l'abri des regards d'autrui. Le droit au respect de la vie privée est protégé au titre des droits de la personnalité. Plusieurs textes, nationaux et internationaux définissent le champ de protection de la sphère privée.

[8] CONSEIL D'ETAT. *Etude annuelle 2014, le numérique et les droits fondamentaux*. La documentation française, 2014, p. 68

[9] CONSEIL CONSTITUTIONNEL. Décision N°99-416 DC du 23 juillet 1999 [en ligne]. Disponible à l'adresse https://www.conseil-constitutionnel.fr/decision/1999/99416DC.htm

Plusieurs d'entre eux d'ailleurs imposent la protection de la sphère privée, mais sans en donner une définition bien précise.

Les textes fondamentaux qui régissent la protection de la vie privée sont le Code civil français, le Code pénal français, la Déclaration universelle des droits de l'Homme, la Convention européenne des Droits de l'Homme (CEDH)[10] et la Charte des droits fondamentaux de l'Union européenne[11].

L'article 12 de la Déclaration universelle des droits de l'homme énonce « Nul 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. »

L'article 8 de la CEDH est consacré au respect de la vie privée et familiale

> *Droit au respect de la vie privée et familiale 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.*[12]

L'article 7 de la Charte des droits fondamentaux de l'Union européenne énonce que « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ».

En vertu de l'article 9 du Code civil, et de son interprétation par la jurisprudence, toute personne, quels que soient son rang, sa naissance, sa fortune, ses fonctions présentes et à venir, a le droit au respect de sa vie privée.

Le droit au respect de la vie privée est une notion difficile à délimiter : en effet, ni l'article 9 du Code civil ni l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales n'en donnent de définition précise. Ces articles ne donnent pas non plus une liste précise des droits protégés au titre du droit au respect de la vie privée.

La jurisprudence est donc intervenue afin de faire entrer dans le domaine de la vie privée l'image (Civ. 2e, 5 mars 1997), le sexe (CEDH 25 mars 1992, *Van Oosterwijck c/ Belgique*) , la vie familiale et les origines familiales (Civ. 1re, 16 oct. 1984, Bull. civ. I, n° 268), la santé (Civ. 1re, 6 juin 1987), la voix (Paris, 12 janv. 2005), les convictions personnelles, philosophiques et religieuses (Civ. 1re, 12 juill. 2005), le domicile (Civ. 2e, 5 juin 2003), la vie sentimentale (Civ. 1re, 6 oct. 1998), la mort (Civ. 1re, 20 déc. 2000)…

---

[10] CONSEIL DE L'EUROPE. Convention de sauvegarde des droits de l'Homme et des libertés fondamentales.[en ligne]. 4 novembre 1950. Disponible à l'adresse : https://www.echr.coe.int/Documents/Convention_FRA.pdf

[11] UNION EUROPEENNE. Charte des droits fondamentaux de l'Union européenne. [en ligne]. 18 décembre 2000. Disponible à l'adresse : http://www.europarl.europa.eu/charter/pdf/text_fr.pdf

[12] CONSEIL DE L'EUROPE. Convention de sauvegarde des droits de l'Homme et des libertés fondamentales.[en ligne]. Article 8. 4 novembre 1950. Disponible à l'adresse : https://www.echr.coe.int/Documents/Convention_FRA.pdf

Les données personnelles, un élément de la vie privée

La Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, datant de 1953, ne comporte pas d'article spécifique aux données personnelles. La Cour européenne des droits de l'homme s'est donc appuyée sur l'article 8 de la Convention pour affirmer que « la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention »[13]

L'article 8 de la Charte des droits fondamentaux de l'Union européenne reconnaît le droit à la protection des données personnelles. Il faut souligner que la Charte distingue la protection de la vie privée de celle des données personnelles. Ce choix a été expliqué par G. Braibant comme l'importance des enjeux liés aux données personnelles (notamment en matière de bioéthique ou de l'informatique). On peut également rajouter que la protection des données personnelles est non seulement une garantie du droit à la vie privée, mais plus largement une protection d'autres libertés publiques que sont la liberté d'expression, la liberté syndicale ou encore la liberté religieuse[14].

En 2011, le Conseil d'Etat, dans une décision, en se référant à plusieurs textes (Loi du 6 janvier 1978, CEDH, Convention internationale des droits de l'enfant) a énoncé que :

> *l'ingérence dans l'exercice du droit de toute personne au respect de sa vie privée que constituent la collecte, la conservation et le traitement, par une autorité publique, d'informations personnelles nominatives, ne peut être légalement autorisée que si elle répond à des finalités légitimes et que le choix, la collecte et le traitement des données sont effectués de manière adéquate et proportionnée au regard de ces finalités .*

Il s'agissait en l'occurrence de collecter des empreintes digitales pour des passeports biométriques.[15]

Un droit fondamental à protéger

Dès 1978, le législateur a voulu protéger les libertés fondamentales et l'individu face à la toute puissance des technologies numériques.

Le rôle majeur de la CNIL

La Commission nationale de l'informatique et des libertés occupe un rôle central dans la protection des données à caractère personnel en France. La CNIL est donc l'autorité nationale de contrôle pour l'application du RGPD. Elle prend en charge la publication de référentiels, de codes de bonne conduite et de règlements types sur les nouvelles obligations des opérateurs. Elle peut certifier des organismes et des services. Elle peut être consultée par le Parlement sur les questions de données personnelles. Ses missions, prévues à l'article 11 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, sont les suivantes :

---

[13] CEDH, Gde Ch. 4 décembre 2008, S. et Marper C. Royaume-Uni, n°30562 /04 et 305566 :04 chhttps://rm.coe.int/16806ae19a

[14] CONSEIL D'ETAT. *Etude annuelle 2014, le numérique et les droits fondamentaux*. La documentation française, 2014, p.81

[15] CE, Ass.26 octobre 2011, n°317827, Rec. p.505

- information des personnes concernées et des responsables de traitement ;

- fonction consultative auprès du Gouvernement ;

- participation à la définition du cadre normatif sur la protection des données personnelles ;

- mise en conformité des traitements ;

- avis, approbation ou création d'instruments de « droit souple » ;

- certification de méthodologies d'anonymisation, notamment en vue de la réutilisation des bases de données publiques mises en ligne ;

- conduite de la réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques ;

- promotion de l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données.

La CNIL communique également sur la protection de la vie privée auprès de l'ensemble des citoyens. Afin de sensibiliser le jeune public sur la protection de sa vie privée, a ainsi fait appel en juin 2017 à un célèbre youtubeur *Le Rire Jaune* pour faire une vidéo « Protéger sa vie privée en 6 étapes[16] ». En février 2019, le compteur Youtube indique près de 6 millions de vue, l'objectif a été visiblement atteint.

La CNIL, en tant qu'autorité administrative indépendante a aussi un pouvoir de contrôle et de sanctions en cas de manquement aux obligations du RGPD. Elle peut donc contrôler les organismes à la suite de plaintes qu'elle reçoit, de signalements qui lui sont faits, ou parce qu'elle décide de se saisir d'un cas particulier. Le contrôle peut s'effectuer dans les locaux de l'établissement concerné, sur pièces ou même en ligne. En cas de manquement, la CNIL peut prononcer une mise en demeure (il ne s'agit pas d'une sanction mais une demande adressée à un responsable de traitement ou à un sous-traitant, de cesser un ou plusieurs manquement(s) constaté(s) au RGPD dans un délai fixé) ou bien des sanctions. Il existe plusieurs types de sanctions : « *Prononcer un rappel à l'ordre ; Enjoindre de mettre le traitement en conformité, y compris sous astreinte ; Limiter temporairement ou définitivement un traitement ; Suspendre les flux de données ; Ordonner de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte, Prononcer une amende administrative* »[17].

La protection par le Code civil et le Code pénal

Lorsque le respect de la vie privée d'une personne est menacé par une utilisation détournée de ses données personnelles, plutôt que de recourir à la loi Informatique et Libertés, il peut être plus efficace de recourir au Code civil (article 9). L'article 9 est très avantageux car son champ d'application est très large, ce qui permet d'y avoir recours pour des litiges très divers, et sans avoir à rentrer dans le détail des éléments constitutifs d'une infraction présumée aux dispositions de la Loi Informatique et Libertés. De plus, il est applicable aux services établis à l'étranger contrairement à ceux soumis par l'article 5 de la loi Informatique et Libertés ou à

[16] CNIL. Protéger sa vie privée en six étapes. [en ligne] 20 juillet 2017. Disponible à l'adresse : https://www.cnil.fr/fr/proteger-sa-vie-privee-en-6-etapes

[17] CNIL. La procédure de sanction. [en ligne]. Disponible à l'adresse : https://www.cnil.fr/fr/la-procedure-de-sanction

l'article 4 du RGPD. Enfin le juge peut prendre des mesures en référé et donc obtenir des résultats rapides, sous réserve de confirmation par un jugement au fond.

La protection de la vie privée est aussi assurée par des articles du Code pénal, sans lien avec la loi Informatique et libertés : Ainsi à titre d'exemple on peut mentionner les articles 226-1 et 226-2 sanctionnant l'exploitation des paroles ou de l'image d'une personne se trouvant dans un lieu privé, sans son consentement ; ou bien l'article 226-13 sanctionnant l'atteinte au secret professionnel.

La protection n'est pas absolue et aucune loi, aucune réglementation européenne, ne pourra venir protéger totalement la vie privée des personnes. En effet, ces règles ne protègent pas les personnes contre elles-mêmes. C'est notamment le fameux phénomène d'exposition de soi sur Internet. Mais les sujets qui s'exposent ne le font pas seulement ou d'abord parce qu'ils sont narcissiques mais afin de pouvoir utiliser des services qui leur sont présentés comme gratuits. Si le projet de patrimonialisation des données aboutit en Europe, il faudra peut-être payer les plateformes pour utiliser ces services réputés « gratuits » et conserver en même temps ses données personnelles Selon l'enquête seulement 26,20% des répondants déclarent être particulièrement vigilants à titre personnel sur la protection de leurs données personnelles (note maximale de 5), et 33,03% donnent la note de 3, ce qui démontre une prise de conscience toute relative.

L'anonymat et pseudonymat comme protection

La réputation et la liberté d'expression sont protégées par les mécanismes d'anonymat ou de pseudonymat. L'anonymat est considéré par certains comme garantie à une liberté d'expression et pour d'autres, au contraire, attentatoire à la démocratie. L'anonymat permet de parler en ligne de sujets sensibles : maladie, sexualité, orientation politique ou religieuse. Cependant le véritable anonymat sur Internet est depuis une décennie devenue l'exception : il est extrêmement dur de rester anonyme sur Internet et de se fabriquer une « légende » qui sera épargnée par les multiples croisements de données que n'importe qui peut faire pour retrouver qui se cache derrière un pseudonyme. Mieux vaut parler de pseudonymat dans un tel contexte que d'anonymat.

On a vu apparaître la notion d'e-réputation (réputation numérique, cyber réputation) qui peut être définie comme la réputation sur le web, d'une personne morale (entreprise), d'une marque, et bien évidemment d'une personne physique réelle ou imaginaire. L'e-réputation correspond à l'identité de cette personne associée à la perception que les internautes s'en font. C'est la notoriété numérique. Pour protéger sa e-réputation, il est conseillé, lorsqu'il n'y a pas d'intérêt à se servir de sa réelle identité, d'avoir un pseudonyme ou même de rester anonyme[18]. Juridiquement la loi n'autorise pas l'anonymat, mais elle ne l'interdit pas formellement non plus. Cependant, un certain nombre de situations dans lesquelles il est obligatoire d'utiliser sa véritable identité sont listés par des textes législatifs (par exemple pour voter), ce qui signifie qu'il n'y pas d'obligation pour toutes les autres situations.

[18] UNTERSINGER, M. Anonymat sur Internet. Eyrolles, 2ème ed. 2014 ; p.34-35

Dans la pratique, il s'agit le plus souvent de pseudonymat. Le pseudonyme reste lié à une identité même si celle-ci est fictive, propre au monde du numérique[19]. Sur internet, il s'agit en fait d'un anonymat de façade. Si l'internaute anonyme commet un délit, les services de police n'auront aucune difficulté à retrouver la personne.

Dans un contexte social tendu avec des propos injurieux, des menaces de mort sur des journalistes, avec la crise des « Gilets jaunes », l'anonymat est remis en question. En janvier 2019, à l'occasion d'une rencontre avec les maires de France, lors du Grand débat national, le président de la République, Emmanuel Macron, s'est prononcé pour une levée progressive de l'anonymat sur internet. L'argument avancé est celui de redonner une « hygiène démocratique de l'information ». Il s'agit également de lutter contre les propos haineux ou encore les « fake news », et plus particulièrement sur les réseaux sociaux. L'interdiction de prises de parole anonymes en ligne (si tant est que cela soit possible) n'interdirait pas les propos haineux sur le web. D'ailleurs, on peut observer que de nombreux internautes tiennent des propos condamnables par la loi, sans éprouver la nécessité de se cacher. Olivier Ertzscheid[20] suite aux propos antisémites, racistes tenus lors d'un Facebook Live (qui sera vite arrêté, faute de modérateur des commentaires), mis en place par des journalistes de France 3 lors de la visite du Chef de l'Etat suite à la profanation du cimetière juif de Quatzenheim, préconise que pour lutter contre les propos haineux sur le web trois pistes sont possibles, dont la garantie de l'anonymat (ou un pseudonymat facilement identifiable, et l'importance de la part de narcissisme), la responsabilité des plateformes à respecter leurs propres règles, et enfin l'architecture du faux (ce qui est populaire est vrai).

S'agissant des enfants et des adolescents, les associations de protection les incitent fortement à ne pas utiliser leur réelle identité lors de leurs premiers pas sur le web. L'article 8 du RGPD dispose que le consentement des enfants est licite, sans avoir besoin du consentement des parents, à partir d 'un âge fixé par défaut à 16 ans. Les Etats membres peuvent abaisser cet âge jusqu'à 13 ans. Le législateur français a fixé ce seuil à l'âge de 15 ans.

Le positionnement du Conseil d'Etat

En 2014, l'étude annuelle du Conseil d'Etat portait « Le numérique et les droits fondamentaux ». Le rapport rappelle que le législateur ne doit pas trop intervenir pour prévenir les risques engendrés par le numérique, car cela peut se révéler contre-productif et ainsi perdre de nombreux bénéfices générés par le numérique. Le Conseil d'Etat proposait dans son étude de mettre le numérique davantage au service des droits individuels comme de l'intérêt général. L'intervention publique doit accroître la capacité des personnes à agir pour la défense de leurs droits. Le Conseil d'Etat, par ailleurs, ne recommandait pas de reconnaitre un véritable droit de propriété aux individus sur leurs données, mais plutôt un droit à l'autodétermination ; l'individu se voit garantir le droit de décider de la communication et de l'utilisation de ses données à caractère personnel.

[19] Faut-il lever l'anonymat sur Internet ? Que dit la législation ? *Sud-Ouest* [en ligne] 12 février 2019. disponible à l'adresse : https://www.sudouest.fr/2019/02/12/faut-il-lever-l-anonymat-sur-internet-que-dit-la-legislation-5814310-5166.php

[20] ERTZSCHEID, O. Le live de Quaztenheim, Facebook, la catastrophe et la Shoah. [en ligne] disponible à l'adresse : https://www.affordance.info/mon_weblog/2019/02/facebook-catastrophe-shoah.html

Plusieurs préconisations de ce rapport, ont été mises en œuvre par le législateur national ou européen.

LES DONNEES A CARACTERE PERSONNEL

Le Conseil d'Etat, dans son rapport de 2014, faisait le constat suivant sur l'explosion des données personnelles :

> *Depuis l'adoption de la loi du 6 janvier 1978, les sources et les types de données personnelles en circulation se sont considérablement diversifiées. Les données ne sont plus seulement collectées par des entités organisées (administrations, entreprises, associations), mais aussi mises en ligne par les individus eux-mêmes ou par des tiers ou recueillies de manière automatique. Elles ne correspondent plus seulement aux caractéristiques objectives de l'individu (âge, sexe, profession…) ; il peut s'agir d'informations sur ses goûts, ses opinions, ses relations, ses déplacements ou encore des signaux biologiques ou corporels. Si toutes ces informations restaient disséminées auprès de personnes qui les ont recueillis, les risques pour la vie privée seraient sans doute limités.*[21]

Le cadre général

Définition

En décembre 2017, la Garde des sceaux a présenté un projet de loi relatif à la protection des données personnelles. Ce projet de loi adapte au droit de l'Union européenne la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Il transpose le nouveau cadre juridique européen (le règlement 2016/679 et la directive 2016/680) qui est entré en vigueur en mai 2018. Dans un souci d'intelligibilité, le Gouvernement a enfin fait le choix de conserver, l'architecture de la loi du 6 janvier 1978. Les modifications apportées à notre droit par la loi du 20 juin 2018 ont été codifiées dans la loi fondatrice de 1978 afin d'offrir un cadre juridique lisible à chaque citoyen et acteur économique.

La loi informatique et libertés (article 2) reprise par le RGPD (article 2.1) définit la donnée à caractère personnel comme « toute information se rapportant à une personne physique identifiée ou identifiable ». En indiquant qu'être réputée « identifiable » une personne physique peut être identifiée directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Ainsi, des identifiants, comme une adresse IP sont susceptibles d'identifier, au moins indirectement, une personne physique. Au vu de cette définition, on perçoit aisément qu'une très grande proportion de données collectées par des technologies numériques constitue une donnée à caractère personnel.

[21] CONSEIL D'ETAT. *Etude annuelle 2014, le numérique et les droits fondamentaux*. La documentation française, 2014, p.15-16

Selon Anne-Laure Stérin[22]

> *Les données à caractère personnel sont toutes les informations relatives à une personne physique identifiée, ou qui peut être identifiée en croisant des données la concernant*

Si un numéro de sécurité sociale est évidemment une donnée à caractère personnel, d'autres informations peuvent paraître plus insignifiantes. Mais le croisement de données a priori insignifiantes avec d'autres données peut permettre l'identification d'une personne. Ainsi sont des données personnelles les informations suivantes : nom, prénom, âge, profession, photo, adresse postale ou électronique, numéro de téléphone, date de naissance, adresse IP d'un ordinateur, tout numéro d'identification, une empreinte digitale.

Les droits des usagers

Le règlement sur la protection des données à caractère personnel renforce et précise les droits fondamentaux des personnes physiques à l'égard du traitement de leurs données au sein de l'Union européenne. Plus précisément, les droits concernés sont le droit à la transparence, à l'information, à la rectification, à l'effacement, et le droit d'opposition.

Le RGPD, par son article 12, oblige le responsable du traitement à fournir des informations transparentes, facilement accessibles et intelligibles. Le traitement des données suppose en effet la transparence, les personnes concernées doivent être en mesure de connaître l'existence des traitements et bénéficier, lorsque des données sont collectées auprès d'elles, d'une information effective et complète au regard des circonstances de cette collecte. Le même article détaille les modalités concrètes, à savoir la fourniture d'une information concise, aisément accessible et facilement compréhensible, c'est-à-dire formulée en des termes clairs et simples et, s'il y a lieu, illustrée à l'aide d'éléments visuels en particulier lorsqu'elle s'adresse à des enfants.

Les informations que le responsable du traitement est tenu de fournir à la personne concernée sont précisées à l'article 13 du RGPD. Il s'agit des informations sur la durée de conservation, le droit d'introduire une réclamation, l'existence d'un profilage.

Le droit d'accès de chaque individu à ses données à caractère personnel (droit reconnu depuis 1981 par les Etats membres du Conseil de l'Europe, signataires de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel) sont rappelées par l'article 15 du règlement. Le droit d'accès est un droit de questionnement de la personne concernée sur l'existence ou non d'informations la concernant dans un traitement de données. Ce questionnement porte sur le droit de savoir si des données font effectivement l'objet d'un traitement et dans l'affirmative, quelles sont les données précisément traitées et quelle est leur origine.

Le droit à rectification est consacré par l'article 16 du RGPD. Le responsable du traitement des données doit prendre :

[22]STERIN. Anne-Laure. « Le point sur les données à caractère personnel ». *Questions Ethique et droit en SHS* [en ligne] Disponible à l'adresse : https://ethiquedroit.hypotheses.org/1717#more-1717

toutes les mesures raisonnables (…) pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soit effacées ou rectifiées, sans tarder.

Des modalités sont précisées par le règlement pour accéder sans frais aux données collectées, à leur rectification, ou leur effacement ou l'exercice d'un droit d'opposition. Le responsable du traitement doit répondre aux demandes de la personne concernée, dans les meilleurs délais et au plus tard dans un délai d'un mois et doit motiver sa réponse lorsqu'il n'a pas donné suite à de telles demandes. Ainsi on peut justifier un refus de suppression de l'affichage public d'une date de naissance dans un fichier autorité auteurs, en arguant de l'intérêt du processus de désambiguïsation des autorités d'un catalogue (nous y reviendrons ultérieurement); même si la demande de la personne peut être valable.

L'article 17 fixe les conditions d'un droit à l'oubli numérique. Le responsable de traitement ayant rendu publiques des données à caractère personnel doit informer les tiers de la demande de la personne concernée d'effacer tout lien vers ces données ou les copies ou reproductions qui en ont été faites. Le droit à l'oubli numérique a été renommé en droit à l'effacement. Le droit à l'oubli n'est pas un droit absolu : il ne s'applique pas lorsqu'il s'agit de garantir la liberté d'expression et d'information ou encore le droit à l'histoire (archivage dans l'intérêt public, scientifique, statistique ou historique). Le législateur européen a ainsi opéré une balance de proportionnalité entre le droit des internautes à accéder à l'information et les droits fondamentaux de la personne concernée, en particulier le droit au respect de sa vie privée.

Une bonne connaissance de la part des bibliothécaires

Dans l'enquête menée dans le cadre de mémoire, il a été posé deux questions sur ce que les bibliothécaires identifiaient comme données personnelles, et où l'on pouvait trouver de telles données dans les outils généralement utilisés au sein des bibliothèques. Pour chacune des questions, plusieurs réponses étaient possibles.

Dans l'ensemble, les données à caractère personnel sont bien identifiées et sans distinction flagrante selon le type d'établissement dans lequel travaille le répondant.

Il faut rappeler qu'une donnée à caractère personnel qui peut paraitre non significative, peut permettre l'identification d'un individu quand elle est croisée avec une autre donnée.

Cependant, peu de répondants pensent qu'un catalogue de bibliothèque peut contenir des données à caractère personnel ; les fichiers autorités Auteurs ne sont donc pas perçus comme tel.

Pour mémoire, seules les questionnaires complets ont été exploités (soit 439).

Selon vous, sont des données à caractère personnel		
	Bibliothèques universitaires (190 réponses ; 43,28%)	Bibliothèques territoriales (173 réponses – 39,41%)
Un identifiant lecteur	57,89%	62,43%
Un nom	90%	94,80%
Une adresse postale	92,63%	95,95%
Une photo	93,68%	94,80%
Une empreinte	95,26%	97,11%
Une date de naissance	90%	98,27%
Une adresse IP	72,63%	76,88%
Une adresse mail	93,16%	93,64%

Selon vous, peuvent contenir des données à caractère personnel		
	Bibliothèques universitaires (190 réponses ; 43,28%)	Bibliothèques territoriales (173 réponses – 39,41%)
Un catalogue de bibliothèque	32,11%	23,12%
Une base lecteur	97,89%	97,69%
Un identifiant pour accéder à des bases de données	72,11%	69,94%
Un SIGB	90,53%	86,71%
Un ordinateur en libre accès	63,68%	79,19%

Et plus spécifiquement dans les bibliothèques

En 2004, Nancy Kranich publiait un article dans le Bulletin des Bibliothèques de France[23], sur les conséquences du *Patriot Act* sur la liberté d'expression et la protection de la vie privée. Après les attentats du 11 septembre, alors que les individus cherchaient des éléments de réponse dans les bibliothèques, l'administration Bush demandait aux services secrets d'élaborer des techniques à même de sécuriser les frontières des États-Unis et de réduire la probabilité de nouveaux attentats terroristes. Le Congrès votait le *USA Patriot Act*. Ce texte a été

[23] KRANICH, Nancy. « Le Patriot Act. Conséquences sur la liberté d'expression ». *Bulletin des bibliothèques de France (BBF)*[en ligne] , 2004, n° 6, p. -. Disponible à l'adresse: < http://bbf.enssib.fr/consulter/bbf-2004-06-0061-009>

complété par de nouvelles directives qui renforcent considérablement le pouvoir de surveillance du *Federal Bureau of Investigation* (FBI). Celui-ci est autorisé à collecter des renseignements en lui permettant d'accéder à des informations jusqu'alors protégées, et plus spécifiquement ses recherches sur le web (mots clés, sites consultés). Nancy Kranich met également en lumière le manque de transparence autour des mesures prises dans les bibliothèques, sur la base du *Patriot Act* :

> *Ces pouvoirs de surveillance renforcés donnent toute latitude aux représentants de la loi et de l'ordre pour passer au crible les lectures, les recherches et les communications les plus personnelles des Américains. Non seulement plusieurs des dispositions de cette loi adoptée dans l'urgence violent les droits à la vie privée et à la confidentialité de celles et ceux qui fréquentent les bibliothèques. Nous ignorons dans quelles conditions le USA Patriot Act et les mesures associées ont été appliqués aux bibliothèques, aux librairies et autres lieux publics, à cause de la clause sur le secret qui interdit aux individus d'alerter l'opinion sur les enquêtes en cours. L'exécutif a refusé de répondre aux questions posées sur l'incidence de ces activités de surveillance par les membres de la Chambre, les commissions judiciaires du Sénat et des groupes de défense des droits civils ; il a toutefois reconnu la présence d'agents du FBI dans les bibliothèques*.[24]

Un recensement des données à caractère personnel en bibliothèque

En 1999, la CNIL a rendu une délibération concernant les traitements automatisés d'informations nominatives relatifs à la gestion des prêts de livres, de support audio-visuels et d'œuvres artistiques et à la gestion des consultations de documents d'archives.[25]. L'article 3 de cette délibération liste les catégories qui peuvent faire l'objet d'un traitement :

> *nom, prénoms, adresse, année de naissance, catégorie professionnelle, numéro de téléphone […] ; caractéristiques du prêt ou de la communication : désignation de l'œuvre (titre, nom de l'auteur, de l'éditeur etc.) ou du document d'archive, cotes de catalogage ou de classement, date, date(s) relance*

Compte tenu des évolutions, notamment numériques, nous pouvons compléter cette liste par les données suivantes : adresse mail, connexion wifi (adresse Mac ou IP)

La norme NS009 de la CNIL s'appuie sur cette délibération, pour notamment fixer les durées de conservation des données :

> *Pendant la durée d'utilisation du service de prêt pour ce qui concerne l'identité de l'emprunteur. La radiation doit intervenir d'office dans un délai d'1 an à compter de la date de fin du prêt précédent. Jusqu'à la fin du 4ème mois suivant la restitution de l'objet du prêt pour les informations concernant chaque prêt. Au-delà de ce délai, les informations sur support magnétique sont*

[24] KRANICH, Nancy. « Le Patriot Act. Conséquences sur la liberté d'expression ». *Bulletin des bibliothèques de France (BBF)*[en ligne] , 2004, n° 6, p. -. Disponible à l'adresse: < http://bbf.enssib.fr/consulter/bbf-2004-06-0061-009>

[25]CNIL. Délibération n°99-27 du 22 avril 1999 concernant les traitements automatisés d'informations nominatives relatifs à la gestion des prêts de livres, de supports audiovisuels et d'oeuvres artistiques et à la gestion des consultations de documents d'archives publiques [en ligne] Disponible à l'adresse https://www.legifrance.gouv.fr/jo_pdf.do?numJO=0&dateJO=19990528&numTexte=&pageDebut=07890&pageFin=07890

détruites ; elles ne peuvent être conservées sur support papier que pour les besoins et la durée d'un contentieux éventuel. Jusqu'au prochain récolement (inventaire) et dans la limite d'une durée maximum de 10 ans s'agissant des consultations des documents d'archives[26].

Selon l'enquête, les répondants identifient bien (à plus de 92%) que le nom, l'adresse mail ou postale, date de naissance, une photo, une empreinte sont des données personnelles. Cependant, ils ne sont plus que 60,82% à reconnaitre que l'identifiant d'un lecteur est une donnée à caractère personnel, et 76,08% pour une adresse IP. En l'espèce, les répondants étaient face à une question dont il fallait cocher toutes les possibilités pour apporter la réponse appropriée.

Les services offerts dans les bibliothèques nécessitant des données personnelles pour y accéder sont très nombreux : emprunt de documents, prêt d'ordinateur, réservation de salle, prêt entre bibliothèques, service d'impression, consultation des postes publics, consultation des ressources en ligne payante etc.

Le SCD de l'université de Poitiers informe ses usagers de tous les services offerts par le SCD et qui nécessitent la récolte de données à caractère personnel. Pour chaque service offert, le SCD précise les données nécessaires, si elles font l'objet d'une anonymisation ou pas, les prestataires extérieurs partenaires, et la durée de conservation de données[27].

UNE ETHIQUE PROFESSIONNELLE

Lorsqu'une profession est face à des dilemmes, des conflits entre valeurs, l'adoption de code d'éthique peut permettre de rappeler les valeurs que les professionnels défendent. Les valeurs deviennent alors des objectifs à atteindre. Les bibliothécaires se sont donc prononcés sur leur propre éthique, et ont énoncé les valeurs qui motivent leur conduite professionnelle.

L'éthique de l'information

L'éthique de l'information[28], introduite dans les années 80 embrasse le champ du traitement des données, des informations et de leur cycle de vie. Plus précisément, l'éthique de l'information traite des questions relatives à la confidentialité des informations (ou des données), leur fiabilité, leur qualité et leur usage.

La réflexion éthique, initialement placée dans le cadre de l'éthique des affaires, a été complétée par des études philosophiques. L'approche philosophique a ainsi mis en opposition une approche déontologique axée sur les droits fondamentaux (droit au respect de la vie privée, égalité d'accès à l'information) à une approche utilitariste axée sur les systèmes d'informations comme bien commun et non le respect de droits individuels.

Luciano Floridi, théoricien de la philosophie de l'information et de l'éthique de l'informatique, a notamment développé le concept « d'*inforg* » (informational

[26] CNIL. Norme simplifiée. NS-009, Bibliothèques, médiathèques [en ligne] Disponible à l'adresse : https://www.cnil.fr/fr/declaration/ns-009-bibliotheques-mediatheques

[27] SCD BIBLIOTHEQUES DE L'UNIVERSITE DE POITIERS. Données personnelles. [en ligne]. Disponible à l'adresse : http://scd.univ-poitiers.fr/a-votre-service/donnees-personnelles-1652279.kjsp?RH=1504875094961

[28] HAMET Joanne, MICHEL, Sylvie, « Les questionnements éthiques en systèmes d'information », *Revue française de gestion*, 2018/2 (N° 271), p. 99-129

organism)[29], soit des individus, entreprises, des organisations interconnectés avec d'autres organismes biologiques ou des technologies. Il écrit cette définition simple de l'homme dans l'infosphère : « you are your information ». Ce qui fait que, selon lui, toute violation de l'information qui nous constitue est une atteinte à notre intégrité et à notre personnalité. Selon Floridi, il faut veiller à l'usage qui sera fait de nos données, et non considérer que nous en avons la propriété. Il est impossible de patrimonialiser nos données parce qu'elles nous constituent. Aliéner nos données reviendrait à nous aliéner nous-mêmes. Aussi, Floridi avance l'idée d'une intégrité des données qui conditionnerait l'intégrité de notre personnalité. Cela lui permet de faire du droit à la vie privée, un droit fondamental et inaliénable de la personne.

L'Unesco[30] s'est engagé en faveur de l'éthique de l'information, et rappelle que les principes éthiques des sociétés du savoir dérivent de la Déclaration universelle des droits de l'homme et incluent le droit d'expression, l'accès universel à l'information, et en particulier à l'information publique, le droit à l'éducation, le droit à la vie privée et le droit de participer à la vie culturelle. Le débat international sur les dimensions éthiques de la société de l'information (les « infoéthiques ») aborde les aspects éthiques, sociaux et juridiques de la mise en pratique des technologies de l'information et de la communication (TIC).

Déontologie des bibliothécaires

Dans les années 70, Robert Hauptman, rédacteur en chef du *Journal of Information Ethics*, a publié «Professionalism or Culpability? An. Experiment in Ethics » (Professionnalisme ou culpabilité? Une expérience en éthique)[31]. Dans une étude très peu scientifique, dans laquelle il a demandé à treize bibliothécaires de lecture publique et de bibliothèques universitaires des informations sur la construction d'une bombe suffisante pour faire sauter une maison de banlieue, Hauptman a été choqué par le fait que la plupart des bibliothécaires ont volontairement fourni ces informations. Selon Hauptman, les bibliothécaires dans une telle situation devraient placer leur devoir envers le bien-être de la société avant leur obligation professionnelle de fournir des informations.

En l'absence de texte juridique spécifique, la déontologie des professionnels des bibliothèques, est essentiellement régie par des textes rédigés par des instances professionnelles.

Les valeurs du bibliothécaire sont d'abord celles du service public. Il s'agit de valeurs non spécifiques qui régissent l'activité de tout agent public et conditionnent l'application des principes républicains. Ensuite, ces principes sont déclinés en pratiques dans les établissements. Ainsi par exemple le principe de neutralité consiste à mettre à disposition de la documentation pour tous les publics quelque soit leur origine ou leur sensibilité. Les valeurs du service public seront relayées par les pratiques professionnelles du bibliothécaire, mais parfois avec des compromis.

[29] SANTOS, Anouk. De l'importance d'une éthique dans l'infosphère : la quatrième révolution technologique selon Luciano Floridi. *Recherches d'idées* [en ligne].15 novembre 2018. Disponible à l'adresse : https://campus.hesge.ch/blog-master-is/de-limportance-dune-ethique-dans-linfosphere-la-quatrieme-revolution-technologique-selon-luciano-floridi/

[30] UNESCO. Ethique de l'information. [en ligne] Disponible à l'adresse : https://fr.unesco.org/themes/%C3%A9thiques-l%E2%80%99information

[31] HAUPTMAN, Robert. « Professionalism or Culpability? An. Experiment in Ethics. » *Wilson Library Bulletin* 50 (April 1976)

Ainsi il existe des compromis entre le service public notamment d'éducation et cette notion de neutralité : en témoigne le lancinant débat sur le retour de la morale à l'école ou bien, dans les bibliothèques universitaires, les conversations sur la posture qui doit être celle du bon étudiant fréquentant. Parmi les obligations du fonctionnaire, le respect de la vie privée des utilisateurs est une valeur qui serait beaucoup plus capitale dans un lieu de savoir et d'expression du savoir. Le respect de la vie privée en effet est notamment en prise avec le respect de la liberté d'expression et la liberté académique dans un contexte universitaire.

La déontologie peut être définie comme l'ensemble des obligations qui s'imposent aux membres d'un corps professionnel constitué, ainsi que celles qui s'imposent à une activité professionnelle. Elle regroupe des valeurs que l'on peut rapprocher d'une certaine moralité comme l'honnêteté, la responsabilité.

Certaines professions comme les journalistes, les médecins ont adopté depuis longtemps des codes de déontologie. Les professionnels des bibliothèques, tout comme l'ensemble de la fonction publique ne se sont emparés de cette problématique que tardivement ; les droits et devoirs des fonctionnaires étant utilisés comme moyen de substitution à la question plus large de la déontologie.

En l'absence de texte juridique spécifique, la déontologie des professionnels des bibliothèques, est essentiellement régie par des textes rédigés par des instances professionnelles.

Le Code de déontologie du bibliothécaire adopté en 2003 par l'ABF, préconise que le bibliothécaire s'engage à garantir à l'usager la confidentialité des usages qu'il pourrait avoir des services et collections de la bibliothèque. La déontologie renvoie à la question du secret (qui consulte quoi dans ma bibliothèque), de la responsabilité face à l'erreur, du respect des personnes.

En 2012, le Code international de déontologie rédigé par l'IFLA[32] présente une série de propositions éthiques destinées à guider les bibliothécaires dans la rédaction de leurs propres codes de déontologie. Sont notamment mis en avant le droit, l'accès, le partage de l'information, mais aussi la liberté d'opinion, la liberté d'expression. L'article 3 de ce code est consacré à la confidentialité, le secret et la transparence et énonce que les bibliothécaires respectent la vie privée et protègent les données à caractère personnel, qui sont nécessairement partagées entre les individus et les institutions. La relation entre un usager et la bibliothèque repose sur la confidentialité. L'accent est également mis sur le non partage des données des usagers.

En 2015, l'IFLA, dans une « Déclaration sur la vie privée dans le monde des bibliothèques » fait les recommandations suivantes (extraits)[33] :

> *Les bibliothèques et les services d'information doivent respecter et faire progresser la protection de la vie privée à la fois dans les pratiques et en tant que principe.*
>
> *• Les bibliothèques et les services d'information doivent soutenir les actions de plaidoyer au niveau national, régional et international (par exemple*

[32] IFLA Code of ethics for Librarians and other Information Worker . [en ligne]. Disponible à l'adresse : https://www.ifla.org/publications/node/11092

[33] IFLA. Déclaration de l'IFLA sur la vie privée dans le monde des bibliothèques. Ifla.org [en ligne]. 20 août 2015. Disponible à l'adresse : https://www.ifla.org/files/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment-fr.pdf

celles des organismes s'occupant des droits de l'homme et des droits numériques) entrepris pour protéger la vie privée des individus et leurs droits numériques, et encourager les professionnels des bibliothèques à réfléchir sur ces questions.

• Les bibliothèques et les services d'information doivent rejeter la surveillance électronique et toute espèce illégitime de supervision ou de collecte des données personnelle des usagers, ou d'informations sur leurs comportements qui risqueraient de compromettre leur vie privée et d'affecter leur droit à rechercher, à recevoir et à transmettre de l'information. Ils doivent prendre des mesures afin de limiter la collecte des informations personnelles relatives à leurs usagers et les services qu'ils utilisent.

• Même si l'accès des gouvernements aux données des utilisateurs et la surveillance des données ne peuvent être entièrement évités, les bibliothèques et les services d'information doivent s'assurer que l'intrusion des gouvernements en fait d'informations relatives aux usagers ou à leur communication est fondée sur des principes légitimes pour de telles pratiques, nécessaires et en rapport avec des fins légitimes (telles que par exemple décrites dans les « Principes internationaux relatifs à l'application des droits de l'homme à la surveillance des communications »).

La loi relative à la déontologie et aux droits et obligations des fonctionnaires du 20 avril 2016 inscrit dans le statut général des fonctionnaires les obligations de dignité, d'impartialité, d'intégrité, de probité, de neutralité et le respect de la laïcité. Ces obligations ne sont pas nouvelles, elles étaient déjà reconnues par le juge administratif. Selon le gouvernement, cette loi a pour but de renforcer la relation de confiance entre les Français et les fonctionnaires.

La Haute Autorité pour la Transparence de la Vie Publique (HATVP), dans le cadre de la loi du 20 avril 2016 avait formulé plusieurs suggestions pour renforcer la confiance dans les institutions. Le Ministère de la Culture a donc créé en avril 2018, en son sein un collège de déontologie[34], qui fait suite à la fonction de référent déontologue mise en place dès 1983. Ce collège de la déontologie est compétent « pour les fonctionnaires et agents contractuels de droit public de l'administration centrale, des services déconcentrés et des services à compétence nationale du ministère chargé de la culture ; pour les fonctionnaires et agents contractuels de droit public et de droit privé des établissements publics placés sous la tutelle du ministre chargé de la culture ».

Le positionnement des bibliothécaires, et leur rôle dans l'évolution des normes

Les associations professionnelles de bibliothécaires sont des corps intermédiaires qui peuvent exercer des actions de *lobbying,* ou d*'advocacy* auprès des ministères, des législateurs pour faire évaluer les normes, notamment celles relatives à la vie privée et aux questions liées au numérique. Les bibliothèques sont traditionnellement porteuses de valeurs profondément ancrées en faveur de la

[34] OURY, Antoine. Un collège de déontologie au Ministère de la Culture. *Actualitté*, .[en ligne] 26 avril 2018. Disponible à l'adresse : https://www.actualitte.com/article/monde-edition/un-college-de-deontologie-au-ministere-de-la-culture/88584

protection de la vie privée et manifestent une forte motivation pour la protéger. Les bibliothèques ont également des obligations légales et éthiques en matière de protection de la vie privée de leurs usagers. À mesure que la profession adopte les nouvelles technologies, des dilemmes éthiques se présentent, liés à leur utilisation. Les bibliothécaires français s'engagent en faveur de la protection de la vie privée, à l'instar leurs collègues, notamment nord-américains ou via des associations professionnelles internationales.

Les bibliothécaires américains ont pris plusieurs engagements sur la protection de la vie privée de leurs usagers. La liberté intellectuelle, fondement des bibliothèques, exige nécessairement la confidentialité. Dans son interprétation de la Charte des droits de la bibliothèque, *l'American Library Association* (ALA) explique : dans une bibliothèque (physique ou virtuelle), le droit à la vie privée est le droit de mener une recherche sans que le sujet de cette recherche soit examiné. Aux Etats-Unis, bien qu'aucune loi fédérale ne protège la vie privée des usagers des bibliothèques, quarante-huit États ont adopté des réglementations relatives à la confidentialité des archives des bibliothèque, bien que l'étendue de ces protections varie d'un État à l'autre. La communauté des bibliothèques a établi de nombreux documents qui reflètent son engagement éthique en matière de protection de la vie privée des utilisateurs. Le code de déontologie de l'ALA énonce dans son troisième principe :

> *Nous protégeons le droit à la confidentialité de chaque utilisateur de bibliothèque vis-à-vis des informations recherchées ou reçues et des ressources consultées, empruntées, acquises ou transmises*.

L'ALA, en janvier 2019, mis à jour son texte *Bill of rights* et y a ajouté l'article 7 relatif à la protection de la vie privée[35]

> *« Toute personne, indépendamment de son origine, de son âge, de ses antécédents, de ses opinions, dispose d'un droit à la vie privée et à la confidentialité quand elle utilise les services de la bibliothèque. Les bibliothèques devraient défendre, éduquer et protéger la vie privée des gens, en sécurisant toutes les données d'utilisation des bibliothèques, y compris les renseignements personnels identifiables. »*

Les bibliothécaires américains pourront donc s'appuyer sur cet amendement pour protéger les données de leurs usagers.

Le code de déontologie de l'IFLA[36] rappelle que les relations entre les bibliothèques et leurs usagers sont basées sur la confidentialité. L'accent est également mis sur le non partage des données des usagers. Le code de l'IFLA incite les bibliothécaires à, si besoin, critiquer les textes juridiques, mais surtout à préconiser des améliorations.

En outre, le *Library Freedom Project*, lancé en 2015 se veut être une ressource pédagogique pour informer les bibliothécaires sur les menaces, les droits et les outils d'atteinte à la vie privée. Il est proposé aux professionnels des outils pour contrecarrer la surveillance sur les réseaux. Plus particulièrement, ce projet milite pour l'installation de Tor dans les bibliothèques publiques.

---

[35] http://www.ala.org/advocacy/intfreedom/librarybill *article* VII. All people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use. Libraries should advocate for, educate about, and protect people's privacy, safeguarding all library use data, including personally identifiable information.

[36] IFLA. Code d'éthique de l'IFLA pour les bibliothécaires et autres professionnel(le)s de l'information. [en ligne]. Août 2012.Disponible à l'adresse : https://www.ifla.org/files/assets/faife/codesofethics/frenchcodeofethicsfull.pdf

En France, la question a été abordée par une journée d'études organisé en janvier 2018 par l'ABF ayant pour sujet « (Auto)-censure et surveillance de masse, quels impacts pour les bibliothèques[37] ».Comme indiqué sur le site de l'ABF pour introduire la journée :

> *Qu'elle soit organisée par les géants du web ou les gouvernements, dans un objectif économique, politique, ou encore de lutte contre le terrorisme la surveillance nous concerne tou·te·s. Outil de protection des populations ou de l'ordre public pour les uns, une surveillance généralisée peut entraîner pour d'autres un développement de l'autocensure, menacer la vie privée, la liberté d'expression ou la liberté d'accéder à l'information. Ce contexte nouveau plonge les professionnels de l'information-documentation dans de nombreux questionnements et débats éthiques et juridiques.*

Les bibliothécaires ne doivent pas aller au-delà du cadre légal, mais ils peuvent néanmoins affirmer que le cadre légal doit évoluer. Le terrorisme a fragilisé l'idéal démocratique affirmé par les bibliothèques. Plusieurs lois ont été votées pour légaliser une certaine forme de surveillance. Les bibliothécaires sont donc face à un dilemme entre libre accès à l'information, protection des données personnelles, protection de la vie privée et besoin de sécurité. Xavier Galaup, président de l'ABF, dans son introduction à la journée d'études, reconnait que la profession est très partagée sur ces questions : doit-on fournir les données, doit on contribuer à cette lutte contre le terrorisme.

[37] ABF. Journée d'étude nationale. (Auto)-censure et surveillance de masse, quels impacts pour les bibliothèques. [en ligne]. 26 juillet 2018. Disponible à l'adresse : http://abf.asso.fr/5/181/733/ABF/-auto-censure-et-surveillance-de-masse-quels-impacts-pour-les-bibliotheques

ASSURER UNE PROTECTION

Afin d'instaurer une relation de confiance entre les usagers et les établissements, il est primordial que ces derniers mettent tout en œuvre pour protéger les données de leurs usagers. Le RGPD a changé le modèle qui était alors en vigueur. Il s'agit de maîtriser non seulement les données, mais aussi les risques pouvant affecter celles-ci, et enfin pour les bibliothèques s'appuyer sur un réseau de partenaires.

MAITRISER LES DONNEES PERSONNELLES

Le principal changement avec le RGPD c'est la fin des déclarations à la CNIL, et également le recueil du consentement éclairé de l'usager et de l'accès à ses propres données.

Jusqu'à présent, le régime de protection des données, sur le plan réglementaire, s'appuyait sur l'obligation qu'avaient les entreprises ou les administrations de déclarer leurs fichiers. Maintenant il existe une obligation pour les établissements de documenter sa conformité. On appelle cela aussi le principe de responsabilité. Il s'agit également d'un enjeu majeur de confiance entre les établissements, entreprises, services publics et leurs clients ou usagers. Il ne s'agit plus de déclarer les traitements à la CNIL, dans la plupart des cas, mais en contrepartie, l'établissement doit s'organiser pour vérifier qu'en interne, il a été mis en œuvre des procédures, des règles, des cadres, pour que les données qui sont récoltées soient respectées, collectées et traitées de manière respectueuse vis-à-vis du cadre réglementaire. Jusqu'à présent, la CNIL disposait d'un pouvoir de sanctionner les responsables de traitement qui ne respectent pas la loi, mais il était limité, puisque la CNIL ne pouvait prononcer que des amendes d'un faible montant. À partir de mai 2018, la CNIL peut prononcer des amendes jusqu'à 20 millions d'euros (pour le secteur public), ou 4 % du chiffre d'affaires mondial d'une entreprise. Cela change d'échelle.

Du point de vue des collecteurs de données, la dichotomie « fluid data » vs « static data » peut être opérante. Les données statiques sont celles entrées par le bibliothécaire lors de l'inscription (ou par l'enseignant en début d'année, cf. Nom, prénom, profession du père, etc.) et les données fluides sont celles récoltées au jour le jour depuis les interfaces de bibliothèques ou les sites pédagogiques type Moodle pour mesurer et analyser l'activité de l'apprenant. Nous verrons dans un premier temps, les données semées par les usagers et dans un second celles récoltées par les établissements.

Les données semées

Le développement d'outils tels que les blogs, puis les réseaux sociaux, depuis quelques années, permettent à des individus de s'exposer et de livrer eux-mêmes de l'information nominative, parfois très confidentielle ou intime, des photos, des vidéos.

On parle alors d'identité numérique, Olivier Ertzscheid définit celle-ci comme :

> *l'identité numérique est constituée de la somme des traces numériques se rapportant à un individu ou à une collectivité : des traces « profilaires » correspondant à ce que je dis de moi (qui suis-je ?) ; des traces « navigationnelles » qui renseignent sur les sites que je fréquente et sur lesquels je commente ou j'achète (comment je me comporte) ; enfin des traces inscriptibles et déclaratives – ce que je publie sur mon blog par exemple – qui reflètent directement mes idées et mes opinions.*

L'identité numérique c'est également la somme des traces que nous laissons sur les réseaux. Les formes sont diverses : écrits, contenus audios ou vidéos, messages sur des forums, identifiants de connexion, etc. Les individus ont plus ou moins conscience du dépôt de ces empreintes lors de leur navigation sur le web. Les moteurs recherchent utilisent ensuite ces empreintes pour les faire ressortir.

L'identité numérique est constituée de plusieurs éléments : nom, prénom, pseudos, adresse IP, *cookies*, courrier électronique, coordonnées (personnelles, administratives, professionnelles, sociales, bancaires,), photos, avatars, logos, tags, liens, vidéos, articles, commentaires de forums, données géolocalisées, empreintes numériques, etc.

Le règlement européen vise à protéger les internautes, mais rappelons le principe selon lequel si la personne consent à la mise en ligne d'une information, le règlement sera d'un faible secours en cas de problème. C'est notamment sur ces questions que la formation et l'éducation populaire ont leur importance : les bibliothèques sensibilisent les usagers à leurs traces numériques (ou encore e-réputation).

Il y a donc un enjeu, au-delà du cadre juridique de sensibilisation des personnes, à l'éducation numérique, pour être en capacité de connaître les outils informatiques disponibles et d'arbitrer les situations dans lesquelles l'individu est d'accord pour livrer de l'information ou dans lesquelles, par mesure de prudence, il ne souhaite rien divulguer.

Il convient de garder à l'esprit que l'université est en situation de sous-traitant dans la mesure où elle collecte en vue de fournir à certains services les données relevant de communautés rattachées à l'Ecole ou l'institution avec laquelle elle a contractualisé, et ce qu'il y ait ou non contrepartie financière. Toutes les conventions qu'un SCD pourrait signer devront donc intégrer un chapitre « *Protection des données personnelles* ». La tutelle s'engage à traiter les données personnelles uniquement pour la seule finalité qui fait l'objet de la convention (par exemple l'inscription du lecteur) ; en garantir la confidentialité ; fournir l'information relative à l'exercice du droit d'accès aux données aux personnes concernées ; notifier au cosignataire toute violation de données personnelles dans un délai maximum de 72 heures après en avoir pris connaissance ; mettre en œuvre les mesures de sécurité permettant de garantir la confidentialité, l'intégrité, et la disponibilité du système d'information ; détruire ces données personnelles au terme de la prestation.

Les données récoltées

Dans l'enquête, à la question de savoir quels outils peuvent contenir des données à caractère personnel, seuls 30,52% reconnaissent qu'un catalogue de bibliothèque peut contenir des données personnelles. Cela pose donc question sur la gestion et connaissance des fichiers autorités au sein des bibliothèques.

Les fichiers autorités

Du point de vue français

Il existe deux établissements qui gèrent les fichiers autorités sur le territoire national : l'Agence bibliographique de l'enseignement supérieur (ABES) et la Bibliothèque nationale de France (BnF). Leur positionnement est très proche, notamment en opérant une distinction entre l'interface public et l'interface professionnelle.

L'ABES en matière de fichier « Auteurs », a toujours refusé les demandes de suppression car les informations de publication sont des données publiques. Ainsi les dates de naissance des auteurs peuvent être rendues non publiques, mais pas supprimées car cette donnée personnelle permet d'éviter les risques d'homonymie.

Pour toute demande d'un usager de modification dans le catalogue collectif géré par l'ABES, le Sudoc, d'une donnée le concernant, le site de l'ABES lui indique de contacter une des bibliothèques qui a rédigé la notice litigieuse[38]. L'ABES met également à disposition du demandeur, un lien vers la CNIL qui propose un modèle type de courrier.

Il est impossible d'empêcher que son nom et son prénom soient liés à sa thèse sur le catalogue public. En effet, le Sudoc sert de registre national des thèses et toute thèse soutenue doit y être enregistrée avec le nom de son auteur (et un lien vers le répertoire IdRef.). Cependant dans des cas exceptionnels et rares, compte tenu du sujet sensible d'une thèse ayant pour cadre par exemple un pays non démocratique, l'ABES a pu prendre la décision de rendre non public le document afin d'assurer la protection de l'auteur.

L'entrée en vigueur du RGPD n'a pas bouleversé le traitement du fichier *Autorité Auteurs Personnes* de la BnF. En effet, le fichier avait déjà fait l'objet d'une déclaration à la CNIL. Les auteurs ont un droit de regard et de modification sur leurs données, cependant la BnF se place sous le régime d'exception scientifique et conformément au décret de 1994[39], l'identification des auteurs fait partie de ses missions.

Le fichier auteur est géré par le département des Métadonnées (MET). Les auteurs peuvent demander une rectification ou un retrait depuis le catalogue et le bouton « signaler une erreur ». Les demandes d'effacement total du fichier sont refusées au motif de la mission scientifique de la BnF. Les demandes de rectification portent essentiellement sur les dates de naissance (une centaine en 2018), le MET explique dans un premier temps à l'usager l'intérêt de ce champ pour éviter les homonymies, tentant ainsi de le convaincre d'abandonner sa demande. Si l'auteur réitère sa demande, la date de naissance est ensuite masquée du catalogue public mais reste accessible aux professionnels.

Les bases internationales

Les bases internationales sont gérées par des pays soumis, ou non, au RGPD, ce qui rend plus complexe l'application de règles uniformes.

[38] ABES STP. Demander la correction d'une notice me concernant dans le catalogue. [en ligne]. Disponible à l'adresse : https://stp.abes.fr/node/12615/edit?origine=sudoc

[39] Décret n°94-3 du 3 janvier 1994 portant création de la Bibliothèque nationale de France

L'ISNI (International Standard Name Identification)[40]

Il s'agit d'un code international normalisé qui permet d'identifier des identités de personnes ou d'organismes qui participent à tout processus de création. Cette base est alimentée par une trentaine de contributeurs dont la BnF, et gérée par OCLC (société américaine, mais ayant un bureau à Leiden et traitant de données de citoyens européens, est soumise au RGPD).

ISNI a donc consulté un avocat dont les conclusions sont proches de la politique de la BnF sur la gestion du fichier Autorités Personnes. La principale difficulté de cette base, est qu'une modification d'une donnée d'un auteur réalisée par l'ISNI, n'est pas systématiquement transposée dans les catalogues des autres contributeurs. La BnF veille à cette transposition, dans un souci de la qualité des données.

VIAF (Virtual International Authority File)[41]

VIAF croise des données autorités et données bibliographiques de ses partenaires. La base est notamment alimentée par IdRef[42], Cette base est hébergée par OCLC mais sans personnel dédié (contrairement à ISNI). OCLC est un agrégateur de données pour une cinquantaine de membres qui alimentent VIAF. Seuls une vingtaine de membres sont situés dans l'Union européenne, et avec des visions très différentes sur l'interprétation de l'application du RGPD. La problématique est plus ardue car il n'y a pas de politique globale sur le fichier. Il a été instauré un « Conseil Viaf », des bibliothèques nationales. Ce groupe de travail est constitué des bibliothèques nationales de France, Espagne, Allemagne, Japon et de la Bibliothèque Royale de Suède et celui-ci est chargé de faire des recommandations pour le prochain congrès de l'IFLA.

Le cœur de VIAF est un algorithme dans lequel la date de naissance joue un rôle important pour le rapprochement des données. Le principal écueil aujourd'hui est que VIAF ne permet pas de distinguer les données publiques des données professionnelles, un effacement total de données (comme le font aujourd'hui les bibliothèques allemandes) risquerait donc d'impacter la qualité des données.

Open Researchers and contributers ID (ORCID

Orcid est un code numérique permanent attribué à un chercheur, et qui permet de l'identifier et de lever le doute sur toute homonymie. A cet identifiant, le chercheur peut lier ses publications, obtenir un CV etc. l'inscription est gratuite. Certains éditeurs demandent l'identifiant Orcid lorsqu'un article leur est soumis.

Comme l'indique l'article du réseau des Urfist, « L'identité numérique des chercheurs : quel accompagnement ? » [43], les bibliothèques ont un rôle important à jouer dans l'accompagnement des chercheurs et l'apprentissage de leur identité numérique. L'article rappelle que :

> *…alors que l'identité numérique aborde des questions comme les données personnelles, la prise de parole ou encore l'éthique, « les*

[40] http://www.isni.org/

[41] https://viaf.org/

[42] https://www.idref.fr/

[43] URFISTINFO. L'identité numérique du chercheur : quel accompagnement ? [en ligne]. 24 août 2018. Disponible à l'adresse : https://urfistinfo.hypotheses.org/3219

bibliothécaires doivent agir pour continuer leur rôle traditionnel de champions de la vie privée et de la liberté intellectuelle à l'ère numérique » (Sarah Shik Lamdan), faisant même de cette protection des données personnelles un élément de leur image de marque.

Le CNRS a un projet en cours d'inclure une clause RGPD dans le cadre des accords ORCID. Dans le cas d'ORCID, il y a consentement de l'auteur sur ses données.

Le consortium Couperin envisage d'attendre ces résultats et pourrait s'inspirer de cette clause pour l'intégrer à la licence-type et à la lettre d'accord.

MAITRISER LES RISQUES

Les bibliothèques doivent savoir anticiper pour mieux se protéger. Elles doivent donc déterminer quelles sont les valeurs à protéger, essayer de déterminer les risques et menaces possibles, anticiper autant que possible notamment en adoptant une démarche de *Privacy by design.*

Les valeurs à protéger

Les bibliothèques se doivent de protéger plusieurs valeurs, mais parfois certaines entrent en tension. Par exemple, dans le cas de la fourniture d'ebooks,un établissement peut choisir élargir l'offre documentaire, mais cela peut se faire au détriment des données personnelles de l'usager (Nous traiterons ultérieurement de la fuite de données à des partenaires commerciaux via *Adobe Digital Editions*) Accompagner le mouvement de recueil des *learning analytics* pour étudier et renforcer l'engagement des étudiants dans leurs études peut paraître un bon objectif, mais cela peut porter atteinte à la liberté de lire en toute confidentialité. Le filtrage des accès web à la bibliothèque, notamment aux mineurs, est contrebalancé par l'interdit de la censure qui normalement fait partie de l'éthique du bibliothécaire. Les professionnels devront alors opérer des choix ; nous traiterons de ces questions ultérieurement.

Le patrimoine informationnel et/ou la réputation de la bibliothèque doivent donc être protégés. Ces valeurs impliquent de garantir l'exclusivité des données, en les conservant confidentielles, ou à diffusion très restreinte et maitrisée.

La poursuite d'activité : cette valeur implique de garantir la disponibilité des données nécessaires au fonctionnement de l'établissement.

La pérennité d'activité : cette valeur nécessite de protéger la qualité des données nécessaire au fonctionnement de l'établissement.

Les évènements redoutés

Il existe trois catégories d'évènements redoutés : l'accès illégitime aux données (c'est-à-dire par un tiers non autorisé), la destruction non souhaitée ou l'inaccessibilité des données, la modification non autorisée des données.

La menace

La source du risque est généralement humaine. Il peut s'agir de personnes internes ou externes à la bibliothèque. Elle peut également être plus rarement naturelle (incendie, rongeur…).

Les supports exposés peuvent être de nature technique ou humaine. Les éléments techniques sont de deux ordres : les éléments matériels (ordinateurs, serveurs etc.) qui peuvent faire l'objet de mesures de sécurisation comme par exemple des dispositifs de contrôle d'accès, de détection d'intrusion. On peut citer l'exemple des enregistreurs de frappe (*Keylogger*) ressemblant à des adaptateurs et branchés sur les ordinateurs publics pour obtenir des identifiants de connexion. Cette technique a été utilisée notamment sur des postes publics à la bibliothèque de l'université de Lausanne[44] (un usager a ainsi pu avoir accès à des données privées, photos, codes bancaires, de près de 2700 étudiants) Les éléments immatériels (logiciels, bases de données etc.) auxquels peuvent être appliqués des mesures antivirus, ainsi que des sauvegardes régulières.

Les personnes intervenant sur les données exposées aux risques et qui si elles sont vulnérables (corruptibilité, ou ressentiment envers l'organisme) peuvent répondre favorablement à la menace.

S'agissant d'une menace de vulnérabilité humaine, on peut également envisager, la réponse à une demande présentée comme pressante par des personnes malintentionnées (par exemple des personnes usurpant l'identité d'un DSI, ou toute autre procédé de « *phishing* » pour obtenir des identifiants).

Le niveau de risque

Une fois identifiés les événements redoutés et l'élément causal pouvant les déclencher, il faut établir des priorités parmi les risques caractérisés. L'évaluation du niveau de risque permettra à la bibliothèque d'établir des priorités et de définir les principes de sa politique de sécurité. L'évaluation du risque s'appuie sur sa gravité et sur sa vraisemblance.

La CNIL met à disposition un guide « Gérer les risques sur les libertés et la vie privée »[45] pour les responsables de traitement et leur proposer une méthode pour la gestion des risques. La gestion dépendra bien évidemment du type de données récoltées, et en bibliothèques les données sont rarement sensibles comme elles le sont souvent dans le milieu médical ou judiciaire. Cependant, en cas de nervosité sécuritaire, dû à un contexte particulier, ces mêmes données peuvent devenir sensibles.

Répondre à la menace, avant l'atteinte

Sur le plan organisationnel :

La mise en place d'un processus de pilotage de la sécurité des données implique notamment de :

[44] HADDOU, R. « Des centaines de photos intimes piratées à l'UNIL ». *La Tribune de Genève* [en ligne] 15 février 2018. Disponible à l'adresse : https://m.tdg.ch/articles/5a85d8b2ab5c371445000002.

[45] CNIL. Guide : gérer les risques sur la liberté et la vie privée. [en ligne]. Juin 2012. Disponible à l'adresse : https://www.cnil.fr/sites/default/files/typo/document/CNIL-Guide_Securite_avance_Methode.pdf

Dégager une classification des données à protéger, qui seront ensuite soumises à des restrictions d'accès et/ou d'usage adaptées ;

Se doter de moyens de détection des atteintes possibles, ainsi que d'outils et d'une organisation permettant de réagir et d'en limiter rapidement les effets préjudiciables ;

- Nommer un responsable de la sécurité des systèmes d'information (RSSI), disposant de moyens humains et financiers adaptés, nouant un partenariat fort avec la direction de l'organisme. Mettre en place des procédures visant à impliquer le RSSI et ses équipes dans tout nouveau projet.
- Mettre en place une stratégie de sensibilisation et de formation des agents et des tiers afin d'expliquer les risques et les menaces pesant sur les données ainsi que leur impact potentiel, puis diffuser largement les règles applicables
- Mettre en place des dispositifs de contrôle de sécurité permettant d'identifier et de traiter rapidement, au travers de moyens humains ou automatisés, des éventuelles failles ou défauts de sécurité.

Sur le plan technique : la protection des données se traduira par la mise en place d'outils permettant d'automatiser les mécanismes de protection :

Identification / authentification des usagers. L'objectif étant d'établir un lien entre l'identité humaine et l'identité numérique de ces derniers. Ce type de technologie se traduit par un contrôle préalable d'accès par des moyens d'identification / authentification, dont le plus courant est le plus faible est le mot de passe. Celui-ci présente de nombreux défauts puisqu'il se donne, se vole, s'écrit, se réutilise etc. On pourrait sécuriser avec une double authentification, un badge par exemple, mais ce n'est guère pratiqué et un peu trop contraignant pour ouvrir seulement un SIGB.

- Le contrôle d'accès : l'objectif est de réguler (autoriser ou refuser) une action réalisée par un usager sur une ressource informatique
- Le filtrage des flux a pour objectif d'autoriser ou de refuser un flux de données entre deux ressources informatiques, par un dispositif par exemple de *Firewall*
- La détection et réaction a pour objectif de mettre en œuvre des moyens techniques capables de détecter et de bloquer les attaques. Ce type de technique doit être constamment mise à jour.

En matière de suppression des données, si celle-ci est automatique, le responsable doit s'assurer que les données sont effectivement supprimées. Faire confiance aux programmes informatiques ne suffit pas.

A l'université de Lille, à l'issue des actions de conseil réalisés par le DPD au printemps 2018, un correspondant « CIL » a été désigné au sein du SCD. Un audit a été réalisé sur la déclaration des données recueillies en vue d'intégration dans le registre de traitement de données. Ainsi, la plateforme des thèses, et la future plateforme de formation pour les étudiants ont été jugées conformes au RGPD. S'agissant des comptes lecteurs accessibles depuis Primo, et stockés sur un cloud, il faut attendre l'avenant proposé par Ex-Libris (fournisseur de Primo), pour étudier la conformité. Il a également été préconisé que toutes les enquêtes de public menées

par le SCD devront être soumises au préalable au DPD pour une analyse des objectifs et des informations récoltées.

Le règlement intérieur du SCD devra être également soumis au DPD pour mise en conformité.

Adopter une démarche de *Privacy by design*

Dès la conception d'une nouvelle application ou d'un projet, avoir une démarche de *Privacy By Design* c'est garantir le respect de la vie privée. Il s'agit de s'assurer de la pertinence des données collectées, comprendre les risques pour les personnes concernées, anticiper l'information et le droit d'accès, etc. C'est donc une mesure préventive et obligatoire.

La Loi Informatique et Libertés, dans l'article 34, demandait déjà au responsable de traitement de « prendre toutes les précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données » mais n'imposait pas explicitement la mise en œuvre d'une démarche de *Privacy By Design*. De ce fait, peu d'organisations ont déjà mis en place une telle démarche.

Adopter une démarche *Privacy By Design* minimise les efforts fournis pour se conformer à la loi tout en évitant une mise en conformité a posteriori. Toute modification, adaptation ultérieure est généralement plus complexe et plus coûteuse.

Pour favoriser cette démarche, la CNIL a publié en juillet 2015 un guide de gestion des risques sur la vie privée, pour inciter les responsables de traitement à s'engager dans ce type de projet. La CNIL a mis à jour ce guide en l'adaptant au RGPD et propose ainsi une méthode pour mener des *Privacy Impact Assessment* (PIA) ou études d'impact sur la vie privée (EIVP).

UN RESEAU DE PARTENAIRES

Les bibliothèques travaillent depuis longtemps en réseaux, dans de nombreux domaines (conservation, politique documentaire…), s'agissant de la protection des données à caractère personnel, elles peuvent non seulement s'appuyer sur leurs partenaires les plus proches au sein de leurs tutelles, mais aussi sur des partenaires extérieurs officiels et associatifs.

En interne

La personne ressource de la structure à laquelle appartient la bibliothèque (Université, collectivité etc) est bien évidemment le Délégué à la protection des données.

Délégué à la protection des données (DPD) ou *Data Protection Officer* (DPO)

Avant le RGPD, il existait un CIL (Correspondant Informatique et Libertés) ; généralement le CIL a pris les fonctions de DPD (ou dénommé plus fréquemment selon l'acronyme anglais aussi DPO, *Data Protection Officer*). Le CIL, était facultatif, et était déjà chargé de veiller à ce que son établissement respecte la Loi Informatique et Libertés. Selon la liste publiée des CIL déclarés (près de 20.000 au

total) par la CNIL[46], seules 3 bibliothèques avaient désigné un CIL (BnF, Bulac, BNU), 4 Comue (Languedoc-Roussillon, Université Côte d'Azur, Université Lyon, Grenoble) mais de très nombreuses (99) communautés de communes et plus de 600 mairies. On peut supposer que les bibliothèques universitaires pouvaient s'appuyer sur le CIL de leur université et c'est toujours le cas avec le DPD. Cependant le CIL n'est pas devenu automatiquement DPD : c'est le cas à Rennes 1 mais pas à l'INSA Rennes par exemple où la DPD (exception à la règle) est bibliothécaire.

Ce qui change, par rapport au CIL que la loi Informatique et libertés rendait facultatif, c'est que le délégué à la protection des données devient obligatoire.

Dans certains cas (les autorités ou les organismes publics, les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle, les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions)[47]. Cela concerne tout le secteur public, puisque ce que dit le règlement européen, c'est que toutes les structures du secteur public doivent, désormais, désigner un délégué à la protection des données. Pour tous les autres cas, la CNIL incite fortement à la désignation d'un DPD.

Le Délégué à la Protection des Données a un statut public, c'est-à-dire que sa désignation doit être enregistrée officiellement, auprès de la CNIL, via une procédure particulière, de même que les personnes fichées doivent être officiellement et formellement informées de l'existence du délégué, ce qui peut passer par une information sur le site internet de l'établissement .

Il y a plusieurs missions que doit réaliser le délégué à la protection des données. La première est incontournable, il doit avant tout informer et conseiller non seulement l'organisme qui l'a désigné, mais également les employés et les personnes qui vont mettre en œuvre ces opérations de conformité. La seconde mission est plus en relation avec l'extérieur, il s'agit de coopération avec l'autorité de contrôle qu'est la CNIL qui est à même de discuter avec l'organisme sur certains projets.

Mais le délégué peut aussi être le point de contact pour les personnes concernées par les traitements de données, et ces personnes bien sûr, peuvent aussi bien être des agents que des usagers d'une bibliothèque.

L'enquête révèle globalement que 25,51% des répondants déclarent ne pas savoir ce qu'est un Délégué à la protection des données et 30,75% des répondants ne connaissent pas ses missions.

Si on affine les résultats par catégories, on note une certaine disparité entre les agents. En effet s'agissant des catégories A, ils sont 51,95% à connaître les missions d'un DPD, 29,44% à ne pas les connaître et 18,61% à ne pas du tout savoir ce qu'est un DPD. Pour les catégories B, ils sont 29,63% à connaître les missions d'un DPD, 37,96% à ne pas les connaître et 32,41% à ne pas du tout savoir ce qu'est un DPD.

Enfin les catégories C, sont 23,08% à connaître les missions d'un DPD, 33,33% à ne pas les connaître et 43,59% à ne pas du tout savoir ce qu'est un DPD.

[46] DATA.GOUV.FR. Correspondants informatique et libertés [en ligne] Disponible à l'adresse : . https://www.data.gouv.fr/fr/datasets/correspondants-informatique-et-libertes-cil/

[47] CNIL. Désigner en ligne votre délégué à la protection des données auprès de la CNIL. [en ligne]. 28 mars 2018. Disponible à l'adresse : https://www.cnil.fr/en/node/24251

Cette disparité tient probablement au fait que les DPD interagissent davantage avec les cadres ou les chargés de mission notamment sur le SIGB.

On remarque une forte volonté des DPD de s'associer au sein de réseaux ou d'associations. Ainsi il existe principalement le réseau *SupDPO* qui regroupe les DPD des établissements de l'enseignement supérieur. SupDPO travaille en collaboration avec la Conférence des Présidents d'Université (CPU) et la CGE (Conférence des grandes écoles) Les missions de ce réseau sont les suivantes :

- favoriser les échanges et les partages d'expérience entre les DPD du réseau ;
- participer aux actions menées dans le cadre des partenariats CPU / CNIL et CGE / CNIL ;
- contribuer à une meilleure diffusion de la culture Informatique et Libertés vis-à-vis de tous les acteurs de l'enseignement supérieur (étudiants, enseignants-chercheurs, personnels administratifs).

Il existe également l'association UDPO (l'Union des DPO)[48], qui milite et assure des formations et examens notamment pour une certification des DPO.

L'AFCDP (Association française des correspondants à la protection des données à caractère personnel) a édité une Charte de déontologie du DPO[49] afin de promouvoir une culture de l'éthique des DPO. L'AFCDP préconise que la Charte soit également signée par le responsable de traitement ou son sous-traitant.

Et enfin l'ADPO (Association Data Protection Officers)[50], fondée par Alain Bensoussan (Avocat spécialisé en droit des technologies avancées) s'adresse

> *aux DPO des entreprises, pouvoirs publics, universités, etc., en France comme à l'international, et leur propose une palette unique de moyens et d'outils : commissions, groupes de travail, publications, veilles juridiques, organisation d'évènements, conférences, partenariats.*

En externe

Les partenaires possibles peuvent être soit des agences gouvernementales ou bien des associations de défense des usagers face au numérique.

La Commission nationale de l'informatique et des libertés (CNIL)

La loi du 20 juin 2018 relative à la protection des données personnelles modifie l'article 11 de loi n° 78-17 pour confier à la CNIL de nouvelles missions prévues par le règlement, ou compléter certaines missions déjà exercées.

Les autorités administratives indépendantes utilisent largement le droit souple, sous forme de recommandations ou de lignes directrices, dans le cadre de leur rôle

[48] UNION DES DPO. [en ligne]. Disponible à l'adresse : https://www.udpo.fr/

[49] ASSOCIATION FRANCAISE DES CORRESPONDANTS A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL. Charte de déontologie du DPO. [en ligne]. Disponible à l'adresse : https://afcdp.net/charte-de-deontologie-du-dpo/

[50] ASSOCIATION DATA PROTECTION OFFICERS.[en ligne]. Disponible à l'adresse : https://www.data-protection-officer-association.eu/

de régulation. Ce recours au droit souple est défendu par Isabelle Falque-Pierrtin qui a présidé la CNIL de 2011 à janvier 2019 pour trois raisons essentielles

- compte tenu des limites même de la norme générale dans un environnement en pleine mutation ;

- le traitement des données personnelles est de plus en plus déterritorialisé ;

- la protection des données personnelles est en train de changer de paradigme.

A ce sujet, Isabelle Falque-Pierrotin précise à propos du règlement (UE) 2016/679 que :

> *Initialement le régime juridique était fondé sur un système relativement binaire : formalités préalables (déclarations, autorisations, etc.) d'une part ; plaintes, contrôles et éventuellement sanctions, d'autre part. Cependant aujourd'hui, face à l'explosion des données personnelles et à leur circulation généralisée, la protection des données personnelles ne peut plus passer uniquement par ces deux volets sauf à accepter une action de régulation limitée et peu efficiente.*[51]

Parmi les instruments de droit souple, figurent les recommandations qui sans être juridiquement contraignantes par elles-mêmes, précisent les conditions d'application de la loi dans un secteur donné. Si, en règle générale, la CNIL examine chaque situation en tenant compte de ses caractéristiques propres, les recommandations visent une approche plus générale de la règle de droit.

La labellisation permet quant à elle, à un responsable de traitement qui le souhaite d'obtenir un label "CNIL", à condition de s'engager à respecter une série d'obligations définies par le régulateur, qui vont au-delà de la loi mais lui permettent en retour de se prévaloir de ce haut niveau de conformité à l'égard de ses clients.

Il est également possible de parler de référentiel.

Le 30 janvier 2019, la CNIL et la Conférence des présidents d'université (CPU) ont renouvelé leur convention de partenariat[52]. Ce partenariat a pour objectif de sensibiliser et former au respect de la protection des données les étudiants, enseignants, enseignants-chercheurs, chercheurs et personnels administratifs.

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Agence créée en 2009, rattachée au Secrétaire général de la défense et de la sécurité nationale elle a pour mission d'aider le Premier Ministre à coordonner l'action gouvernementale en matière de sécurité et de défense des systèmes d'information.

L'Anssi apporte son expertise aux entreprises mais également aux administrations. Son avis est en général suivi par le RSSI et peut avoir des contrecoups fâcheux sur la protection des données en bibliothèque. Un avis défavorable sur le réseau Tor a

[51] FRANCE. ASSEMBLEE NATIONALE. Étude d'impact - N° 490 – Projet de loi relatif à la protection des données personnelles [en ligne] disponible à l'adresse : http://www.assemblee-nationale.fr/15/projets/pl0490-ei.asp

[52] CNIL. La CNIL et la Conférence des Présidents d'Université (CPU) renouvellent leur convention de partenariat. [en ligne]. 30 janvier 2019. Disponible à l'adresse : https://www.cnil.fr/fr/la-cnil-et-la-conference-des-presidents-duniversite-cpu-renouvellent-leur-convention-de-partenariat

conduit le RSSI à supprimer *Tor browser* qui était installé sur les postes publics de la bibliothèque en 2016 à l'INSA Rennes. Dans son avis[53], l'Anssi reconnaît que Tor protège relativement bien ses utilisateurs du suivi des communications et donc leur vie privée sur Internet, mais peut aussi être utilisé à des fins malveillantes ; en effet grâce à l'emploi d'un réseau d'anonymisation tel que Tor, un utilisateur, dont l'intention n'est d'ailleurs pas forcément malveillante, peut recourir à cette solution pour contourner des mesures de sécurité mises en oeuvre pour limiter les risques de fuites d'informations, ou l'accès à des contenus inappropriés dans un établissement scolaire.

Lors de l'entrée en vigueur du RGPD, l'Anssi a mis en ligne un kit de la sécurité des données [54] Les bibliothèques peuvent s'appuyer sur ce kit pour mettre en place des formations. L'ANSSI a créé un MOOC (*Massive Open Online Course*) [55] afin de former le plus grand nombre sur la sécurité du numérique.

La Quadrature du Net

Association fondée en 2008, dans un contexte où les questions liées au numérique (liberté sur internet, surveillance, droit d'auteur) faisaient débat, la Quadrature du net (LQDN) a pour but la défense des droits et libertés des citoyens sur internet.

Cette association milite sur des sujets comme les données personnelles, la censure, la surveillance sur internet[56].

LQDN est un soutien majeur pour les bibliothèques (Lionel Maurel, conservateur de bibliothèque et juriste, est un des fondateurs historiques de l'association). Le 25 et 28 mai 2018, quelques jours après l'entrée en vigueur du RGPD, LQDN (mandatée par près de 10.000 personnes pour saisir la CNIL) alliée à une autre association, *None of your Business*, a déposé auprès de la CNIL une plainte contre Google pour non-conformité au RGPD. Le 21 janvier 2019, la CNIL a sanctionné Google à une amende de 50 millions d'euros[57] pour manquement à ses obligations de transparence et d'information vis-à-vis du traitement des données des internautes européens. La Cnil estime également que Google ne recueille pas suffisamment le consentement des internautes dans le cadre du traitement de leurs données à des fins de personnalisation de la publicité. En effet, pour créer son compte sur Google l'utilisateur est invité à cocher les cases « j'accepte les conditions d'utilisation de Google » et « j'accepte que mes informations soient utilisées telles que décrit ci-dessus et détaillées dans les règles de confidentialité ». Ce dispositif impose à l'utilisateur de consentir en bloc, pour toutes les finalités poursuivies par Google sur la base de cet accord (personnalisation de la publicité, reconnaissance vocale, etc.). Or, selon le RGPD, le consentement doit être donné pour chaque finalité de traitement et ce de façon distincte quand il y a plusieurs finalités. La CNIL estime donc que le consentement des utilisateurs n'est pas suffisamment éclairé. Il faut que

[53] Bulletin d'actualité du CERT-FR. 29 février 2016https://www.cert.ssi.gouv.fr/actualite/CERTFR-2016-ACT-009/

[54].ANSSI. RGPD, renforcer la sécurité des données à caractère personnel [en ligne]. Disponible à l'adresse : https://www.ssi.gouv.fr/administration/reglementation/rgpd-renforcer-la-securite-des-donnees-a-caractere-personnel/

[55]ANSSI. SecNumAcédémie [en ligne]. Disponible à l'adresse : https://www.ssi.gouv.fr/entreprise/formations/secnumacademie/

[56]LA QUADRATURE DU NET. [en ligne]. Disponible à l'adresse : https://www.laquadrature.net/

[57].CNIL. La formation restreinte de la CNIL prononce une sanction de 50 millions d'euros à l'encontre de la société Google LLC. [en ligne].21 janvier 2019. Disponible à l'adresse : https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la

l'internaute fasse la démarche de cliquer sur « plus d'options » pour accéder au paramétrage et ainsi avoir accès à la totalité des options. L'utilisateur n'a donc pas conscience de l'ampleur des traitements, et leurs usages compte tenu de l'opacité des documents et de leur nombre. Google a décidé de contester cette sanction.

Cependant le montant de cette amende est assez dérisoire, par rapport à ce que la CNIL aurait pu demander. En effet, le chiffre d'affaires de Google étant proche de 110 milliards de dollars, l'amende aurait pu s'élever à plus de 4 milliards d'euros (les 4% du chiffre d'affaires prévus par le RGPD). La CNIL aurait voulu faire un exemple de sanction, tout en restant acceptable.

Les bibliothèques peuvent donc s'appuyer sur des associations ou organismes de défense de droits des usagers du monde numérique, pour non seulement de la formation, de la prévention, ou encore des actions en justice.

OPERER DES CHOIX

Dans l'enquête à la question posée de savoir si « La protection des données à caractère personnel doit être un élément décisif dans le choix des outils ou services (abonnement à des bases de données, applications de réservation, livres électroniques ...) mis à disposition des usagers », ils sont 46,70 % à déclarer être entièrement d'accord avec cette proposition (échelle de note sur 5), 29,38% à donner la note de 4, et seulement 2,51% à ne pas être du tout d'accord avec cette affirmation[58].

Si l'on réduit les résultats aux agents travaillant dans un service « Ressources électroniques », le positionnement est moins tranché : », ils sont 36,36 % à déclarer être entièrement d'accord avec cette proposition (échelle de note sur 5), 30,30% à donner la note de 4, et aucun ne déclare ne pas être du tout d'accord avec cette affirmation. Ce positionnement peut être mis en rapport avec l'absence d'analyse sur les données personnelles dans les consignes de COUPERIN inscrits dans la feuille de route des négociateurs.

Nous verrons que les bibliothécaires peuvent infléchir leur politique en faveur de la protection de la vie privée, en opérant des choix en matière de politique documentaire (sur support numérique) mais également dans leur offre de services et outils mis à disposition de leurs usagers.

EN MATIERE DE POLITIQUE DOCUMENTAIRE

Comme l'indiquait, dès 2015, Thomas Fourmeux[59] en analysant un article de *Slate* qui traitait déjà des données personnelles en bibliothèques

> *Au-delà de nos prestataires techniques (SIGB/Portails), nous contractualisons de plus en plus avec une variété de fournisseurs : livres*

[58] Seuls les questionnaires complets ont été analysés, soit 439 répondants.

[59] BIBLIONUMERICUS. Qui contrôle les données des usagers des bibliothèques ? [en ligne]. 12 Novembre 2015. Disponible à l'adresse : https://biblionumericus.fr/2015/11/12/qui-controle-les-donnees-des-usagers-des-bibliotheques/

numériques, bases de données scientifiques, revues, systèmes de gestion de parcs informatiques, wifi. Autrement dit, nous multiplions les risques que les données personnelles des usagers puissent être utilisées par chacun de ces fournisseurs. La possibilité pour les usagers d'accéder aux données collectées (et exercer leurs droits définis en France par loi informatique et liberté de 1978) dépend donc des contrats établis entre l'établissement et un fournisseur qui conditionne la façon dont les données sont utilisées, exploités ou exposées.

Selon l'enquête si l'on restreint les résultats aux agents travaillant dans un service « Collections » c'est-à-dire d'achats, les chiffres sont sensiblement identiques, ils sont 46,94 % à déclarer être entièrement d'accord avec cette proposition (échelle de note sur 5), 26,53% à donner la note de 4, et 4,08% à ne pas être du tout d'accord avec cette affirmation.

Les abonnements aux bases de données

Internet est souvent perçu comme un espace de liberté et pourtant, c'est un espace où des contrôles sur l'identité de ses usagers sont fréquents. Ainsi pour accéder à de nombreux services, il est nécessaire de s'enregistrer et ensuite il existe une phase de contrôle d'accès. Durant cette phase, l'identité de l'utilisateur va être vérifiée. Le fournisseur d'accès a intérêt à contrôler l'identité pour distinguer ceux qui ont payé ou non pour accéder aux services, vérifier que les utilisateurs ont bien acquitté leurs droits. Très souvent, les services permettent de faire de la personnalisation et donc vérifier l'identité va permettre au fournisseur de service de fournir le contenu adapté.

En outre, cette vérification d'identité est également justifiée par une nécessité légale. L'utilisateur doit déposer ses données pour obtenir un service, et en conséquence le fournisseur, dans le respect de la loi, doit assurer la protection des données de ses utilisateurs. Mais cette obligation légale oblige l'utilisateur dans ses usages ; le fournisseur de service souhaite éviter que les utilisateurs détournent le service pour un usage non conforme ou même illégal. Enfin ce contrôle permet à l'éditeur d'améliorer le service en fonction de votre profil.

Les éditeurs définissent le mode d'accès à leurs ressources numériques. Il en existe plusieurs. Deux modes d'authentification (et donc de contrôle et de récolte des données à caractère personnel) sont possibles pour accéder aux bases de données : par reverse proxy ou par Shibboleth et EZ proxy. Shibboleth peut être utilisé seul mais on ajoute souvent un reverse proxy car tous les éditeurs n'implémentent pas Shibboleth notamment les petits éditeurs. EZ proxy est un reverse proxy mais propriétaire (OCLC).

Shibboleth utilise le mécanisme SSO (Single Sign On web). Il s'agit de la fédération d'identité qui rend l'accès plus simple et plus rapide aux ressources électroniques. L'usager se connecte sur le site d'un éditeur au moyen des codes personnels attribués par exemple par son université pour les autres services usuels (sans avoir à se connecter au préalable sur le site de sa bibliothèque universitaire, qui redirigeait ensuite sur le site de l'éditeur). Un des inconvénients de cet outil est que l'établissement n'est plus en mesure de faire le suivi fin des accès aux bases par ses utilisateurs.

Les éditeurs souhaitent garder une "connexion" avec l'authentification via nos systèmes et captent des données relatives à nos utilisateurs (login par exemple). Les statistiques de consultation sont uniquement possibles par l'éditeur. Par ailleurs, les éditeurs utilisent ces données d'exploitation pour notamment nourrir des algorithmes de préconisations de ressources.

Certains éditeurs comme *Encyclopedia universalis* utilisent un système de *cookie*, qui permet le traçage de l'utilisateur et lui donne accès à la ressource. C'est alors à l'éditeur de se mettre en conformité avec le RGPD.

Par le mécanisme du reverse proxy, les éditeurs acceptent que les établissements assurent l'authentification des utilisateurs. Les établissements conservent donc toutes données (login, Ip, Niveau d'études etc.) relatives à un utilisateur (de façon anonymisées). Les établissements peuvent donc en extraire des statistiques fines d'usage et les confronter à celles fournies par l'éditeur. C'est donc l'établissement qui doit veiller à sa conformité avec le RGPD

La proxyfication de l'accès aux ressources est ressentie comme malcommode par les chercheurs qui préfèreraient s'authentifier directement pour accéder à la documentation depuis l'URL publique. Les éditeurs utilisent cet argument pour pousser une authentification qui leur permettrait de récupérer un plus grand nombre d'attributs de la personne dans l'annuaire de l'université. Mais cela protège aussi les éditeurs car seules les personnes ayant des identifiants valides et contrôlés peuvent se connecter à leurs bases

Pour faciliter l'accès aux ressources numériques, il faut signaler le projet *RA21*[60] (*Resource Access for the 21st Century*), à l'initiative de *International Association of Scientific, Technical, and Medical Publishers* et *National Information Standards Organization*. L'objectif de RA21 est d'aligner et de simplifier les voies d'accès aux plateformes scientifiques participantes. RA21 reconnaît des objectifs différents selon les fournisseurs, les utilisateurs et notamment :

- Fournir un accès individualisé et différencié pour une meilleure communication des informations aux organes directeurs et aux clients
- Offrir des services personnalisés pour accélérer la compréhension et la découverte
- Assurer l'intégrité du contenu sur les plateformes institutionnelles et commerciales
- Réduire la lourdeur administrative liée à la fourniture d'accès aux communautés d'utilisateurs autorisés
- Maximiser l'utilisation des ressources achetées
- Protéger la vie privée des communautés d'utilisateurs et défendre leur sécurité[61]

Le projet s'engage également auprès des bibliothèques en renforçant l'utilisation des ressources mais aussi en visant à permettre une granularité de leur utilisation, tout en leur permettant de protéger l'identité de leurs utilisateurs.

Depuis l'entrée en vigueur du RGDP, certains éditeurs de base de données ont envoyé des avenants aux contrats en cours directement aux établissements. Certains

[60] https://ra21.org/

[61] https://ra21.org/index.php/what-is-ra21/

établissements ont donc sollicité leur délégué à la protection des données pour avis sur ces avenants.

Ainsi un avenant pour la base *Taylor & Francis* a fait l'objet d'une analyse juridique d'un DPD d'une université, et ce dernier émet des réserves sur plusieurs clauses :

> *Proposition de clause de la part de l'éditeur « celui-ci peut alors collecter ces informations dans un fichier spécifique au Titulaire de licence (les différentes fins définies dans la présente clause 7.1 seront collectivement nommées « Fins »). »*
>
> *Analyse du DPD : « La clause 7.1 n'est pas recevable, elle annonce elle-même qu'elle propose une définition floue des finalités.*
>
> *Fondement juridique : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, art 5 « Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités »*
>
> *Proposition de clause de la part de l'éditeur : « Ces données pourront être utilisées aux fins directement associées au Matériel sous licence et peuvent uniquement être fournies aux parties tierces au format agrégé »*
>
> *Analyse du DPD : « Qu'est ce qui est entendu par l'expression « format agrégé » ? Les articles 20 et 28 du Règlement exigent que le fournisseur nous donne des détails techniques afin que nous soyons assurés du respect du droit à la portabilité.*
>
> *Fondement juridique : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, art 20 « Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine ».*[62]

Il est également souhaitable de mettre en corrélation les statistiques de consultation des bases de données, et les types d'usagers, pour ajuster éventuellement la politique documentaire, l'offre de formation ou encore la valorisation des ressources de l'établissement. L'outil EzPaarse, logiciel libre et gratuit développé par le consortium Couperin et par l'Inist-CNRS, outil d'évaluation des ressources numériques, permet notamment de quantifier les accès des usagers, par leurs connexions mais de manière anonyme : le protocole d'anonymisation des logs est compris dans le package EZPaarse. On mentionnera, que déjà utilisé par près de 60 établissements de l'Enseignement supérieur et de la recherche en France, les performances de ce logiciel ont favorisé le prochain partenariat, en février 2019 entre OCLC et Couperin. Il s'agit pour les deux organismes de s'associer avec deux objectifs communs : « l'amélioration du logiciel d'authentification EZproxy d'OCLC par Couperin, et le développement de l'utilisation du logiciel EZPaarse de Couperin hors de France grâce aux établissements membres d'OCLC »[63].

[62] Echange avec J. Kalfon. Couperin.

[63] JOST, C. « OCLC et Couperin s'associent en faveur de leurs logiciels respectifs EZproxy et ezPAARSE ». *Archimag.com* [en ligne], 15 février 2019. Disponible à l'adresse https://www.archimag.com/bibliotheque-

Comme l'indique Cécile Touitou[64] :

> *On peut rêver que dans un avenir proche, ces données globales pourront être affinées par type d'usagers.*

Les livres électroniques

Les *Digital Rights Management* (DRM) sont une technique de protection et de gestion de restriction numériques. C'est une protection pour les œuvres couvertes par le droit d'auteur. Il s'agit de concilier droit d'auteur et protection de la vie privée des lecteurs de livres électroniques.

En octobre 2013 et octobre 2014, le principal éditeur de DRM, Adobe Digital Editions, a été identifié comme ayant d'importantes failles de sécurité ayant entraîné la fuite de données de ses utilisateurs[65].

En mai 2018, dans une lettre ouverte[66] adressée aux professionnels des bibliothèques *Savoir com1* a pris la position suivante :

> *nous condamnons fortement les ressources qui s'adossent à des DRM qui constituent une menace pour les libertés numériques et les droits fondamentaux des individus. Non seulement les DRM installent des enclosures sur la connaissance mais en plus ils représentent bien souvent des menaces pour la vie privée des internautes. Nous recommandons par exemple aux bibliothèques d'éviter les prestataires de livres numériques qui reposent sur la solution de gestion de droits numériques d'Adobe Digital Editions.*

En juin 2018, Hervé Bienvault alertait sur son blog *Aldus*[67], des problèmes de non-conformité avec le RGPD du logiciel DRM Adobe et d'un défaut flagrant d'information de l'éditeur sur l'utilisation des données personnelles de ses usagers. L'accent est mis sur les dysfonctionnements de la version 4 du logiciel, et l'auteur recommande d'utiliser la version précédente qui semble être moins litigieuse sur l'utilisation des données personnelles. Dans ce même billet, il est rappelé qu'en 2014 Adobe avait déjà fait l'objet de critiques aux Etats-Unis et en Grande-Bretagne sur l'utilisation des informations fournies par les lecteurs.

La politique de la plateforme *OpenEdition*, est très claire sur ce sujet. Les E-books sont accessibles sans aucun DRM.

---

edition/2019/02/15/oclc-couperin-associent-developper-logiciels-respectifs-ezproxy?fbclid=IwAR0mtv-nPbykNDWYq0l3WXvWvQd-A5V6GDmf4fFcwW-TQLpKPs2DAkvJZiE

[64] TOUITOU, C. « Marketing, mais encore ? » dans Bibliothèques universitaires : nouveaux horizons. Editions du Cercle de la librairie. p. 270

[65] ADAM, L. Adobe Digital Editions, un programme un peu trop curieux ? *ZDNet* [en ligne]. 8 octobre 2014. Disponible à l'adresse : https://www.zdnet.fr/actualites/adobe-digital-editions-un-programme-un-peu-trop-curieux-39807423.htm

[66] SAVOIRS COM1. Lettre ouverte adressée aux professionnels des bibliothèques pour une mise en conformité du RGPD. [en ligne] 5 mai 2018. Disponible à l'adresse : https://www.savoirscom1.info/2018/05/lettre-ouverte-adressee-aux-professionnels-des-bibliotheques-pour-une-mise-en-conformite-du-rgpd/

[67] ALDUS.DRM Adobe : en attente de la conformité au nouveau RGPD . [en ligne]. 1er juin 2018. Disponible à l'adresse :https://aldus2006.typepad.fr/mon_weblog/2018/06/drm-adobe-en-attente-de-la-conformit%C3%A9-au-nouveau-rgpd.html

Non dans un souci de protection des données personnelles, mais plutôt de verrouillage des fichiers, le consortium Couperin avait en 2013 refusé une offre de l'éditeur Numilog pour cause de DRM[68].

Pour éviter le logiciel Adobe, il existe un nouveau type de DRM, dit allégé. Le logiciel *Readium LCP*, selon l'analyse faite en 2017 par Thomas Fourmeux, *Readium LCP* est protecteur des données personnelles des usagers, aucun tiers n'ayant accès aux statistiques et aux données du lecteur. Ce nouveau DRM fait l'objet d'une attention toute particulière de l'ERDLAB et est en passe de devenir un standard international[69]

Le consortium Couperin, la puissance d'un réseau

Le consortium Couperin, association à but non lucratif qui a pour mission notamment d'évaluer, négocier et organiser l'achat de ressources documentaires numériques au bénéfice de ses membres. Couperin s'attache également à développer un réseau national de compétences et d'échanges en matière de documentation électronique notamment concernant les politiques d'acquisitions, les plans de développement de collections, les systèmes d'information, les modèles de facturation des éditeurs, l'ergonomie d'accès, les statistiques d'usage...

L'accent est également mis sur les relations contractuelles avec les éditeurs de ces ressources numériques. Couperin met à disposition de ses membres plusieurs documents d'analyse et de négociation avec les éditeurs.

A titre d'exemple, le document « Offre idéale d'e-book », datant de 2009, prônait déjà l'absence de DRM pour les livres électroniques. L'argument avancé était la libéralisation des usages, mais cela bénéficie, dix années plus tard, à la protection des données des utilisateurs.

Avec l'entrée en vigueur du RGPD, certains membres du consortium Couperin se sont inquiétés de la conservation des données des utilisateurs par les éditeurs de bases de données. Le Consortium devra lister les différentes pratiques des éditeurs en matière de protection des données personnelles des usagers. Plusieurs points litigieux pourraient faire l'objet d'un positionnement, voire de négociation entre les éditeurs et Couperin. Les questions d'accès et d'identification des usagers est le point central de la protection des données personnelles, et donc celle de la confiance accordée à la bibliothèque, intermédiaire entre l'éditeur et l'utilisateur.

Nous pouvons évoquer plusieurs cas, qui peuvent être questionnés. Ainsi l'éditeur, grâce à l'authentification, peut capter des données relatives à l'utilisateur (via le login de connexion), et éventuellement déceler une non-conformité des conditions d'usages ; l'usager n'est pas averti de telles pratiques. Le Consortium pourrait demander la fin de ces modalités d'accès, ou du moins en informer clairement les utilisateurs. Une autre modalité d'accès aux bases de données peut se faire par la création, obligatoire d'un compte personnel pour accéder au service une fois le lecteur arrivé sur la plateforme (plateforme dont l'accès a été ouvert via une authentification locale) ; l'éditeur récupère donc des données à caractère personnel alors que le service est offert par la bibliothèque. Enfin, une dernière possibilité

[68]COUPERIN. Négociations arrêtées. Numilog. [en ligne]. Disponible à l'adresse : https://www.couperin.org/negociations/archives/item/303-numilog

[69] OURY, Antoine. Une DRM ouverte basée sur LCP en passe de devenir un standard. *Actualitté*, .[en ligne] 12 septembre 2018. Disponible à l'adresse : https://www.actualitte.com/article/lecture-numerique/une-drm-ouverte-basee-sur-lcp-en-passe-de-devenir-un-standard/90877

offerte aux usagers est celle qui consiste pour ces derniers d'accéder à des services supplémentaires (archivage de ses requêtes) sous condition de se créer un compte. L'utilisateur est libre de laisser ou non ses données personnelles directement sur le site du fournisseur, on peut donc se demander si la bibliothèque a une responsabilité particulière vis-à-vis de ce dernier.

En matière de protection des données personnelles, le consortium peut jouer un rôle d'impulsion important lors des négociations avec les éditeurs, mais également alerter les bibliothécaires sur certaines pratiques ou points de vigilance.

A l'heure actuelle, les fiches d'évaluation des ressources, consultables sur le site de Couperin, ne mentionnent pas la question de l'utilisation des données par les éditeurs. Après l'entrée en vigueur, certains éditeurs ont commencé à envoyer des avenants aux contrats signés par différents établissements pour se mettre en conformité avec la loi. Cependant, ces avenants sont loin d'être exemplaires et une centralisation des avenants au niveau de Couperin serait souhaitable.

Refuser une offre, même gratuite pour protéger les usagers

Quant à la garantie de la non réutilisation des données personnelles des lecteurs par les éditeurs commerciaux, cela peut être un élément à prendre en compte pour un abonnement. Ainsi un SCD avait reçu une offre gratuite *d'Adaptative Channel*, qui proposait un accès aux étudiants pour un an. Ces derniers devaient installer sur leurs *smartphone* une application et donc enregistrer leurs données personnelles. Faute de réponse du fournisseur quant à l'utilisation notamment commerciale des données personnelles des étudiants, le SCD a refusé cette offre néanmoins gratuite.

En pareille situation, l'adage « Si c'est gratuit, c'est vous le produit », pourrait certainement s'appliquer. En effet, une entreprise commerciale ne fait jamais d'offre réellement gratuite ; les données (profil, connexion, consultation etc.) des utilisateurs pourraient être revendues à d'autres entreprises commerciales.

Favoriser l'open access

L'Open access, selon la définition fournie par le Consortium Couperin est un « mode de diffusion des articles de recherche sous forme numérique, gratuite et dans le respect du droit d'auteur ».

Un éditeur commercial a trois éléments à défendre lors d'une négociation commerciale : son contrat avec les auteurs (et plus particulièrement la cession de l'exclusivité de l'auteur à l'éditeur), la taille de sa plateforme (plus celle-ci est grande par le volume, plus elle draine de flux et donc de consultation) et enfin le dernier qui découle des deux premiers : la réputation, la marque.

Dans le schéma de l'Open access, la plateforme de l'éditeur n'est plus le seul point d'accès à la publication et donc l'accès est libre. Cet accès peut se faire par authentification ou sans identification et dans ce cas le traçage du lecteur est moindre.

SUR LES OUTILS ET SERVICES OFFERTS

Les outils technologiques de protection de la vie privée consistent en une variété de logiciels spécialisés. Ceux-ci incluent Web plugins de navigateur qui contrarient le suivi comportemental et la collecte de données, des outils pour

protéger les données de transit (par exemple réseaux privés virtuels -VPN), ou à masquer son adresse IP (par exemple, le navigateur *Tor*), ou encore le chiffrement des données stockées.

Les moteurs de recherche et outils de découverte

Les principaux moteurs de recherche Web, tels que Google, Bing et Yahoo, collectent des informations sur l'historique des recherches des utilisateurs, et de nombreuses informations personnelles. En vendant ces données à des annonceurs, des courtiers en données, ces entreprises sont capables de réaliser des bénéfices tout en fournissant « gratuitement » un outil. En plus de tirer profit des données des utilisateurs, les moteurs de recherche Web les utilisent également pour améliorer l'expérience utilisateur de leurs produits. La collecte et l'analyse des données utilisateur permettent aux systèmes de connaître les préférences de l'utilisateur en fournissant des résultats de recherche personnalisés facilitant la navigation. La collecte et le partage des données des utilisateurs qui se produisent sur le Web sont profondément troublants pour les bibliothèques, dont l'éthique professionnelle incarne les valeurs de la vie privée et de la liberté intellectuelle.

L'université de Nantes et celle de Rennes 1 ont pris la décision d'installer, en janvier 2019, le moteur de recherche *Qwant*[70] sur l'ensemble de ses ordinateurs. Le vice-président de l'université en charge du numérique de l'université de Nantes marque ainsi la volonté d'assurer la protection de la vie privée, la confidentialité des données personnelles de l'ensemble de la communauté universitaire. Le choix s'est porté sur cet outil qui d'une part ne conserve aucun des historiques de recherche de ses utilisateurs et d'autre part qui stocke des données en France. *Qwant* se distingue par sa transparence dans le domaine de la vie privée.

On peut également signaler le projet du moteur de recherche *INNOOO*[71], dont l'idée fondatrice est l'absence de publicité (la cible annoncée est celle des services publics : école, hôpital ; tribunal. Les bibliothèques ne sont pas citées. *INNOOO* propose à l'internaute d'isoler ses trois vies (symbolisées par les trois O de son nom) : le cercle de la vie privée, celui de la vie professionnelle et enfin celui de la vie publique sur internet.[72]

Plus largement, l'enjeu n'est pas seulement un enjeu de protection des données de navigation. Il y a aussi et de manière indirecte un enjeu de formation : les moteurs de recherche comme *Qwant*, *Duckduckgo* ou *Startpage*, en ne basant pas leur chiffre d'affaire sur le monnayage de l'historique de navigation de l'utilisateur (le modèle économique repose sur de la publicité non ciblée) permettent également à chacun de sortir de sa bulle de filtre. La bibliothèque est-elle libre d'installer sur ses postes par défaut d'autres navigateurs et moteurs de recherche que ceux promus par sa DSI qui parfois n'est guère sensible à ces enjeux ?

Protéger la confidentialité des utilisateurs au-delà des enregistrements d'emprunt, tout en permettant l'utilisation éthique des données des utilisateurs pour améliorer

[70] https://www.qwant.com

[71] https://www.innovativity.org/moteur-de-recherche-innooo.php?PHPSESSID=

[72] RUBIELLO, Luc. La face cachée d'internet et des données personnelles. Innovativity. 2018, p.106-119

l'expérience utilisateur est une des questions posées par la mise en place d'outils de découverte[73].

Les outils de découverte de bibliothèque actuels se répartissent en trois catégories : les catalogues en ligne, les couches de découverte, et les outils de découverte à l'échelle Web (un interface utilisateur améliorée reposant sur un index central réunissant les ressources du catalogue de bibliothèque, des bases de données d'abonnements et des référentiels numériques). Ces outils sont généralement intégrés à divers systèmes externes, notamment des serveurs proxy, des prêts entre bibliothèques et des bases de données, sites Web d'éditeurs individuels, etc. Pour la plupart, les bibliothèques achètent des outils de découverte auprès de fournisseurs tiers. Certaines bibliothèques utilisent des couches de découverte open source, mais il n'existe actuellement aucune option open source pour les outils de découverte à l'échelle du Web.

Même si ces outils devaient évoluer pour devenir eux-mêmes absolument privés (sans collecte ni partage de données), d'autres partenaires (fournisseur d'accès à internet, navigateurs Web, annonceurs, etc.) auraient toujours accès aux données utilisateur par d'autres moyens, tels que les cookies et les traces numériques. La réalité opérationnelle et technique est telle que les bibliothèques ne peuvent contrôler immédiatement ni complètement la confidentialité. Les bibliothèques ne peuvent à elles seules garantir la confidentialité de leurs usagers, mais elles peuvent et doivent en atténuer les méfaits dans la mesure du possible. Dans le même temps, ignorer complètement les avantages de l'utilisation des données des utilisateurs pour améliorer l'expérience de découverte peut menacer la viabilité de la bibliothèque à l'ère de Google. Si les systèmes excluent toutes les données personnelles et les données relatives à l'utilisation, les services résultants seront unidimensionnels et stériles. Les bibliothèques doivent fournir des services personnalisés, dynamiques, pour rester attractives dans l'environnement actuel.

Les bibliothèques sont de plus en plus à la merci de tiers pour le développement et la conception d'outils de découverte. Malheureusement, ces tiers n'ont pas les mêmes obligations éthiques que les bibliothécaires de protéger la vie privée de leurs clients. En outre, les directives existantes sur la protection des données utilisateur dans les technologies de bibliothèque s'adressent aux bibliothécaires et non aux fournisseurs tiers. La communauté des bibliothèques doit tenir les tiers responsables de la conception éthique des outils de découverte des bibliothèques. Une stratégie pour ce faire serait de développer un processus de classement ou de certification de ces outils basé sur un ensemble de standards de la communauté. La mention de la protection des données à caractère personnel doit également être mentionnée dans le cahier des clauses techniques pour tout marché public ; et si possible lui accorder une note élevée au moment de l'analyse des offres.

Les logiciels libres, un gage de protection

Le choix d'un logiciel libre permet d'assurer une plus grande protection des données à caractère personnel. En effet, les développeurs de logiciel libre,

[73] PEKALA, S. « Privacy and User experience in 21st Century library discovery ». *Ital* [en ligne], 2017, Vol 36, N°2. Disponible à l'adresse : https://ejournals.bc.edu/ojs/index.php/ital/article/view/9817

s'appuyant sur leur éthique, propose des codes exempts de transfert de données personnelles vers des fonctionnalités marketing.

Les logiciels libres assurent également la protection de la vie privée. Ainsi l'association *Framasoft* (réseau d'éducation populaire, issu du monde éducatif) vise à développer des services en ligne libres, éthiques, décentralisés et solidaires afin de permettre aux utilisateurs de trouver rapidement des alternatives aux produits de Google (entre autres) mais respectueux de leurs données et de leur vie privée. Dans sa charte, l'association s'engage à démontrer : « sa probité en permettant à chaque utilisateur de vérifier le code source, éventuellement de l'améliorer, et surtout de s'assurer qu'aucun usage déloyal ne sera fait de ses données, de son identité et de ses droits. »[74]

En 2014, *Framasoft* lançait une campagne visant à promouvoir les logiciels libres face aux puissants GAFAM (Google, Apple, Facebook, Amazon, Microsoft). Le projet « Dégooglisons Internet » devait s'étaler sur trois années et proposer 30 services alternatifs tous issus du libre. Ce projet a pris fin en 2017. A titre d'exemple de service alternatif proposé on peut signaler le projet *Chatons.org*. (Collectif des Hébergeurs Alternatifs, Transparents, Ouverts, Neutres et Solidaires). Il vise à rassembler des structures souhaitant éviter la collecte et la centralisation des données personnelles au sein de silos numériques du type de ceux des GAFAM

En 2015, lors d'une journée organisée par l'ABF sur les données personnelles en bibliothèques[75], la pratique de la Bulac a fait l'objet d'un exposé et plus précisément sur les logiciels libres. Le SIGB de la Bulac, est développé sous un logiciel libre Koha (sous Linux). Mettre à disposition du public des ordinateurs en libre accès, dotés de Linux, permet qu'à chaque fermeture de session, les données sont effacées.

En 2015, un accord signé entre le Ministère de l'Education nationale et Microsoft a été vivement critiqué, notamment sur la question des données personnelles des élèves. Une charte entre les deux signataires a fait l'objet d'une analyse critique de la CNIL. Cette dernière soulignait notamment l'absence dans la charte de la protection des données des enseignants (seuls les étudiants étaient mentionnés), et un manque de précision sur les conditions de l'analyse des traces de l'apprentissage.[76]

Les logiciels libres peuvent également être utilisés pour l'analyse des flux et fournir des statistiques. *Matomo* (anciennement dénommé *Piwik*) est un des logiciels libre et open source de mesure statistique web. S'agissant de la mesure d'audience des cookies, le consentement des internautes doit être recueilli. Il existe cependant des exemptions, dont la CNIL liste les conditions[77]. *Matomo,* est un des deux outils exemptés du recueil du consentement par la CNIL Il fournit des fonctionnalités additionnelles qui ne sont pas directement liées à l'analyse du trafic. Parmi celles proposées, il en est une consacrée à la vie privée —et permet d'anonymiser les

[74] FRAMASOFT. *Charte*. https://framasoft.org/fr/charte/

[75] VIGUIE, C. « Données personnelles et usagers : quel rôle pour les bibliothécaires ? ». *Bulletin des bibliothèques de France (BBF)*[en ligne], 2016, n° 7, p. -. Disponible à l'adresse : <http://bbf.enssib.fr/tour-d-horizon/donnees-personnelles-et-usagers-quel-role-pour-les-bibliothecaires_65756>.

[76] ADAM , L. Microsoft/Education nationale : la CNIL émet des réserves. *ZDnet* [en ligne].27 juin 2017. Disponible à l'adresse : https://www.zdnet.fr/actualites/microsoft-education-nationale-la-cnil-emet-des-reserves-39854192.htm

[77]CNIL. Solutions pour les cookies de mesure d'audience. [en ligne]. 15 décembre 2017. Disponible à l'adresse : https://www.cnil.fr/fr/solutions-pour-les-cookies-de-mesure-daudience

adresses IP, de supprimer régulièrement certaines données, de choisir si l'on souhaite ne pas être suivi. Cette possibilité peut expliquer l'importante part de marché (13%) de *Matomo* en Allemagne.[78].

Les *learnings analytics*, ayant pour vocation de mesurer l'engagement étudiant peuvent avoir un impact sur les bibliothèques, notamment en demandant aux bibliothécaires par exemple de croiser les titres empruntés ou téléchargés depuis le catalogue, avec ceux de la bibliographie du cours présent sur une plateforme de type Moodle. S'agissant des *learning analytics* le rapport « L'école sous algorithmes »[79], publié en 2016 par le *think thank* français Terra Nova plaide :

> *pour une prise de conscience des enjeux politiques sous-jacents au choix d'outils pédagogiques employés dans les écoles, à l'égard des promesses des learning analytics (analyse des modalités d'apprentissage pour déceler des profils pédagogiques et personnaliser l'enseignement) et les craintes de commercialisation des données des élèves par des entreprises privées. Les auteurs insistent sur la nécessité de construire un environnement juridique adéquat pour que l'État puisse se doter de logiciels appropriés, avec des mécanismes de contrôle par les pouvoirs publics (comme l'Office parlementaire d'évaluation des choix scientifiques et technologiques) ; ils soulignent également le besoin en termes de comparaisons internationales, pour étudier les relations tissées dans d'autres systèmes éducatifs avec les acteurs du numérique.*

Les ordinateurs offrant internet en libre-accès

Le débat sur la surveillance des usagers utilisant les ordinateurs mis à leur disposition dans les bibliothèques fait débat au sein de la profession. Les bibliothécaires basent leur argumentation sur deux concepts, parfois de façon opposée : l'application de la loi et la liberté d'accéder à l'information.

On distingue des points de vue différents selon les types de bibliothèques : bibliothèques de lecture publique et bibliothèques universitaires. En effet, en bibliothèques de lecture publique, la protection des mineurs est mise en avant alors qu'en bibliothèques de l'enseignement supérieur (avec un public majoritairement majeur, à l'exception du public lycéen) le vaste champ des sujets de recherche justifie toute absence (ou faible) surveillance.

L'enquête confirme cette divergence selon les différents établissements, et surtout selon leurs différents publics.

[78] WIKIPEDIA. Matomo. [en ligne]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/Matomo_(logiciel)

[79] AGACINSKI, D ; BRUN, F, ISART, C, JAMES, M. L'école sous algorithmes. Terra Nova, [en ligne. 10 mars 2016. Disponible à l'adresse : http://tnova.fr/etudes/l-ecole-sous-algorithmes

« Estimez-vous avoir une responsabilité quant à l'usage des ordinateurs publics de la bibliothèque ? » (Plusieurs réponses étaient possibles).		
	Agents travaillant en bibliothèques territoriales (173 réponses)	**Agents travaillant en bibliothèques universitaires (190 réponses)**
Oui, pour garantir un usage équitable entre tous les utilisateurs	73,41%	60%
Oui, pour empêcher la consultation de sites interdits par la loi	61,85%	49,47%
Oui, pour empêcher la consultation de sites inappropriés pour des jeunes lecteurs	68,21%	37,37%
Oui, pour permettre une consultation la plus sûre et confidentielle possible	83,82%	73,16%
Non, pas de responsabilité particulière	2,89%	10,53%

Le législateur, en 2004 (Loi pour la confiance dans l'économie numérique) et 2006 (Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers) a validé une approche sécuritaire sur la surveillance. Selon la législation, les fournisseurs d'accès ont donc l'obligation de détenir et conserver les « données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont (ils) sont prestataires » et de communiquer ces données à l'autorité judiciaire, sur demande de cette dernière. Sont également tenus à l'obligation de conservation des données de connexion « 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 »[80] S'agissant des établissements qui offrent, dans un cadre public, à des visiteurs une connexion en ligne, et les « fournisseurs d'accès à des réseaux de communications électroniques accessibles via une borne wifi » que ce soit à titre payant ou non, sont également soumis à cette obligation. En 2011, un décret a précisé les données qui devaient être conservées par les fournisseurs d'accès et hébergeurs pour permettre l'identification des personnes ayant contribué à la création d'un contenu en ligne.

[80] Code des postes et des télécommunications électroniques. art. L34-1. Disponible à l'adresse : https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070987&dateTexte=20190221

Compte tenu de l'ampleur de la surveillance, le fantôme du *« big brother* numérique » a été avancé. En 2007, la CNIL a fait part d'une certaine réserve du fait de l'imprécision du texte et du risque de dérive possible.

En 2014[81] et 2016[82], la Cour de Justice de l'Union européenne (CJUE) s'est prononcée contre la conservation généralisée des données connexion et invalidé la directive 2006/24/CE du Parlement européen et du Conseil 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 Compte tenu de ces décisions, plusieurs associations, dont la Quadrature du Net, ont demandé en juillet 2018 que 17 Etats membres de l'Union européenne, dont la France, se conforment à cette jurisprudence. Le projet de recherche *NetCommons* va même plus loin en recommandant aux opérateurs de se conformer au droit européen supérieur, selon la hiérarchie des normes, au droit français[83]. Mais quel poids aurait une bibliothèque de taille moyenne avec cet argument face à une tutelle qui veut faire appliquer la loi française ?

Au sein des bibliothèques, la question de l'identification d'un usager utilisant un ordinateur en libre accès, est différemment appréciée. Certains établissements enregistrent nom, prénom et heure de la session (avec numéro du poste), dans le respect de la législation française, d'autres refusent tout enregistrement faisant valoir le principe de la hiérarchie des normes et donc les décisions de la CJUE.

En 2016, l'ABF publiait la « Charte du droit fondamental des citoyens à accéder à l'information et aux savoirs par les bibliothèques »[84]. L'article 6 « Le droit d'accéder à un internet public ouvert et fiable », dispose d'une part que « les bibliothèques ne doivent pas mettre en place de restrictions ou de contraintes à l'accès internet autres que ce que prévoit la loi, que ce soit en termes d'identifications des usagers, de restrictions de la bande passante ou de filtrage de contenus » et d'autre part que « lors de leur consultation d'Internet à la bibliothèque, les citoyens doivent avoir la garantie que leur droit à la vie privée es respecté et qu'aucune donnée personnelle les concernant n'est collectée, ni transmise à des tiers en dehors des cas explicitement prévus par la loi ». La profession s'engage donc vers un accès très libre à Internet et une protection maximale de la vie privée des usagers. Cependant dans la pratique, selon les établissements mais aussi selon le contexte politique ou social, cet engagement peut être perçu différemment.

En 2017, la *Gazette des Communes* posait la question suivante : « Les bibliothèques risquent-elles d'être instrumentalisées par la lutte anti-terroriste ? », en relayant le communiqué de l'ABF appelant ses adhérents à protéger la vie privée des usagers. Ce n'est pas sans rappeler dans les années 50, sous le Maccarthysme, l'infiltration d'agents du *Federal Bureau of Investigation*- FBI- (Agence créée et dirigée par John Edgar Hoover, ancien vacataire à la bibliothèque du Congrès) dans

[81] CJUE, n° C-293/12, Arrêt de la Cour, Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a, 8 avril 2014

[82] CJUE, aff C-203/15, Tele2 Sverige AB c/ Post-och telestyrelsen et aff C-698/15, Secretary of State for the Home Department c/Tom Watson e.a, 21 décembre 2016

[83] NETCOMMONS. Internet en libre accès. p.4 [en ligne]. Disponible à l'adresse https://www.netcommons.eu/sites/default/files/2018-01-29-guide_internet_en_libre_acces.pdf

[84] La Charte a été mise à jour le 12 octobre 2018.

les universités américaines pour surveiller la nature anti-américaine des activités des organisations politiques et d'éducation

En février 2018, l'association La Quadrature du Net a mis en ligne un guide juridique « Internet en libre accès : obligations en matière de vie privée et de liberté de communication »[85]. Comme indiqué sur le site internet de l'association, ce guide était initialement à destination des bibliothèques, mais est également valable pour toute structure mettant à disposition un accès à internet.

En juin 2018, la revue de l'ABF, *Bibliothèque(s)* a publié deux points de vue de bibliothécaires sur le sujet : « Devenir bibliothécaire, devenir militante » et « Militant de la liberté ou sentinelle du pacte républicain ? ». Chloé Lailic[86] (directrice de la bibliothèque de l'Insa de Rennes) dans le premier article affirme que les dispositions prises depuis la Loi renseignement et destinées à lutter par la surveillance électronique des communications contre les menaces terroristes sont de vraies menaces pour les libertés, et que leur efficacité pour empêcher tout attentat n'est pas prouvée. Selon elle, les mesures de protection sont en fait des mesures de surveillance et de contrôle. En contrepoint à cette position, Anna Marcuzzi (directrice des médiathèques de la ville et de l'Eurométropole de Strasbourg)[87] affirme que le bibliothécaire, fonctionnaire et non militant, peut en effet être confronté à des conflits de valeurs : la protection des données personnelles ou une protection plus large que serait le Pacte Républicain.

Les bibliothèques ne peuvent être tenues responsables des agissements de leurs usagers. En cas de problèmes de consultation de sites litigieux, les bibliothécaires ne sont pas compétents, il s'agit du ressort des services de police.

Ce débat a mis en lumière des divergences sur le positionnement déontologique des bibliothécaires : entre respect du droit d'un côté et accusation de militantisme de l'autre. L'inspection générale des bibliothèques tiendra un séminaire en 2019 sur les questions de surveillance en bibliothèque.[88]

DES PRECONISATIONS DE LA PART DES BIBLIOTHECAIRES

Lors de la journée d'étude de l'ABF en janvier 2018 sur « (*Auto)-censure et surveillance de masse, quels impacts pour les bibliothèques ?»*, le président de l'ABF, Xavier Galaup, rappelait que les bibliothèques et les bibliothécaires bénéficient de la confiance de leurs usagers, et que nous devons donc en être responsables.

[85]LA QUADRATURE DU NET. Guide juridique : internet en libre accès, quelles obligations ? [en ligne]. 31 janvier 2018. Disponible à l'adresse : https://www.laquadrature.net/2018/01/31/guide_internet_libre_acces/

[86] LAILIC, C « *Devenir Bibliothécaire, devenir militante* ». Bibliothèque(s), N° 92-93 Juin 2018, p. 150-151

[87] MARCUZZI, A. *« Militant de la liberté ou sentinelle du Pacte Républicain ?* ». Bibliothèque(s), N° 92-93 Juin 2018, p. 151-153

[88]BIBLIONUMERICUS. 2019, intimité numérique et données personnelles : le combat des bibliothécaires ?[en ligne]. 3 février 2019. Disponible à l'adresse : https://biblionumericus.fr/2019/02/03/2019-intimite-numerique-et-donnees-personnelles-le-combat-des-bibliothecaires/

Une prise de conscience, parfois difficile, des professionnels

En 2015 un bibliothécaire de la *Kobe High School* a dévoilé des souches d'emprunt de l'écrivain japonais Haruki Murakami[89] et publiées par le journal Kobe Shimbun. La *Japan Library Association* s'est insurgée, contre cette violation de la vie privée puisque l'utilisateur, n'a jamais donné son consentement à cette divulgation.

Jean-Pierre Le Bouler et Joëlle Bellec Martini, conservateurs à la Bibliothèque nationale, ont établi la liste des emprunts effectués par George Bataille à la Bibliothèque nationale entre 1922 et 1950. Cette liste figure dans le tome XII des œuvres complètes de Georges Bataille, publié par Gallimard en 1988[90]. 836 emprunts ont été listés en consultant les cinq registres de la bibliothèque. *« Dans les 836 fiches, parmi Freud, Nietzsche, Eluard, Hegel, Marx, Kant, Valéry ou Lautréamont, on trouve aussi « Les Pieds nickelés ». Ces emprunts renseignent beaucoup sur l'emprunteur. »*[91] Ainsi une des préconisations d'Umberto Eco dans « De Bibliotheca »[92] quand il imagina le modèle négatif de la bibliothèque, est le conseil suivant : « On découragera le prêt ». Si les bibliothécaires avaient mis en application un tel principe, les lectures de Murakami et de G. Bataille seraient restées secrètes.

En janvier 2017, la Bibliothèque nationale de France, à l'occasion des travaux de rénovation du site Richelieu et de la salle Labrouste, a exhumé quelques cartes d'anciens lecteurs[93]. Sur ces cartes de lecteurs figurent de nombreuses données personnelles : photo, date de naissance, adresse, et même les conditions d'acquisition de la nationalité française (comme celle de Nathalie Sarraute). Le Community manager de la page Facebook de la BnF explique la diffusion de ces cartes d'illustres lecteurs car « Il s'agit ici des doubles des cartes de lecteurs, conservés par la bibliothèque. Ces doubles ayant plus de 50 ans, ils sont librement communicables à l'issue de ce délai, prévu dans le Code du Patrimoine pour la protection de la vie privée ».

Mais parfois, les bibliothécaires dans un souci d'un intérêt supérieur à celui de la protection de la vie privée, peuvent ne pas respecter (sans intention malhonnête) certaines règles. Si une bibliothèque dispose de l'identité d'un lecteur dont le comportement a été repéré comme suspect (tentative de vol, atteinte à la pudeur, etc.) a-t-elle le droit de prévenir d'autres bibliothèques contre ce lecteur en diffusant l'identité relevée sur une liste de diffusion ? Normalement la diffusion de ce signalement, qui s'accompagne d'une identité précise devrait être faite par l'intermédiaire de la police, et de façon sécurisée.

---

[89]HEURE, G. Les fiches de bibliothèque de Murakami, futur auteur de « 1Q84 » ont été dévoilées : il lisait Kessel. *Télérama* [en ligne] 4 décembre 2015. Disponible à l'adresse : https://www.telerama.fr/livre/les-fiches-de-bibliotheque-de-murakami-l-auteur-de-1q84-ont-ete-devoilees-il-lisait-kessel,135163.php

[90] BATAILLE, G. Œuvres complètes.12. Articles 2. 1950-1961. Gallimard, 1988. P. 549-621

[91] *Ibid*, p.61, note 89.

[92] ECO, Umberto. De Bibilotheca. L'Echoppe, 1986.p.18

[93]VINOGRADOFF, L. La BnF retrouve les cartes de lecteur d'André Breton, Aimé Césaire ou Hannah Arendt. *Le Monde* [en ligne].6 janvier 2017. Disponible à l'adresse : https://www.lemonde.fr/big-browser/article/2017/01/06/la-bnf-retrouve-les-cartes-de-lecteur-d-andre-breton-stefan-zweig-ou-hannah-arendt_5058720_4832693.html?fbclid=IwAR1gld1M1OsZaWSx6N1GO-mSMLu_Wm5WOdg84tHQ-uQJFeBiDJbHz5g1WHA

Si ces exemples révèlent certaines pratiques, la profession est tout de même consciente des enjeux de la protection de la vie privée et par différents projets ou prises de position, vise à tout mettre en œuvre pour assurer la protection de ce droit.

Une intégration dans les marchés publics

Les bibliothèques concluent de nombreux contrats avec des prestataires. Avant la conclusion du contrat, les professionnels peuvent donc décider de l'importance qu'ils vont donner à la protection des données de leurs usagers. Cette vigilance peut se faire avant la passation du contrat, notamment lors de la rédaction du cahier des charges dans le cadre d'un marché public, ou bien lors du choix du prestataire quand il n'y a pas de marché.

Dans le cadre du Système de Gestion de Bibliothèque Mutualisé (SGBM) à l'université de Lille, le cahier des charges contient un chapitre *Protection des données personnelles*, listant les obligations juridiques du titulaire du marché, l'engageant notamment, en qualité de sous-traitant, dès la conception des produits et services sur la protection de la confidentialité des données et sur le signalement immédiat à l'université de toute violation. L'université est quant à elle en charge d'informer les personnes concernées par les opérations de traitement au moment de la collecte des données.

Les travaux de préparation du marché SGBM ont conduit à analyser de près les données recueillies et à en encadrer la durée de conservation à deux ans à compter de la première inscription sauf cas de renouvellement demandé par l'usager à l'expiration de ses droits.

En outre, les bibliothécaires de Gironde ont mis en ligne un modèle de contrat[94] de sous-traitance pour les bibliothèques.

Un aménagement spatial

Les contraintes matérielles, d'espaces peuvent avoir un rôle à jouer en matière de protection de la vie privée. Prévoir des zones de confidentialité au moment des inscriptions, des ordinateurs qui ne sont pas visibles de tous. L'aménagement des bureaux, le positionnement des postes informatiques en libre accès doit être pris en compte par les établissements.

Dans un article publié dans la Gazette des Communes, le 9 juillet 2018 « Les bibliothécaires ne veulent pas espionner les usagers », Chloé Lailic énonce que dans la mesure du possible il est souhaitable de positionner les écrans de façon à protéger la confidentialité de la consultation des sites qui peuvent être fait par les usagers.

Il est cependant admis, de restreindre l'accès à internet pour les mineurs, et donc de mettre en œuvre un filtrage. Cependant, il est difficile pour les bibliothécaires de gérer ces filtres, car cela relève généralement du domaine de la DSI. Par ailleurs, le filtre de protection des mineurs peut refléter des biais et une réelle volonté de

[94]BIBLIO.GIRONDE. Données personnelles en bibliothèque. [en ligne].10 septembre 2018. Disponible à l'adresse : http://biblio.gironde.fr/index.php?option=com_content&view=article&id=6228:donnees-personnelles-en-bibliotheque&catid=21:juridique&Itemid=73

censure de la part de ceux qui le paramètrent. Les écrans doivent être également visibles par les professionnels, plus dans un souci de protection que de censure.

Rédiger des lignes directrices

Les bibliothécaires français pourraient s'inspirer de leurs collègues américains et rédiger des lignes directrices sur la confidentialité et le respect de la vie privée des usagers. L'exemple des *Library privacy Guidelines*[95] de l'ALA sont très complètes et adaptées selon les cas rencontrés par les bibliothèques. Il en existe ainsi pour les thématiques suivantes :

- Règles de confidentialité des bibliothèques pour les prêteurs de livres électroniques et les fournisseurs de contenu numérique
- Règles de confidentialité des bibliothèques pour l'échange de données entre des périphériques et des services en réseau
- Règles de confidentialité des bibliothèques pour les ordinateurs et réseaux à accès public
- Consignes de confidentialité des bibliothèques pour les sites Web des bibliothèques, les OPAC et les services de découverte
- Règles de confidentialité des bibliothèques pour les systèmes de gestion de bibliothèque
- Règles de confidentialité des bibliothèques pour les élèves des écoles de la maternelle à la 12e année

Ces directives ont pour objectif de fournir aux bibliothèques des informations sur les pratiques de sécurité et de gestion des données appropriées en ce qui concerne les informations personnellement identifiables de leurs usagers, ainsi que sur leurs habitudes de lecture ou leur utilisation des ressources de la bibliothèque.

Il est également préconisé que les établissements s'engagent dans un processus proactif pour informer les utilisateurs de tout changement apporté aux politiques de confidentialité de la bibliothèque. Les *Guidelines* sont illustrées par des exemples précis comme celui sur les fonctionnalités d'un outil de découverte : si celui-ci offre la possibilité de sauvegarder l'historique de leurs recherches, il devrait s'agir d'une fonctionnalité d'activation non activée par défaut.

Les bibliothécaires ont donc plusieurs leviers d'action pour protéger la vie privée de leurs usagers. Mais ces leviers ne seront activés que s'il y a une réelle volonté politique des établissements en la matière. Mais le positionnement et les initiatives de certaines bibliothèques, encore minoritaires, peuvent être la figure de proue d'un mouvement plus massif au sein de la profession.

[95] AMERICAN LIBRARY ASSOCIATION. Library Privacy Guidelines.[en ligne]. Disponible à l'adresse : http://www.ala.org/advocacy/privacy/guidelines

FORMER ET S'INFORMER

Nous verrons dans un premier temps, la nécessité de la formation en interne et dans un second temps que les bibliothèques ont un rôle à jouer dans la formation de leurs usagers en matière de protection de la vie privée.

LA FORMATION INTERNE

Selon l'enquête (analyse uniquement sur les questionnaires complets, soit 439 répondants), 34,17% des répondants déclarent qu'aucune formation en interne n'est assurée (ou en projet pour 2018/2019). Et les répondants jugent essentiel d'assurer non seulement des formations aux personnels (71,75%), mais également aux usagers (41,50%).

S'agissant de la vigilance des professionnels sur leurs propres données, selon leur âge, l'enquête révèle que les bibliothécaires y sont globalement très sensibles. Les répondants les plus âgés sont ceux qui se déclarent le moins vigilant, mais ils représentent un faible échantillon, donc les 25% se déclarant pas ou peu d'accord avec l'énoncé de la question ne sont pas forcément pertinents. Les agents de plus de 61 ans, en représentent de 3,64% de l'ensemble des répondants, ce qui peut démontrer un intérêt moindre sur la question des données personnelles. Les réponses à cette question, en fonction des âges des répondants, ne permettent donc pas de dégager une tendance très forte selon les générations.

A titre personnel, êtes-vous particulièrement vigilant sur la surveillance électronique de masse, et la protection de vos données à caractère personnel ?					
	20/30 ans 73 réponses (16,63%)	**31/40 ans** 130 réponses (30,30%)	**41/50 ans** 138 réponses (31 ;44%)	**51/ 60 ans** 79 réponses (18%)	**61 ans et plus** 16 réponses (3,64%)
1 (pas du tout d'accord)	1,37%	0,75%	2,17%	2,53%	12,5%
2	10,96%	6,77%	13,77%	6,33%	12,5%
3	30,14%	39,85%	25,36%	40,51%	18,75%
4	34,25%	27,07%	31,16%	24,05%	25%
5 (Entièrement d'accord)	23,29	25,56%	27,54%	26,58%	31,25%

Un manque de formation

Les bibliothécaires ont des obligations éthiques qui les obligent à bien comprendre comment et quand les données des utilisateurs sont saisies par les outils des bibliothèques et autres technologies Web, et comment ces informations sont compilées et partagées à un niveau supérieur. Les bibliothécaires doivent non seulement comprendre les aspects techniques des technologies, mais également les avantages liés à l'expérience utilisateur, les préoccupations en matière de confidentialité et les implications éthiques qui en résultent. Les bibliothécaires adoptent de nouveaux outils sans toujours bien comprendre leurs technologies dans le détail et l'utilisation des données qui en est faite par les éditeurs. À mesure que la technologie évolue, les bibliothécaires devraient être tenus de poursuivre leur apprentissage dans ces domaines. Ces compétences en informatique sont partiellement incorporées dans les formations initiales des personnels des bibliothèques.

L'enquête révèle une disparité entre les bibliothèques territoriales et les bibliothèques de l'enseignement supérieur en matière d'offre (ou de projet) de formation sur la protection de la vie privée. La formation pour les personnels est relativement faible, rarement externalisée (on peut supposer que cela est dû en partie pour des raisons financières), et la majorité des répondants ignorent l'offre au sein de leur établissement.

Des formations sur la protection de la vie privée des utilisateurs sont-elles proposées (ou en projet pour 2018/2019) ?		
	Bibliothèques universitaires (190 réponses ; 43,28%)	Bibliothèques territoriales (173 réponses – 39,41%)
Aux personnels	24,74%	16,76%
Aux usagers	6,32%	13,29%
Aucune formation n'est assurée en interne	27,89%	45,66%
Toutes les formations sont externalisées	2,11%	5,78%
Je ne sais pas	46,84%	34,10%

Nous avons limité les résultats de cette question, aux répondants qui ont déclaré travailler dans un service de formation, et ceux-ci sont assez édifiants (avec tout de même la limite de l'échantillonnage à savoir 22 répondants, soit 5,01% de l'ensemble des répondants.). On peut relever que 50% d'entre eux déclarent ignorer l'existence d'une offre de formation sur la protection de la vie privée. Pourtant nous verrons que l'entrée en vigueur du RGPD a été une opportunité pour plusieurs établissements de proposer des formations sur la vie privée ou les données personnelles. Nous pouvons supposer que les actions de formations ont été mises en place après la clôture de l'enquête.

Des formations sur la protection de la vie privée des utilisateurs sont-elles proposées (ou en projet pour 2018/2019) ?	
Aux personnels	13,64%
Aux usagers	4,55%
Aucune formation n'est assurée en interne	31,82%
Toutes les formations sont externalisées	0%
Je ne sais pas	50%

Le RGPD une opportunité pour la formation interne

L'entrée en vigueur du RGPD a été l'occasion pour plusieurs établissements de former en interne les agents sur les questions liées à la protection des données à caractère personnel. Certaines bibliothèques ont partagé leurs supports de formation, outils, retours d'expérience.

Plusieurs établissements ont mis à disposition de la communauté professionnelle de nombreux outils en ligne pour assurer la formation continue des bibliothécaires. Ainsi, certaines collectivités locales, comme le Département du Val d'Oise[96] ont mis à disposition des supports de présentation, explications et préconisations sur le RGPD à destination des bibliothécaires. Dans ce cas précis, on note une forte volonté de la tutelle de soutenir la bibliothèque. Les bibliothécaires de Gironde ont mis à disposition une check-list des données personnelles en bibliothèque[97] pour vérifier la conformité de son établissement avec le RGPD. Cet outil a une portée très pratique.

Les formations ayant lieu en début d'année, suite aux arrivées de nouveaux collègues dans les établissements à la faveur de mutations, de concours ou de recrutement, peut être une occasion à saisir pour former les collègues. Ainsi la BnF a instauré une formation pour tout nouvel arrivant, sur la protection des données et plus largement sur la sécurité informatique. Cette formation est assurée conjointement par le responsable du Département des systèmes d'information et la déléguée à la protection des données de l'établissement. Elle propose également des fiches pratiques et une sélection de liens vers le site de la CNIL pour l'ensemble de ses agents sur son intranet : « Comment faire un formulaire de collecte de données personnelles », « Déclarer ses fichiers », « Que faire si une personne demande à avoir accès, à rectifier, ou à supprimer ses données ? », « Que faire lors d'un contrôle de la CNIL ? »

Le SCD de l'université de Paris 1 Panthéon-Sorbonne a fait, en juillet 2018, une présentation du RGPD, lors de la journée de son réseau. Cela a été l'occasion de voir

[96] VAL D'OISE. Le RGPD : petit guide à l'usage des bibliothécaires [en ligne]. Disponible à l'adresse : http://www.valdoise.fr/2364-rgpd-et-bibliotheques.htm

[97] BIBLIO.GIRONDE. Données personnelles en bibliothèques : la check-list pour se mettre en conformité. [en ligne]. Disponible à l'adresse : http://biblio.gironde.fr/images/stories/auteur_bdp/lisa/bao_rgpd_978f0.pdf

notamment les zones de notes qui figurent dans le fichier lecteur, et que de nombreuses bibliothèques utilisent. Des exemples permettent de voir quelles notes sont correctes, celles qu'il faut corriger, et celles qui sont strictement prohibées.

La formation des bibliothécaires peut également être assurée par les DSI des établissements, notamment sur les questions liées à la sécurité numérique. Nous avons évoqué précédemment la menace de *phishing*, il est nécessaire que les DSI rappellent sans cesse et forme les personnels à ces types d'attaques de la part de pirates informatiques, pour éviter toute fuite de données des usagers.

Si des formations techniques et juridiques sont nécessaires, elles doivent également s'accompagner de formations à l'éthique et la déontologie des bibliothécaires et de procédures pour la mise en œuvre et répondre aux demandes des usagers.

L'enquête révèle que les bibliothèques ont instauré très peu de procédures internes pour répondre aux droits de leurs usagers. Selon l'enquête, les procédures en bibliothèques universitaires font grandement défaut, mais cela peut s'expliquer par des procédures existant au niveau de l'université, et non pas au niveau propre du SCD.

L'enquête ayant été menée peu de temps après l'entrée en vigueur du RGPD, de nombreux établissements n'ont sans doute pas eu le temps de rédiger des procédures.

Avez-vous une procédure pour répondre à une demande d'usager au sujet de ses données à caractère personnel		
	Bibliothèques universitaires (190 réponses ; 43,28%)	Bibliothèques territoriales (173 réponses – 39,41%)
Pour le déréférencement	8,42%	6,94%
Pour la suppression des données	14,21%	27,17%
Pour donner l'accès aux données de l'usager	10,53%	13,87%
Pour permettre à l'usager de récupérer ses données	5,79%	6,94%
Pour obtenir la liste des prêts précédents	11,05%	23,70%
Il n'existe aucune procédure	67,37%	58,96%

LA FORMATION DES USAGERS

La formation aux usagers est une des missions fondamentales des bibliothèques, de lecture publique ou universitaire. Dans un souci d'instauration de lien de confiance, mais aussi d'assurer la défense de droits fondamentaux, les bibliothèques sont nombreuses à proposer des formations (ou actions de sensibilisation) sur la protection de la vie privée à leurs usagers. On note un engagement relativement fort de la profession, et une offre variée de formations adaptées à différents types de publics.

Un engagement de la profession

Une bibliothèque qui est incapable de contrôler la façon dont sont administrées les données à caractère personnel de ses utilisateurs risque de provoquer un sentiment d'insécurité. Si l'établissement ne peut préserver l'intégrité des données confiées par les usagers cela risque de mettre en péril la confiance que ces derniers lui accordent.

L'American Library Association (ALA) fournit de nombreuses lignes directrices, des points de contrôle et des boîtes à outils à destination des personnels de bibliothèque. Ces ressources sont axées sur l'atténuation menaces à la vie privée tout en répondant aux besoins des bibliothèques de collecter les données des utilisateurs et fournir des services personnalisés. L'accent est mis sur l'espace physique de la bibliothèque et les offres de ressources, et moins sur un aspect plus large de la protection de la vie privée de ses usagers. A l'instar des bibliothèques publiques de New-York[98], engagées dès 2012 dans la formation des professionnels pour répondre aux demandes des usagers sur la confidentialité de leurs données à caractère personnel grâce au *Data Privacy Project*, il existe plusieurs initiatives au sein des bibliothèques françaises.

On peut ainsi signaler le mouvement des *CryptoParty*, né en Australie dans les années 90, qui s'est véritablement installé en France à partir de 2013 (dans le sillage des révélations de l'affaire Snowden). Les « CryptoParty » (aussi dénommés Café Vie privée) se sont développés dans plusieurs grandes villes françaises : Lyon, Rennes, Marseille, Nantes, Lille, et ont pour objectif d'initier toute personne à la cryptographie et au chiffrement, de sensibiliser les personnes aux atouts des logiciels libres, de présenter les fournisseurs d'accès internet associatifs etc. Des ateliers en bibliothèques sont organisés, du type « Protection de ses données et de sa vie privée en ligne ? : Échanges autour des enjeux de la protection de la vie privée, des bonnes pratiques d'hygiène numérique, et des outils et des alternatives libres à notre disposition ».

Dès 2015, Thomas Fourmeux mettait en ligne un « Kit pour protéger ses données personnelles en bibliothèques », et recommandait notamment l'utilisation d'un moteur de recherche comme *Qwant* et d'opter pour *Framadrive, Owncloud* pour stocker ses fichiers et photos plutôt que le *GoogleDrive.*

A titre d'exemple, on peut signaler le dossier mis en place par la médiathèque Georges Wolinski de Noisy-Le-Grand[99] et intitulé « Vous voulez protéger vos

[98] https://dataprivacyproject.org/

[99]MEDIATHEQUE GEORGES WOLINSKI. Vous voulez protéger vos données personnelles, on peut vous y aider. [en ligne] Disponible à l'adresse : http://mediathequegeorgeswolinski.fr/entre-nous/le-blog-de-l-atelier/573-vous-voulez-proteger-vos-donnees-personnelles-on-peut-vous-y-aider#privacy

données personnelles, on peut vous y aider ! ». Dans la présentation du dossier en ligne, les bibliothécaires de Noisy-Le-Grand prennent clairement position en annonçant : « Nous pensons qu'il est important de pouvoir trouver de l'information et de choisir par soi-même plutôt que de se laisser enfermer dans des bulles filtrantes informationnelles conditionnées par les algorithmes des plateformes et des services en ligne. ». Les bulles filtrantes désignent le filtrage de l'information qui parvient à l'internaute par différents filtres ; et l'état d'isolement intellectuel et culturel dans lequel il se retrouve suite à la personnalisation (faite à son insu) de ses recherches sur le web. La formation des étudiants de licence de Rennes 1 et Rennes 2 délivrées par les bibliothécaires incluent systématiquement cette notion de bulles de filtre et la recherche sur des moteurs de recherche qui ne favorisent pas ces *filter bubbles*.

Les bibliothèques doivent donc intégrer la protection de la vie privée en ligne dans la formation des usagers, tout en s'adaptant aux besoins de leurs publics.

Des formations pour le grand public

Plusieurs bibliothèques de lecture publique proposent des formations sur l'identité numérique et sur la sécurisation des données personnelles. A titre d'exemple, on peut citer le projet « Les voyageurs du numérique » [100]sous la houlette de *Bibliothèques sans frontières*, qui propose des formations et ateliers pour le grand public (mais également pour les professionnels) autour des questions liées au numérique.

La sensibilisation, à la protection des données personnelles, se traduit également dans le milieu scolaire grâce notamment au CLEMI (Centre de liaison de l'enseignement et des médias d'information) et au DANE (Délégation Académique au Numérique Educatif). Afin d'attirer un jeune public, le vecteur des *Escape games*, est un moyen sérieux de former et informer la nouvelle génération. Ainsi, on peut signaler, dans l'académie de Besançon, la création du jeu « Connais-moi, échappe-toi », un jeu d'évasion autour des données personnelles[101]

Des formations pour la communauté universitaire

La communauté universitaire est depuis plusieurs années confrontée aux évolutions du numérique, non seulement dans la pédagogie, les ressources. Aujourd'hui l'accent est mis sur les données de la recherche, et bien évidemment sur les données personnelles de chaque membre de la communauté (non seulement dans sa sphère éducative, mais aussi dans sa sphère privée et qui sera ensuite transposée dans la sphère professionnelle).

Le 30 janvier 2019, la CNIL a signé un partenariat[102] avec la Conférence des présidents d'université. Les partenaires s'engagent à :

[100]BIBLIOTHEQUES SANS FRONTIERES. Voyageurs du numérique. [en ligne] . Disponible à l'adresse : https://voyageursdunumerique.fr/le-projet/

[101] https://dane.ac-besancon.fr/connais-moi-echappe-toi-evasion/

[102] CNIL. La CNIL et la Conférence des Présidents d'Université (CPU) renouvellent leur convention de partenariat. [en ligne]. 30 janvier 2019. Disponible à l'adresse https://www.cnil.fr/fr/la-cnil-et-la-conference-des-presidents-duniversite-cpu-renouvellent-leur-convention-de-partenariat

- Organiser des actions de sensibilisation auprès des universités sur les principes de protection des données personnelles et sur la mise en conformité au RGPD
- Encourager dans les cursus d'enseignement supérieur les formations à la protection des données
- Soutenir les travaux de recherche sur la protection des données

En bibliothèques universitaires, les attentes et besoins sont très différents entre un L1, des doctorants et la communauté des enseignants-chercheurs. Les formations doivent donc être de différents niveaux, d'une découverte à une formation experte. Pour les étudiants de licence, les formations peuvent porter sur l'e-reputation ou le contrôle des données personnelles. A partir du niveau Master 2, des formations pourront porter sur l'intégration de la protection des données personnelles des patients ou de personnes interrogées lors d'une enquête réalisée dans le cadre de travaux universitaires.

En outre, le soutien à la recherche sur les données personnelles est un engagement fort de la part de plusieurs institutions. Ainsi la CNIL et l'INRIA ont créé en 2016 un prix européen visant à encourager la recherche scientifique sur la protection de la vie privée. En 2019, le prix a été décerné à Pierre Laperdrix pour son article « *Beauty and the beast : diverting modern web browsers to build unique browser fingerprints*[103]» sur les empreintes de navigateurs laissées sur le web.

Ainsi quelques jours après l'entrée en vigueur du RGPD, le SCD de l'université de Limoges en partenariat avec l'université de Bordeaux a organisé une formation intitulée « Protection des données personnelles : quelles implications pour la recherche »[104] à destination des chercheurs.

Sensibiliser les étudiants

Les étudiants de 2018, faisant partie de la génération Z, les natifs numériques, ont toujours connu internet, les réseaux sociaux. On les considère généralement comme très à l'aise avec le numérique. Ils sont cependant plus consommateurs que créateurs du numérique.

Les formations peuvent être de plusieurs niveaux. Un premier niveau d'information générale sur les données collectées, et conservées par l'université, et les droits des usagers ; peut permettre de sensibiliser les étudiants à la protection de leurs données personnelles.

Les étudiants peuvent également être acteurs de leur propre formation. Ainsi le hall de la bibliothèque de l'Insa de Lyon a accueilli « Privé de vie privée »[105], une exposition organisée par les étudiants sur les conséquences d'un « *like* » sur les données personnelles.

Les bibliothèques peuvent aussi informer les étudiants sur les nouvelles pratiques que sont les *learning analytics*. Pour définir des profils pédagogiques, des

[103] LAPERDRIX, P, RUDAMETKIN, W, BAUDRY, B. Beauty and the Beast: Diverting modern web browsers to build unique browser fingerprints. *37th IEEE Symposium on Security and Privacy (S&P 2016)*, May 2016, San Jose, United States. [en ligne]. Disponible à l'adresse : http://www.ieee-security.org/TC/SP2016/〉. 〈hal-01285470v2〉

[104]UNIVERSITE DE LIMOGES. SCD. La protection des données personnelles : quelles implications pour la recherche ? [en ligne]. Disponible à l'adresse : https://www.unilim.fr/scd/2018/05/04/la-protection-des-donnees-personnelles-quelles-implications-pour-la-recherche/

[105] http://scd.docinsa.insa-lyon.fr/exposition-prive-de-vie-privee

difficultés d'apprentissage, les équipes pédagogiques peuvent s'appuyer sur l'analyse systématique des traces que les étudiants peuvent laisser sur les réseaux de l'université. Certaines traces numériques peuvent être complétées par des données physiques comme le rythme cardiaque par exemple. Il semble nécessaire que les étudiants soient informés des usages fait par leurs établissements grâce à ces nouveaux outils. L'analyse des données récoltées permettra alors de réorienter l'étudiant vers des activités dont le contenu et le niveau de difficulté sont censés correspondre à ses besoins, son niveau et à ses capacités. L'enseignant peut s'appuyer sur ces données pour adapter son enseignement. Ces nouveaux services collectent donc de façon massive des données personnelles. On peut donc mettre en place une analyse prédictive de l'apprentissage, et des compétences qui seront acquises. Le caractère prédictif de tels outils n'est pas sans poser question d'un point de vue éthique il faut donc que le monde universitaire soit particulièrement vigilant.

Ainsi comme le rappelle le rapport de Terra Nova : « *La question de l'usage et du contrôle des données issues des parcours des élèves apparaît comme primordiale, à la fois pour garantir le respect de l'anonymat et pour faciliter les progrès des dispositifs mis en place. »*[106]

A la fin de leur parcours universitaire et avant l'intégration sur le marché du travail, les étudiants peuvent se voir proposer des formations notamment sur leur réputation numérique[107], et ce dans un souci de se positionner face à de futurs recruteurs.

Un accompagnement spécifique pour les chercheurs

Les bibliothèques universitaires ont une mission toute particulière auprès des chercheurs et enseignants chercheurs. Les bibliothèques essayent de renouer un lien avec le monde de la recherche et notamment par le biais des questions liées au numérique.

Via les notices d'autorités, les bibliothèques gèrent déjà des données personnelles des chercheurs, et participent donc à une meilleure identité numérique des chercheurs. Valoriser la présence numérique des chercheurs, mettre en avant leurs publications en ligne, favoriser les archives ouvertes, auront un impact positif sur les bibliothèques et permettront de les rendre plus visibles et de faire connaître les compétences techniques de ses agents.

Plusieurs universités proposent des formations sur ce sujet, notamment aux jeunes chercheurs que sont les doctorants. Les intitulés varient mais les objectifs sont identiques. Parmi les objectifs, on peut noter celui de contrôler sa présence en ligne, tout en faisant attention à ses données.

La formation sur l'identité numérique du chercheur[108] est une demande forte de la part de la communauté. Le bibliothécaire universitaire apporte non seulement son aide aux chercheurs pour leurs recherches et publications, mais aussi en tant que

[106] AGACINSKI, D ; BRUN, F, ISART, C, JAMES, M. L'école sous algorithmes. Terra Nova, [en ligne. 10 mars 2016. Disponible à l'adresse : http://tnova.fr/etudes/l-ecole-sous-algorithmes

[107]https://bu.univ-lehavre.fr/former-se-former/notre-offre-de-formations/dans-les-cursus/article/integration-professionnelle-et-e-reputation

[108]https://bibli.ec-lyon.fr/formations/supports-formation/formations-doctorants-2018-identite-numerique-du-chercheur

citoyen numérique.[109] L'identité numérique peut relever de la sphère professionnelle comme de la sphère personnelle.

Les enseignants-chercheurs sont également des utilisateurs de données personnelles, dans le cadre de leurs travaux. La question des données de la recherche impose aux chercheurs de maitriser la récolte, la gestion et la finalité des données personnelles qu'ils pourraient avoir à exploiter dans le cadre de leurs travaux. Ainsi quelques jours après l'entrée en vigueur du RGPD, le SCD de l'université de Limoges en partenariat avec l'université de Bordeaux a organisé une formation intitulée « Protection des données personnelles : quelles implications pour la recherche »[110] à destination des chercheurs.

Les fiches pratiques rédigées en février 2019 par l'université Paris Lumières, Université Paris Nanterre et l'Université Paris 8[111] répondent aux besoins spécifiques des chercheurs notamment sur le choix de l'anonymisation des données, ou encore en cas de projet de recherche conjointe multipartenaires la nécessité de rédiger une convention prévoyant les responsabilités de chacun en matière de traitement des données personnelles.

On peut signaler la formation qui a eu lieu en novembre 2018 à la bibliothèque de Chevreul de l'université de Lyon 2 : « Recherche SHS : et si on faisait attention aux données personnelles ? »[112]. La formation s'est déroulée en deux temps : une présentation théorique, avec des retours d'expérience et ensuite des ateliers pour répondre aux questions individuelles en lien avec les recherches des usagers.

COMMUNIQUER, UNE NECESSITE

Comment les bibliothèques peuvent-elles témoigner auprès de leurs équipes mais également auprès de leurs usagers des efforts consentis pour protéger leurs données ?

Selon l'enquête, on peut noter un défaut flagrant de communication sur le sujet (21,82% des répondants, déclarent que leur établissement n'assure aucune communication auprès de ses usagers sur la question de la protection des données à caractère personnel). Quand les structures communiquent, les moyens et les usages diffèrent selon leurs types. En effet, les établissements relevant du Ministère de l'Enseignement Supérieur et de la Recherche, communiquent en grande majorité sur la protection des données à caractère personnelle de leurs usagers. Les canaux de diffusion sont multiples et parfois redondant. Les supports de communication qui arrivent en tête sont : le site internet de l'établissement (47,89%), les mails, les affiches etc.
S'agissant des bibliothèques territoriales, le site web est un support de communication selon 36,42% des répondants, contre 57,80% qui déclarent utiliser

[109]URFISTINFO. L'identité numérique du chercheur : quel accompagnement ? [en ligne]. 24 août 2018. Disponible à l'adresse : https://urfistinfo.hypotheses.org/3219

[110]https://www.unilim.fr/scd/2018/05/04/la-protection-des-donnees-personnelles-quelles-implications-pour-la-recherche/

[111] http://www.u-plum.fr/app/webroot/upload/files/Janvier%202019/Guide%20RGPD%202019%20web.pdf

[112] https://www.univ-lyon2.fr/bibliotheques/journee-donnees-de-la-recherche-le-26-novembre-782300.kjsp

d'autres canaux (lors de l'inscription, à la demande des usagers, dans la Charte informatique etc.).

Communication interne et externe

Il est primordial que les établissements communiquent leur politique, les personnes ressources, les données concernées, leurs procédures dans un premier temps à l'ensemble des collègues et dans un second temps auprès de leurs usagers. Si possible, il est souhaitable de rédiger un plan de communication sur les changements (et ce qui reste inchangé) impliqués par le RGPD au sein de l'établissement. Il faut également veiller au niveau de l'information diffusée, si elle peut être qualifiée d'experte pour les professionnels, il faut veiller à ce qu'elle soit compréhensible par l'usager.

En effet, si les agents ne sont pas bien informés, ils ne peuvent répondre de façon satisfaisante à leurs usagers. La communication interne peut se faire selon les moyens traditionnels : réunion, intranet, mail, support ad hoc. La BnF, peu de temps après l'entrée en vigueur du RGPD, a organisé un « Midi de l'Info » pour l'ensemble de ses agents. Il s'agissait d'une présentation générale sur les rôles du DPD, de la CNIL et du RSSI.

Une fois la communication interne assurée, les bibliothèques pourront mettre en place la communication externe pour les usagers. Parmi les commentaires libres des répondants à l'enquête, il apparait que la communication de la bibliothèque sur les données personnelles est conditionnée par celle de la tutelle (Collectivité territoriale, ou université). La bibliothèque, en conformité avec sa tutelle, a tout intérêt à faire une communication ciblée auprès de ses usagers avec notamment des exemples précis des données récoltées (prêt de document par exemple), et leur usages et durée de conservation par l'établissement et ce dans un souci de transparence et donc de confiance.

Les canaux de communication

Les canaux de communication sont multiples et variables selon le type et la taille de la bibliothèque. Si le canal numérique est important, il ne faut pas négliger la communication dans les espaces de la bibliothèque et celle qui peut être faite en présentiel avec l'usager.

De nombreuses bibliothèques communiquent sur leur site internet leur politique de protection des données personnelles de leurs usagers. Lorsque l'information est diffusée sur les sites internet des différents établissements, on note des degrés variables du niveau d'information fournie et des modalités de contact très variables. Certains sites communiquent sous une rubrique « mentions légales », plus ou moins développée, et d'autres sous une rubrique plus spécifique « données personnelles ». Le contact pour que l'usager puisse exercer ses droits, peut être une adresse postale de la bibliothèque (comme à la bibliothèque municipale de Rouen[113]) ou bien de la mairie (comme la bibliothèque de Montreuil[114]). On peut également trouver des

[113] http://rnbi.rouen.fr/fr/page-descriptive/mentions-l%C3%A9gales

[114] http://www.bibliotheque-montreuil.fr/mentions-legales/

adresses mails comme celle générique de l'établissement (comme à la bibliothèque municipale de Grenoble[115]) ou bien l'adresse mail du DPD.
S'agissant des bibliothèques universitaires, les sites internet des bibliothèques renvoient vers la page de l'université, et le DPD de celle-ci. Il peut s'agir d'une adresse générique (comme c'est le cas à l'Enssib[116]), ou bien personnalisée (c'est le cas à l'université Panthéon-Assas[117]).
S'agissant des bibliothèques interuniversitaires (BIU Cujas[118], BIS[119], BIUM[120],), on peut observer un vrai manque d'information et de contact pour l'exercice des droits de leurs usagers.
Sur le site de la BNU, il existe une rubrique très significative et clairement intitulée « mes données personnelles à la BNU [121]», c'est un signe fort de transparence pour l'usager.

Certains établissements, comme le SCD de Nice précisent le cas particulier de certains éditeurs de bases de données : « Nota bene : Certains éditeurs de ressources électroniques demandent la création de compte personnel pour accéder à leur ressource et récupèrent ainsi vos données personnelles. Ils sont également soumis aux lois et règlements en vigueur. »[122]

Il ressort de l'enquête, que la communication orale est un vecteur très fort. Mais il ne suffit pas. Les établissements pourront multiplier les canaux de communication auprès de leurs usagers : mail, site internet, affichage dans les espaces numériques, fond d'écran, Charte informatique, formulaires d'inscription ; newsletter, ateliers, Festival des libertés numériques[123].

Des expositions peuvent également avoir un impact immédiat auprès des usagers. Ainsi, la bibliothèque de l'Ecole polytechnique de Lausanne a organisé au Rolex Center une exposition intitulée « Data Detox, reprends le contrôle de tes données personnelles »[124]. L'exposition est interactive, et divisée en quatre thématiques (Géolocalisation, Navigateurs, Réseaux Sociaux et Solutions alternatives). Tout au long du parcours, les visiteurs peuvent faire des exercices sur les tablettes mises à disposition ou directement sur leurs appareils connectés.

Informer les usagers de leurs droits

Le droit à l'information est un droit qui existait avant l'entrée en vigueur du RGPD. La loi de 1978 et la directive de 1995 consacraient déjà ce droit, inspiré de la crainte d'une surveillance réalisée à l'insu des personnes. Le droit à l'information, c'est en fait une garantie de transparence pour l'usager. C'est permettre aux

[115] https://www.bm-grenoble.fr/1478-mentions-legales.htm

[116] https://www.enssib.fr/mentions-legales

[117] https://www.u-paris2.fr/fr/mentions-legales

[118] http://biu-cujas.univ-paris1.fr/fr/credits

[119] http://www.bibliotheque.sorbonne.fr/biu/spip.php?rubrique27

[120] http://www.biusante.parisdescartes.fr/mentions.php

[121] http://www.bnu.fr/mes-donnees-personnelles-la-bnu

[122] https://bu.univ-cotedazur.fr/fr/mentions-legales

[123] Verbatim de l'enquête en annexe.

[124] https://library.epfl.ch/wp-content/uploads/2018/09/Data_Detox_brochure_28pages_final.pdf

personnes d'être informées de ce que l'on fait de leurs données, comment, pourquoi, qui y a accès, où sont-elles traitées, par qui, etc. Et ce doit être fait de manière concise, aisément accessible et facile à comprendre.

Les autres droits traditionnels sont, par exemple, le droit d'accès aux données. C'est la possibilité pour les personnes de demander à avoir accès aux données les concernant sur tous les traitements qui sont installés dans un organisme. C'est aussi la possibilité de faire rectifier des données erronées ou de s'opposer au traitement de leurs données. Et sous certaines conditions, de solliciter l'effacement.

Le droit d'opposition

Le droit d'opposition permet, lors de la collecte ou de la diffusion de données, de refuser que ses données soient prises en compte. La demande se fait au responsable du traitement. Si l'usager fait valoir ce droit d'opposition, soit l'établissement n'aura pas le droit de collecter ses données, soit elle devra arrêter de les diffuser.

Le droit d'opposition est un droit très intéressant car il permet de se rétracter. L'usager peut, dans un premier temps, autoriser la collecte de ses données ou leur diffusion. Si ultérieurement il souhaite que ses données soient retirées, le droit d'opposition lui permettra de faire que ses données soient retirées du site. De la même façon, si le responsable du traitement, le service refuse de retirer ses données ou laisse la demande sans réponse, il suffira de saisir la CNIL et les tribunaux afin que les données soient retirées. Le droit d'opposition n'est pas universel et par exemple ne s'applique pas à certains services (police, sécurité sociale, administration fiscale)[125].

Les limites au droit d'accès

Le responsable du fichier peut refuser la demande d'accès, mais il doit motiver sa décision et informer l'usager des voies et délais de recours permettant de contester ce refus.

Le responsable du fichier peut ne pas répondre aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique.

Les fiches pratiques de la BnF indiquent que si un agent reçoit une demande d'accès ou d'opposition (par écrit ou sur place), il doit la transmettre dans les plus brefs délais au délégué à la protection des données de l'établissement. Ce dernier se chargera de l'instruction et de la réponse à la demande, en lien avec les services ayant recueilli les données personnelles concernées.

A titre d'exemple, le délégué à la protection des données de l'Université de Lille a demandé aux responsables de services aux publics des cinq bibliothèques du SCD l'instauration d'une procédure particulière pour les lecteurs extérieurs :

- L'ajout dans les informations légales DPD sur le site de l'Université d'une rubrique spéciale « lecteurs extérieurs ». Juste après son inscription auprès des personnels dans chaque bibliothèque, tout lecteur extérieur individuel trouvera dans le message de confirmation qui lui est adressé par mél non

[125] FRANCE. ASSEMBLEE NATIONALE. Étude d'impact - N° 490 – Projet de loi relatif à la protection des données personnelles [en ligne] disponible à l'adresse : http://www.assemblee-nationale.fr/15/projets/pl0490-ei.asp

seulement un lien cliquable lui permettant de récupérer son identifiant en indiquant son accord pour l'utilisation de son adresse mél dans les limites indiquées.

La CNIL est chargée de gérer les plaintes et réclamations des usagers, pour non-respect du RGPD. En 2018, elle a reçu près de 11.000 réclamations (en augmentation de 30% par rapport à 2017)[126].

La formation initiale et continue des professionnels sur la réglementation sur la protection de la vie privée, et plus particulièrement sur les données à caractère personnelle, est une nécessité absolue. Celle-ci devra être accompagnée de procédures internes, qui seront ensuite réutilisables pour former et informer les usagers de leurs droits et obligations (notamment pour les chercheurs qui pourront collecter des données à caractère personnel dans le cadre de leurs travaux).
Nous pouvons d'ores et déjà saluer les initiatives (sous des formes très variées) de plusieurs établissements et collègues, et la réelle volonté de partager les supports avec le plus grand nombre.

[126] https://www.data.gouv.fr/fr/datasets/plaintes-recues-par-la-cnil/

CONCLUSION

Les bibliothécaires français, agents du service public, ardents défenseurs des principes fondamentaux du droit et protecteurs des valeurs républicaines, sont des remparts de protection de la vie privée de leurs usagers. Ils ne se limitent pas à une simple application du droit, ils défendent des valeurs via les prises de positions de leurs associations professionnelles mais également par les politiques qu'ils peuvent mettre en place au sein de leurs établissements et enfin par leurs actions de formations et d'information envers leurs collègues et au final leurs lecteurs.

Comment se positionner entre différentes valeurs, différents droits, selon le contexte notamment politique, questionne la profession et les débats en son sein y sont parfois vifs. Les professionnels continueront sans doute de débattre entre vigilance et aveuglement volontaire, mais ces deux notions s'appuient sur les meilleures intentions du monde et sur des droits fondamentaux équivalents. La difficulté reste à faire concilier ces droits.

La protection de la vie privée est sans cesse en mouvement, compte tenu des évolutions technologiques liées au numérique, des évolutions sociétales, politiques ou même économiques. Les bibliothécaires doivent donc être attentifs aux débats sociétaux autour de la vie privée s'adapter, se remettre parfois en question.

De nombreux collègues et établissements initient de nombreux projets pour sensibiliser leurs lecteurs à toutes ces questions, et les former afin de les rendre autonomes et conscients des usages qui peuvent être faits de leurs données à caractère personnel. Nous gageons que ces initiatives seront de plus en plus nombreuses dans les bibliothèques et donc les citoyens de plus en plus conscients de dérives possibles et donc acteurs pour contrer ces dernières.

A l'heure du *Big data,* de l'émergence de la question de la marchandisation des données personnelles, de l'importance des données de la recherche dans le monde universitaire, du poids économique considérable des *Gafam,* de la puissance des réseaux sociaux lors d'évènement politiques majeurs (comme lors de la dernière élection présidentielle américaine), et afin de se prémunir de toutes les dérives possibles des usages de données à caractère personnelles et outils numériques, les professionnels de l'information doivent se saisir de ces questions pour maintenir, et même renforcer la confiance qu'ont leurs usagers dans leurs institutions. La protection de la vie privée, est une des assurances de la démocratie.

SOURCES

Entretien le 5 décembre 2018 avec Vincent Boulet, Bibliothèque nationale de France, Département des Métadonnées / Chef du service des Référentiels

Entretien le 3 décembre 2018 avec Estelle Graff, Bibliothèque nationale de France, Service juridique, Déléguée à la protection des données

Entretien le 7 novembre 2018avec Jérôme Kalfon, Consortium Couperin, Département des négociations documentaires

Echanges de courriels avec Corinne de Munain, SCD Université de Lille Responsable des services aux publics

Echanges de courriels avec Claire Nguyen, Université Paris Dauphine, Bibliothèque, Responsable du service de la politique documentaire

Enquête diffusée, entre le 19 juillet 2018 et le 21 octobre 2018 via les outils et listes de diffusion suivantes : ADBU-Forum, Agorabib, Cryptobib, Juriconnexion, Parcours Numériques, Comptes personnels Twitter et Facebook. Le questionnaire a été conçu avec l'outil Limesurvey, et les données ont été exploitées à partir du même outil.

BIBLIOGRAPHIE

Tous les liens ont été vérifiés le 26 février 2019

TEXTES JURIDIQUES ET RAPPORTS OFFICIELS NATIONAUX

FRANCE. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. *Journal officiel de la République française*. [en ligne]. Disponible à l'adresse : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460

FRANCE. Loi n° 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires. *Journal officiel de la République française*. [en ligne].Disponible à l'adresse : https://www.legifrance.gouv.fr/eli/loi/2016/4/20/2016-483/jo/texte

FRANCE. Loi n° 2018 493 du 20 juin 2018 relative à la protection des données personnelles. *Journal officiel de la République française*. [en ligne]. Disponible à l'adresse : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037085952&dateTexte=&categorieLien=id

FRANCE. ASSEMBLEE NATIONALE. *Etude d'impact : projet de loi relatif à la protection des données personnelles, N°490*. [en ligne]. 12 décembre 2017. Disponible à l'adresse : http://www.assemblee-nationale.fr/15/projets/pl0490-ei.asp

FRANCE. CONSEIL D'ETAT. *Etude annuelle du Conseil d'Etat, 2014 : Numérique et droits fondamentaux*. La Documentation française, 2014. Disponible à l'adresse : https://www.ladocumentationfrancaise.fr/rapports-publics/144000541-etude-annuelle-2014-du-conseil-d-etat-le-numerique-et-les-droits-fondamentaux

FRANCE. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES. *Bibliothèques, médiathèques Norme simplifiée NS-009*. [en ligne]. Disponible à l'adresse : https://www.cnil.fr/fr/declaration/ns-009-bibliotheques-mediatheques?tx_oxcscnildeclaration_pi1[sauid]=0&tx_oxcscnildeclaration_pi1[tuid]=0&cHash=0b8462991cfd6313a91944d43bc7abfd

FRANCE. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES. Délibération N°1999-027 concernant les traitements automatisés d'informations nominatives relatifs à la gestion des prêts de livres, de supports audio-visuel et d'œuvres artistiques et à la gestion des consultations de documents d'archives publiques. *Journal officiel de la République française*. [en ligne]. 28 mai 1999, page 07890. Disponible à l'adresse : https://www.legifrance.gouv.fr/jo_pdf.do?numJO=0&dateJO=19990528&numTexte=&pageDebut=07890&pageFin=07890

FRANCE. SENAT. *Protection des données personnelles.* [en ligne]. 13 décembre 2017. Disponible à l'adresse : http://www.senat.fr/dossier-legislatif/pjl17-296.html

TEXTES JURIDIQUES INTERNATIONAUX

CONSEIL DE L'EUROPE. *Convention de sauvegarde des droits de l'Homme et des libertés fondamentales*. Disponible à l'adresse : https://www.echr.coe.int/Documents/Convention_FRA.pdf

UNION EUROPEENNE. Directive (UE) 95/46/CE du Parlement européen et du Conseil, 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. *Journal officiel des Communautés européennes* [en ligne]. 23 novembre 1995. Disponible à l'adresse : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31995L0046&from=FR

UNION EUROPEENNE. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE. *Journal officiel de l'Union européenne* [en ligne]. 4 mai 2016. Disponible à l'adresse : https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32016R0679

UNION EUROPEENNE. Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977. *Journal officiel de l'Union européenne* [en ligne]. 4 mai 2016.. Disponible à l'adresse : https://eur-lex.europa.eu/eli/dir/2016/680/oj

DEONTOLOGIE ET ETHIQUE

ASSOCIATION DES BIBLIOTHECAIRES DE FRANCE. *Charte du droit fondamental des citoyens à accéder à l'information et aux savoirs par les bibliothèques*. Association des Bibliothécaires de France [en ligne]. Disponible à l'adresse : http://www.abf.asso.fr/6/46/537/ABF/charte-du-droit-fondamental-des-citoyens-a-acceder-a-l-information-et-aux-savoirs-par-les-bibliotheques

CLEFF LE DIVELLEC, Sylvia. « La Responsabilité juridique des professionnels de l'information et de la documentation et les codes de déontologie », *Bulletin des bibliothèques de France* [en ligne]. Juillet 2007. Disponible à l'adresse : http://bbf.enssib.fr/consulter/bbf-2007-04-0102-013

FOURMEUX, Thomas. *Petit guide à destination des bibliothécaires peu respectueux des droits des usagers*. Biblio Numericus [en ligne] 4 juin 2018. Disponible à l'adresse : https://biblionumericus.fr/2018/06/04/petit-guide-a-destination-des-bibliothecaires-peu-respectueux-des-droits-des-usagers

GARDÈRE, Elizabeth et LE MOËNNE, Christian. *Organisations digitales : individus, santé, déontologie en contexte numérique*. Paris : L'Harmattan, 2015.

HAGÈGE, Claude, 2015. *L'éthique de l'Internet face au nouveau monde numérique : mais qui garde les gardes ? essai*. Paris : L'Harmattan.

HAMET, Joanne, MICHEL,Sylvie, « Les questionnements éthiques en systèmes d'information », *Revue française de gestion*, 2018/2 (N° 271), p. 99-129.

IFLA. *Code d'éthique de l'IFLA pour les bibliothécaires et autres profesionnel(le)s de l'information*. [en ligne] 27 décembre 2016. Disponible à l'adresse : https://www.ifla.org/files/assets/faife/codesofethics/frenchcodeofethicsfull.pdf

LAILIC, Chloé. « Devenir bibliothécaire, devenir militante ? », *Bibliothèque(s), Revue de l'Association des bibliothécaires de France*, juin 2018. P. 150-151

MARCUZZI, Anna. « Militant de la liberté ou sentinelle du pacte républicain ? », *Bibliothèque(s), Revue de l'Association des bibliothécaires de France*, juin 2018. P. 151-152

OURY, Antoine. « Un collège de déontologie au Ministère de la Culture », *Actualitté* [en ligne]. 26 avril 2018. Disponible à l'adresse : https://www.actualitte.com/article/monde-edition/un-college-de-deontologie-au-ministere-de-la-culture/88584

PAVLIDÈS, Christophe. « La Déontologie et les bibliothécaires », *Bulletin des bibliothèques de France* [en ligne]. Janvier 2000. Disponible à l'adresse : http://bbf.enssib.fr/consulter/bbf-2000-04-0111-002

TEXIER, Bruno. « Une charte de déontologie pour les DPO », *Archimag* [en ligne]. 30 avril 2018. Disponible à l'adresse : http://www.archimag.com/vie-numerique/2018/04/30/charte-d%C3%A9ontologie-pour-dpo

DONNEES PERSONNELLES

ACCART, Jean-Philippe et RIVIER, Alexis. *Mémento de l'information numérique*. Paris : Éd. du Cercle de la librairie, 2012. Bibliothèques

BENSOUSSAN, Alain, AVIGNON, Céline, BENSOUSSAN-BRULÉ, Virginie, TORRES, Chloé et FALQUE-PIERROTIN, Isabelle. *Règlement européen sur la protection des données : textes, commentaires et orientations pratiques*. Bruxelles : Larcier. Lexing-New Technologies & Law, 2016.

BERGUIG, Matthieu, COUPEZ, François. « Faut-il réellement craindre l'Open data pour la protection de nos données personnelles ? », *Legicom*, 8 mars 2016. n° 56, p. 15-24.

BOURGEOIS, Matthieu, BOUNEDJOUM, Amira, LEPAGE, Agathe et SOUVIRA, Anne. *Droit de la donnée : principes théoriques et approche pratique*. Paris : LexisNexis. Droit & professionnels, 2017.

CALIMAQ. *Données personnelles et vie privée : ce qui va changer avec le RGPD* (support d'intervention et vidéo). S.I.Lex [en ligne]. 29 mai 2018. Disponible à l'adresse : https://scinfolex.com/2018/05/29/donnees-personnelles-et-vie-privee-ce-qui-va-changer-avec-le-rgpd-support-dintervention-et-video

CHATILLON, Georges. *Les données personnelles : enjeux juridiques et perspectives.* Disponible à l'adresse : https://www.pantheonsorbonne.fr/diplomes/master-droit-du-numerique/bibliotheque-numerique-du-droit-de-ladministration-electronique/droit/protection-des-donnees/les-donnees-personnelles-enjeux-juridiques-et-perspectives-rapport-de-georges-chatillon

ERTZSCHEID, Olivier. *Qu'est-ce que l'identité numérique ? : Enjeux, outils, méthodologies* [en ligne]. Marseille : OpenEdition Press, 2013. Encyclopédie numérique. Disponible à l'adresse : http://books.openedition.org/oep/332

FAGOT, Vincent. « Protection des données : la France intègre enfin les dispositions européennes », *Le Monde.fr* [en ligne]. 14 mai 2018. Disponible à l'adresse : http://www.lemonde.fr/politique/article/2018/05/14/protection-des-donnees-la-france-integre-enfin-les-dispositions-europeennes_5298908_823448.html

FAUCHOUX, Vincent, DEPREZ, Pierre, DUMONT, Frédéric et BRUGUIÈRE, Jean-Michel. *Le droit de l'Internet*. 3e édition. Paris : LexisNexis, 2017. Droit & professionnels.

FAUVARQUE-COSSON, Bénédicte, MAXWELL, Winston. « Protection des données personnelles », Recueil Dalloz, 24 mai. 2018.p.1033

FRANCE. ETALAB.*Vade-mecum sur l'ouverture et le partage des données publiques* [en ligne]. 2013. Disponible à l'adresse : http://www.enssib.fr/bibliotheque-numerique/documents/61618-vade-mecum-sur-l-ouverture-et-le-partage-des-donnees-publiques.pdf

GALLIGO, Dinah. « Big data, open data, protection des données personnelles : où en sont la science et l'utilisation des données ? », *Prospectibles* [en ligne]. 12 février 2018. Disponible à l'adresse : http://blogs.sciences-po.fr/prospectibles/2018/02/12/big-data-open-data-protection-des-donnees-personnelles-ou-en-sont-la-science-et-lutilisation-des-donnees

LOIRE, Marion. « Identification, identifiant, identité… individu », *Bulletin des bibliothèques de France* [en ligne]. Janvier 2009. Disponible à l'adresse : http://bbf.enssib.fr/consulter/bbf-2009-03-0095-017

MATTATIA, Fabrice, 2018. *RGPD et droit des données personnelles : enfin un manuel complet sur le nouveau cadre juridique issu du RGPD et de la loi Informatique et Libertés de 2018*. 3e édition. Paris : Eyrolles, 2018.

ROPARS, Fabien. « Solid : le projet de l'inventeur du World Wide Web pour reprendre possession de ses données personnelles », Le Blog du modérateur, [en ligne]. 1er octobre 2018. Disponible à l'adresse : https://www.blogdumoderateur.com/solid-le-projet-de-linventeur-du-world-wide-web-pour-reprendre-possession-de-ses-donnees-personnelles/

RUBIELLO, Luc. *La face cachée d'internet et des données personnelles*. Paris : Innovativity. 2018.

STERIN, Anne-Laure. « Le point sur les données à caractère personnel », *Ethique et droit*. [en ligne]. Août 2017. Disponible à l'adresse : https://ethiquedroit.hypotheses.org/tag/donnees-personnelles

VIE PRIVEE

ASSOCIATION DES BIBLIOTHECAIRES DE FRANCE. *(Auto)-censure et surveillance de masse, quels impacts pour les bibliothèques ?*. Association des Bibliothécaires de France [en ligne]. 14 mars 2018. Disponible à l'adresse : http://www.abf.asso.fr/5/181/733/ABF/-auto-censure-et-surveillance-de-masse-quels-impacts-pour-les-bibliotheques

DERIEUX, Emmanuel. « Vie privée et données personnelles – Droit à la protection et « droit à l'oubli » face à la liberté d'expression », *Nouveaux cahiers du Conseil constitutionnel* [en ligne]. 8 juin 2015. Disponible à l'adresse : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/nouveaux-cahiers-du-conseil/cahier-n-48/vie-privee-et-donnees-personnelles-%EF%BF%BD-droit-a-la-protection-et-droit-a-l-oubli-face-a-la-liberte-d-expression.143873.html

ETIENNE, Jean-Michel. « Vie privée et logo public. Divulgation de données personnelles en présence du logo d'une institution publique : une expérimentation de terrain », *Réseaux* 2015/1 (n° 189), p. 123-149. DOI 10.3917/res.189.0123. Disponible à l'adresse : https://www.cairn.info/revue-reseaux-2015-1-page-123.htm

FOURMEUX, Thomas. *Voulons-nous des bibliothèques sous surveillance en France ?*. Agorabib [en ligne]. 30 mai 2018. Disponible à l'adresse : http://www.agorabib.fr/topic/3353-voulons-nous-des-biblioth%C3%A8ques-sous-surveillance-en-france

HALPERIN, Jean-Louis, « Protection de la vie privée et *privacy* : deux traditions juridiques différentes ? », *Les Nouveaux Cahiers du Conseil constitutionnel*, 2015/3 (N° 48), p. 59-68.

INTERNATIONAL FEDERATION OF LIBRARY ASSOCIATIONS AND INSTITUTIONS (IFLA). *Déclaration de l'IFLA sur la vie privée dans le monde des bibliothèques*. Ifla.org [en ligne]. 20 août 2015. Disponible à l'adresse : https://www.ifla.org/files/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment-fr.pdf

LINUXFR.ORG. « Protéger sa vie privée sur le Web, exemple avec Firefox ». Linuxfr.org. [en ligne]. 26 février 2018. Disponible à l'adresse : https://linuxfr.org/news/proteger-sa-vie-privee-sur-le-web-exemple-avec-firefox

MERCIER, Silvère. *Vie privée et bibliothèques : enjeux et bonnes pratiques.* Bibliobsession [en ligne]. 12 janvier 2016. Disponible à l'adresse : http://www.bibliobsession.net/2016/01/12/vie-privee-bibliotheques-enjeux-bonnes-pratiques

METALLINOS, Nathalie. « Le principe d'accountability : des formalités préalables aux études d'impacts sur la vie privée », *Communication, commerce électronique*, avril 2018.

NITOT, Tristan. *Surveillance://: Les libertés au défi du numériques : comprendre et agir*. C&F Editions.2016

RALLET, Alain ; ROCHELANDET, Fabrice. « La régulation des données personnelles face au web relationnel : une voie sans issue », *Réseaux*, 2011/3 (n° 167), p. 17-47. DOI 10.3917/res.167.0017. Disponible à l'adresse : https://www.cairn.info/revue-reseaux-2011-3-page-17.htm

TANGHE, Hélène, GIBERT, Paul-Olivier. « L'enjeu de l'anonymisation à l'heure du big data », *Revue française des affaires sociales*, 2017/4, p. 79-93. Disponible à l'adresse : https://www.cairn.info/revue-francaise-des-affaires-sociales-2017-4-page-79.htm

UNTERSINGER. Martin. *Anonymat sur Internet : protéger sa vie privée*. Eyrolles, 2ème ed. 2014.

WRIGHT, D, RAAB, C. « Privacy principles risks and harms », *International Review of law*, computers & technology 28. 2014. p.277-298

PRATIQUE DES BIBLIOTHEQUES

BELVÈZE, Damien. *L'identité numérique du chercheur*. Formadoct. [en ligne]. 23 avril 2018. Disponible à l'adresse : https://guides-formadoct.u-bretagneloire.fr/identite_numerique

BELVEZE, Damien. *Vie privée des utilisateurs : la check-list de la bibliothèque*. [en ligne]. Disponible à l'adresse : https://framindmap.org/c/maps/446392/public

CALIMAQ. *Voulons-nous vraiment des bibliothèques sous surveillance en France ?* S.I.Lex [en ligne]. 30 mai 2018. Disponible à l'adresse : https://scinfolex.com/2018/05/30/voulons-nous-vraiment-des-bibliotheques-sous-surveillance-en-france

FOURMEUX, Thomas. *En 2016, protégeons les données personnelles des usagers des bibliothèques*. Biblio Numericus. [en ligne]. Disponible à l'adresse : https://biblionumericus.fr/2016/01/14/en-2016-protegeons-les-donnees-personnelles-des-usagers-des-bibliotheques

FOURMEUX, Thomas. *Kit pour protéger ses données personnelles en bibliothèque.* 1er décembre 2015. Disponible à l'adresse : https://fr.slideshare.net/Biblioveilleur/kit-pour-protger-ses-donnes-personnelles-en-bibliothque

FOURMEUX, Thomas. *Livres numériques : doit-on contribuer à l'exploitation des données personnelles des usagers ?*. Biblio Numericus. [en ligne]. 30 mars 2018. Disponible à l'adresse : https://biblionumericus.fr/2018/03/30/livres-numeriques-doit-on-contribuer-a-lexploitation-des-donnees-personnelles-des-usagers

GARY, Nicolas. « Lecteurs en danger : espionnage et collecte de données. » *Actualitté*. [en ligne]. 21 avril 2018. Disponible à l'adresse : https://www.actualitte.com/article/zone-51/lecteurs-en-danger-espionnage-et-

collecte-de-donnees/88501

HEURTEMATTE, Véronique. « Données personnelles et surveillance de masse à l'étude », *Livres Hebdo*. 17 janvier 2018.

JOLY, Julien. « Avec la Cryptoparty, protégez vos données perso sur internet », *Le Télégramme* [en ligne]. Disponible à l'adresse : http://www.letelegramme.fr/soir/cryptoparty-les-internautes-invisibles-07-06-2017-11545269.php

LA QUADRATURE DU NET. *Guide juridique : Internet en libre accès, quelles obligations ?*. [en ligne] 29 janvier 2018. Disponible à l'adresse : https://www.laquadrature.net/2018/01/31/guide_internet_libre_acces/

LOWE, Marsha. « New assisted digital contract for libraries », *Society of Chief Librarians* [en ligne]. Disponible à l'adresse : http://goscl.com/new-assisted-digital-contract

ROSSI, Julien, BIGOT, Jean-Edouard. « Traces numériques et recherche scientifique au prisme du droit des données personnelles », *Les Enjeux de l'Information et de la Communication*, n°19/2, 2018, p.161-177, [en ligne]. Disponible à l'adresse : https://lesenjeux.univ-grenoble-alpes.fr/2018-dossier/12/

VIGUIÉ, Céline. « Données personnelles et usagers : quel rôle pour les bibliothécaires ? », *Bulletin des bibliothèques de France* [en ligne]. Janvier 2016. Disponible à l'adresse : http://bbf.enssib.fr/tour-d-horizon/donnees-personnelles-et-usagers-quel-role-pour-les-bibliothecaires_65756

SITOGRAPHIE

AMERICAN LIBRARY ASSOCIATION. [en ligne]. Disponible à l'adresse : http://www.ala.org/

ASSOCIATION DATA PROTECTION OFFICERS. [en ligne]. Disponible à l'adresse : https://www.data-protection-officer-association.eu/

ASSOCIATION DES BIBLIOTHECAIRES DE FRANCE. [en ligne]. Disponible à l'adresse : http://www.abf.asso.fr

FRANCE. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES. [en ligne]. Disponible à l'adresse : https://www.cnil.fr/

FRANCE. AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION [en ligne]. Disponible à l'adresse : https://www.ssi.gouv.fr/

INTERNATIONAL FEDERATION OF LIBRARY ASSOCIATIONS AND INSTITUTIONS (IFLA). [en ligne]. Disponible à l'adresse : https://www.ifla.org/

LA QUADRATURE DU NET. [en ligne]. Disponible à l'adresse : https://www.laquadrature.net

RESEAU SUPDPO. [en ligne]. Disponible à l'adresse : https://groupes.renater.fr/wiki/supdpo/doku.php

UNION DES DPO. [en ligne]. Disponible à l'adresse : https://www.udpo.fr/

ANNEXES

TABLE DES ANNEXES

ANNEXE 1 – QUESTIONNAIRE SUR LA PROTECTION DE LA VIE PRIVEE PAR LES BIBLIOTHECAIRES

Enquête diffusée, entre le 19 juillet 2018 et le 21 octobre 2018 via les outils et listes de diffusion suivantes : ADBU-Forum, Agorabib, Cryptobib, Juriconnexion, Parcours Numériques, Comptes personnels Twitter et Facebook.

Limesurvey est le logiciel qui a été utilisé pour l'exploitation des données.

Elève-conservatrice à l'Enssib (DCB27), je travaille sur un mémoire ayant pour sujet la protection des données personnelles par les bibliothécaires français. Il s'agit de voir comment les bibliothécaires français appliquent le nouveau Règlement européen pour la protection des données (RGPD) et leur positionnement éthique et professionnel face à la vie privée de leurs usagers. Toutes les catégories de personnel des bibliothèques peuvent répondre à ce questionnaire, n'hésitez pas à le partager avec vos collègues.
Ce questionnaire est totalement anonyme.
D'avance, je vous remercie de votre participation.

Marion Chovet

Merci de m'accorder environ 8 minutes

Il y a 19 questions dans ce questionnaire

Données à caractère personnel

Aucune connaissance sur les données personnelles n'est prérequise.

Avez-vous été informé(e) du Règlement européen sur la protection des données à caractère personnel ?

Veuillez sélectionner une seule des propositions suivantes :

- ○ Oui
- ○ Non

Selon vous, sont des données à caractère personnel

Cochez la ou les réponses

Veuillez choisir toutes les réponses qui conviennent :

- ☐ Un identifiant lecteur
- ☐ Un nom
- ☐ Une adresse postale
- ☐ Une photo
- ☐ Une empreinte
- ☐ Une date de naissance
- ☐ Une adresse IP
- ☐ Une adresse mail

Selon vous, peuvent contenir des données à caractère personnel

Cochez la ou les réponses

Veuillez choisir toutes les réponses qui conviennent :

- ☐ Un catalogue de bibliothèque

- [ ] Une base lecteur
- [ ] Un identifiant pour accéder à des bases de données
- [ ] Un SIGB
- [ ] Un ordinateur en libre accès

Concrètement dans votre établissement

Votre établissement communique-t-il auprès de ses usagers sur sa politique en matière de protection des données à caractère personnel ?

Cochez la ou les réponses

Veuillez choisir toutes les réponses qui conviennent :

- [ ] Oui sur son site web
- [ ] Oui sur les réseaux sociaux
- [ ] Oui avec des affiches
- [ ] Oui par mail
- [ ] Oui avec d'autres moyens (merci de préciser lesquels)

Si votre établissement ne communique pas, merci de l'indiquer dans "Autre"

Merci de préciser les modes de communication

Répondre à cette question seulement si les conditions suivantes sont réunies : La réponse était 'Oui avec d'autres moyens (merci de préciser lesquels)' à la question '4 [D2]' (Votre établissement communique-t-il auprès de ses usagers sur sa politique en matière de protection des données à caractère personnel ?)

Veuillez écrire votre réponse ici :

Avez-vous une procédure pour répondre à une demande d'usager au sujet de ses données à caractère personnel ?

Cochez la ou les réponses

Veuillez choisir toutes les réponses qui conviennent :

- [ ] Pour le déréférencement (par exemple la date de naissance dans une notice)
- [ ] Pour la suppression des données (par exemple suppression du compte lecteur)
- [ ] Pour donner l'accès aux données de l'usager
- [ ] Pour permettre à l'usager de récupérer ses données (portabilité des données)
- [ ] Pour obtenir la liste des prêts précédents
- [ ] Il n'existe aucune procédure
- [ ] Autre:

Connaissez-vous les missions du Délégué à la protection des données (DPO) de votre établissement ?

Veuillez sélectionner une réponse ci-dessous

Veuillez sélectionner une seule des propositions suivantes :

- ○ Oui je connais les missions d'un DPO
- ○ Non je ne connais pas les missions d'un DPO

○ Je ne sais pas ce qu'est un DPO

Des formations sur la protection de la vie privée des utilisateurs sont-elles proposées (ou en projet pour 2018/2019) ?

Cochez la ou les réponses

Veuillez choisir toutes les réponses qui conviennent :

☐ Aux personnels

☐ Aux usagers

☐ Aucune formation n'est assurée en interne

☐ Toutes les formations sont externalisées

☐ Je ne sais pas

Selon vous, est-il important de proposer des formations sur la protection de la vie privée aux usagers

Veuillez sélectionner une seule des propositions suivantes :

○ 1

○ 2

○ 3

○ 4

○ 5

1 = Pas du tout d'accord

5 = Entièrement d'accord

Selon vous, est-il important de proposer des formations sur la protection de la vie privée aux personnels ?

Veuillez sélectionner une seule des propositions suivantes :

○ 1

○ 2

○ 3

○ 4

○ 5

1 = Pas du tout d'accord

5 = Entièrement d'accord

Votre avis

Les bibliothécaires doivent jouer un rôle dans la protection de la vie privée de leurs usagers *

Veuillez sélectionner une seule des propositions suivantes :

○ 1

○ 2

○ 3

- ○ 4
- ○ 5

1 = Pas du tout d'accord

5 = Entièrement d'accord

La protection des données à caractère personnel doit être un élément décisif dans le choix des outils ou services (abonnement à des bases de données, applications de réservation, livres électroniques ...) mis à disposition des usagers

Veuillez sélectionner une seule des propositions suivantes :

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5

1 = Pas du tout d'accord

5 = Entièrement d'accord

Estimez-vous avoir une responsabilité quant à l'usage des ordinateurs publics de la bibliothèque ?

Veuillez choisir toutes les réponses qui conviennent :

- ☐ Oui, pour garantir un usage équitable entre tous les utilisateurs
- ☐ Oui, pour empêcher la consultation de sites interdits par la loi
- ☐ Oui, pour empêcher la consultation de sites inappropriés pour des jeunes lecteurs
- ☐ Oui, pour permettre une consultation la plus sûre et confidentielle possible
- ☐ Non, pas de responsabilité particulière

A titre personnel, êtes-vous particulièrement vigilant sur la surveillance électronique de masse, et la protection de vos données à caractère personnel ?

Veuillez sélectionner une seule des propositions suivantes :

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5

1 = Pas du tout d'accord

5 = Entièrement d'accord

Si vous souhaitez rajouter quelques éléments qui vous semblent manquer dans ce questionnaire, vous pouvez vous exprimer ici.

Vous pouvez également me laisser votre adresse mail, dans cette zone, pour que je puisse vous contacter.

Veuillez écrire votre réponse ici :

Mieux vous connaître

Vous travaillez dans une bibliothèque

Veuillez sélectionner une seule des propositions suivantes :

- ○ Bibliothèque relevant du Ministère de l'Enseignement supérieur (SCD, BIU etc.)
- ○ Bibliothèque relevant du Ministère de la Culture (BnF, BPI)
- ○ Bibliothèque territoriale
- ○ Bibliothèque ou centre de documentation d'une structure publique (Ministère, Juridiction, Agence etc.)
- ○ Bibliothèque ou centre de documentation d'une structure privée
- ○ Autre

Vous travaillez dans un service de :

Veuillez sélectionner une seule des propositions suivantes :

- ○ Traitement documentaire
- ○ Services aux publics
- ○ Formations
- ○ Collections (achat, monographies, périodiques)
- ○ Ressources électroniques
- ○ Service informatique
- ○ Autre

Vous êtes

Veuillez sélectionner une seule des propositions suivantes :

- ○ Conservateur, ingénieur.e de recherche (ou assimilé)
- ○ Bibliothécaire, ingénieur.e d'étude (ou assimilé)
- ○ Bibas, technicien.ne (ou assimilé)
- ○ Magasinier (ou assimilé)
- ○ Autre

Quelle est votre tranche d'âge ?

Veuillez sélectionner une seule des propositions suivantes :

- ○ 20-30
- ○ 31-40
- ○ 41-50
- ○ 51-60
- ○ 61-

Je vous remercie de votre participation – 21/10/2018

.

Merci d'avoir complété ce questionnaire.

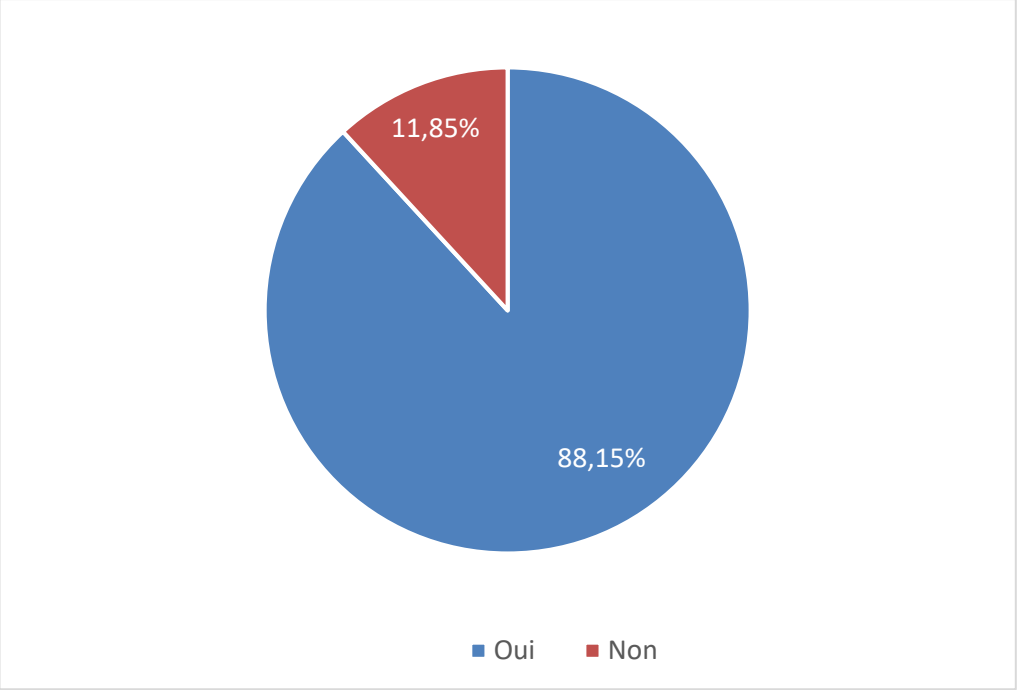
ANNEXE 2 – EXPLOITATION DES RESULTATS DU QUESTIONNAIRE

730 réponses ont été enregistrées, dont 439 complètes (soit 60,14%) et 291 partielles (39,86%). Seuls les questionnaires complets ont été analysés.

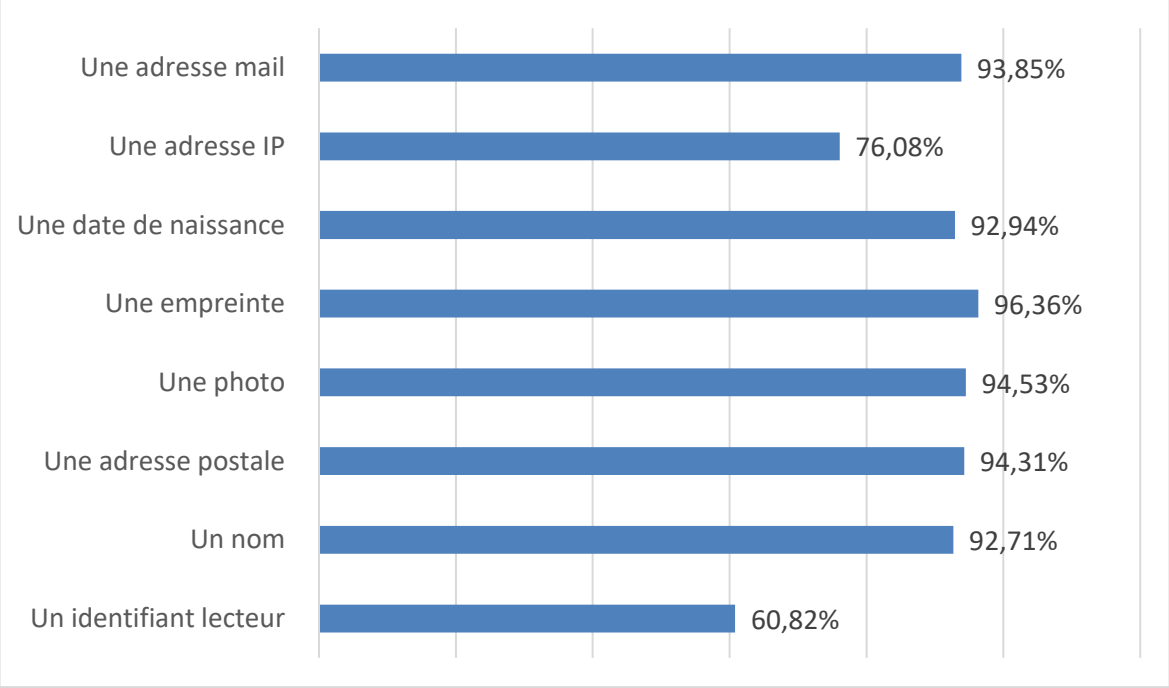
Données à caractère personnel

Aucune connaissance sur les données personnelles n'est prérequise.

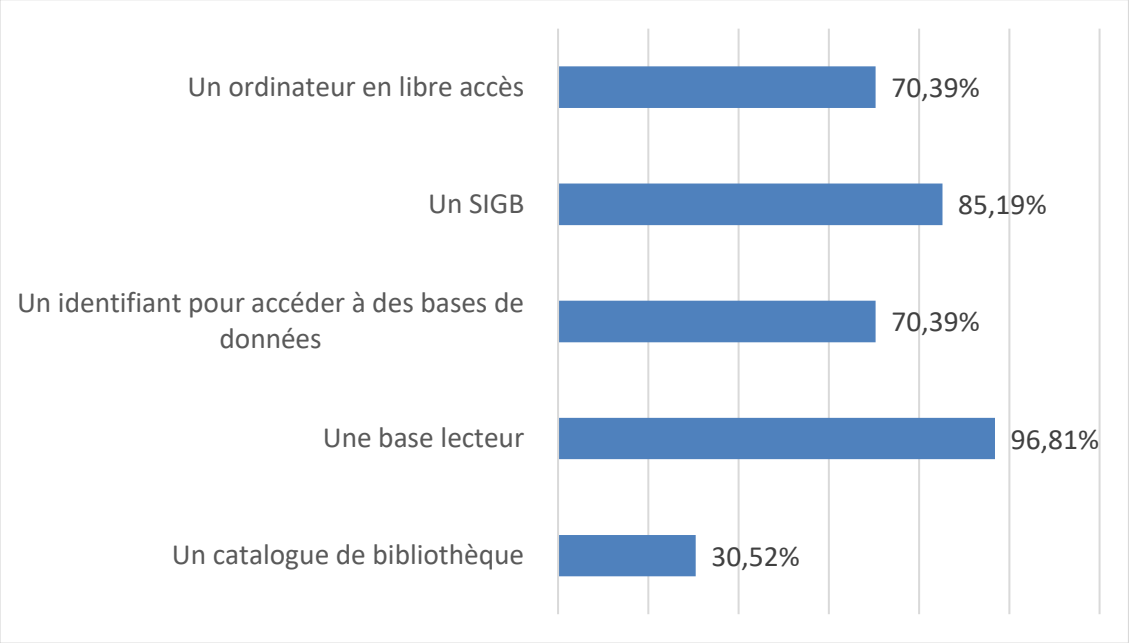
Avez-vous été informé(e) du Règlement européen sur la protection des données à caractère personnel ?



Selon vous, sont des données à caractère personnel

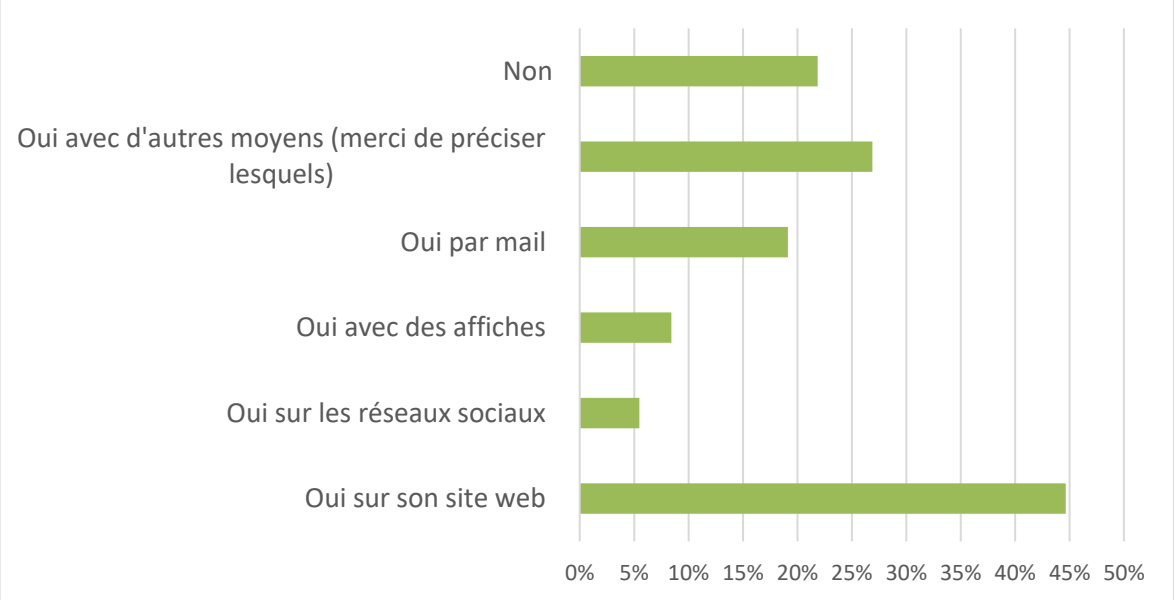


Selon vous, peuvent contenir des données à caractère personnel



Concrètement dans votre établissement

Votre établissement communique-t-il auprès de ses usagers sur sa politique en matière de protection des données à caractère personnel ?



Merci de préciser les modes de communication

Ici, ne serons publiés que les verbatims les plus significatifs

Via le règlement intérieur

Dans les courriers ou contrats, mention dans les clauses.

Lors de l' inscription (finalité de l'adresse mail par exemple) + communication directe si question sur usages données (pourquoi téléphone, pourquoi mail...)
Sinon, le site de la ville l'évoque dans ses mentions légales

Non à l'heure actuelle, le travail autour du RGPD vient d'être lancé au niveau de la Mairie.

Oral en face à face avec le lecteur

Présentation aux usagers

En réalité, c'est non. Nous ne sommes pas encore en conformité avec le RGPD.

sur la page d'accueil du catalogue

Ne communique pas encore, va le mettre en place via le mail et la page d'accueil pour l'accès wifi

JE crois que le travail de communication est en cours

Je ne sais pas si mon établissement communique sur le RGPD

A ma connaissance, aucun modes de communication mis en place pour la RGPD dans mon établissement. C'est un projet en cours

Newsletter

Pratiquement aucune communication, ponctuellement une info sur les sites

Charte informatique
une communication gérée par le réseau des bibliothèques est intégrée à la page d'accueil du catalogue sur l'usage de données personnelles des lecteurs inscrits dans les bibliothèques

on trouve sur le site de mon établissement des mentions au RGPD, mais pas de communication en tant que telle.

Actuellement l'Université n'a rien mis en place, ce sera fait dans trois mois à travers une campagne d'information multisupports (affichage, mail, ENT tc...)

On ne précise rien.

l'information se fait à l'oral

par voie orale

En fait, c'est non, nous devons passer par le service informatique de la ville qui ne répond pas à nos demandes à ce sujet, mais je ne désespère pas !

Affichage

la fiche d'inscription

aucun

Signature de charte informatique

La mairie a mandaté un service départemental pour que tous les services municipaux soient à jour de la nouvelle réglementation. Tout est en cours

Pour le moment, rien. On attend les infos "officielles".

Pas vraiment de communication. Réponses au cas par cas aux usagers qui souhaitent savoir si leurs données personnelles lors de l'inscription sont conservées, si on dispose d'un historique de leurs emprunts...

De visu à l'inscription : propose au nouvel abonné de laisser son mail (ou pas) pour recevoir news lettre

A l'heure actuelle, le service commun de documentation n'a pas communiqué - à ma connaissance. En revanche, l'Université a communiquer sur ce point.

Présentation dédiée

Les seuls moments où l'on parle des données personnelles à nos usagers, me semble-t-il, est lorsque :
- nous demandons leur adresse mail et numéro de téléphone (ils nous demandent parfois comment elles vont être utilisées, nous leur répondons que seule la bibliothèque y a accès afin de leur communiquer l'arrivée d'une réservation ou l'approche d'une échéance de prêt).
- ils souhaitent connaître leurs prêts antérieurs (nous leur expliquons alors que leurs données de prêt sont supprimées tous les trois mois dans le cadre de la protection des données personnelles).

par des formations internes de sensibilisation et enquête interne

Règlement intérieur affiché dans les établissements et distribué à l'inscription. Fonds d'écran sur les postes informatiques publics

Le SCD ne communique pas sur la protection des données personnelles auprès de ses usagers.

Non, c'est la collectivité qui communique pour tous ses services

Autre (=non)

Pour le moment, nous ne sommes pas au point et ne communiquons pas sur le sujet. Affichage et communication en préparation pour la rentrée 2018.

en cours de formalisation concernant la collectivité + idem le fournisseur du SIGB de la bibliothèque

Nous attendons l'arrivée du référent RGPD à la ville pour fournir une communication précise. Nous communiquerons en septembre octobre via notre newsletter et le site internet de la médiathèque. Des informations de prévention sont présentes dans l'espace multimédia.

Pas de communication sur ce sujet, sinon oralement aux lecteurs quand ils ont des questions ("pourquoi voulez-vous mon numéro de téléphone ?").

pas de communication spécifique au niveau des bibliothèques (attente d'une communication au niveau de l'université)

Pas de communication particulière au moment de l'entrée en vigueur du règlement européen.

En banque de communication, lorsqu 'un lecteur veut avoir accès à l'historique de ses réservations.

Formation

Pour le moment pas d'informations précises. Cela va évoluer dans les semaines à venir, nous attendions les directives du référent RGPD de la collectivité. Au regard de l'organisation de la collectivité, il fallait attendre la validation du référent. Cependant, la bibliothèque était déjà en règle vis-à-vis de la CNIL et garde très peu de données personnelles et uniquement celles qui sont nécessaires pour les emprunts.

ne communique pas.

Fiches remplies par les usagers lors de leur insrcription

Pas de communication à ce jour.

Aucun pour l'instant. Prévu lors du changement du site Internet en 2019

en participant au festival des Libertés numériques (table ronde)

Formulaire papier avec des cases à cocher lors de l'inscription / la réinscription à la bibliothèque ou pour des accès aux plateformes numériques (Vodéclic par ex.). On explique à l'usager à ce moment-là.

A l'oral, directement auprès du public (notamment quand la base lecteur est mise à jour ou quand le catalogue ne permettait pas encore de garder un historique des prêts sur le compte de l'utilisateur). Occasion de rappeler nos obligations en termes de protection de leur données (c'était avant le RGPD)

Animations prévues cette année sur ce sujet.

Aucun, nous sommes en réseau (en construction) avec un renouvellement récent des cadres, donc pas de consensus ni de réflexion encore là-dessus

Animations

Il y a un avertissement sur la fiche d'inscription. Il y a un rappel en bas de la newsletter

par une formation spécifique proposée aux agents : (de mémoire intitulé la protection des données des usagers)

Pas de communication pour l'instant, hors verbale. Nous attendons de nos prestataires (SIGB et portail) les éléments nécessaires

aucun

dans charte informatique

On en discute entre collègues.

Règlement intérieur et de façon orale

Aucun

il ne communique pas
impossible de répondre NON à cette question dans le questionnaire (dommage)

oral

Formulaire d'inscription

Sur des formulaires d'inscription (lecteurs extérieurs), lors de l'activation du compte numérique (ENT)

Aucune communication

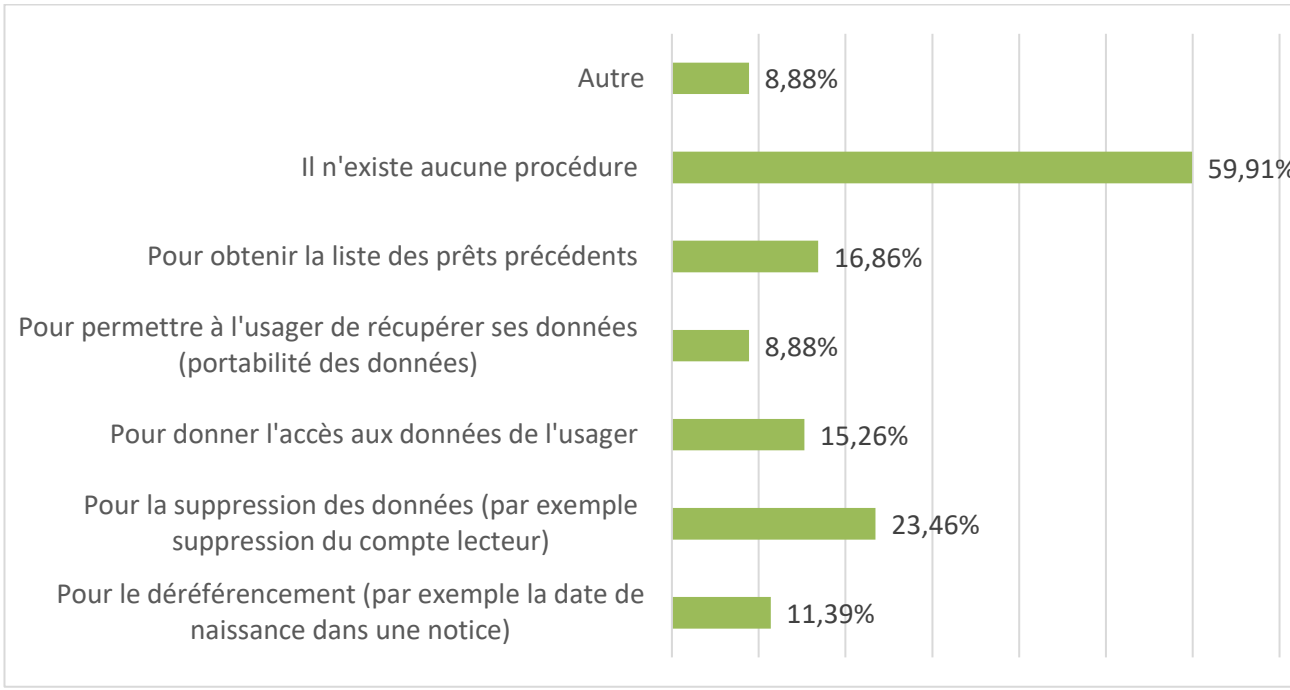
Fiche d'inscription / Charte Espace Numérique

Oralement

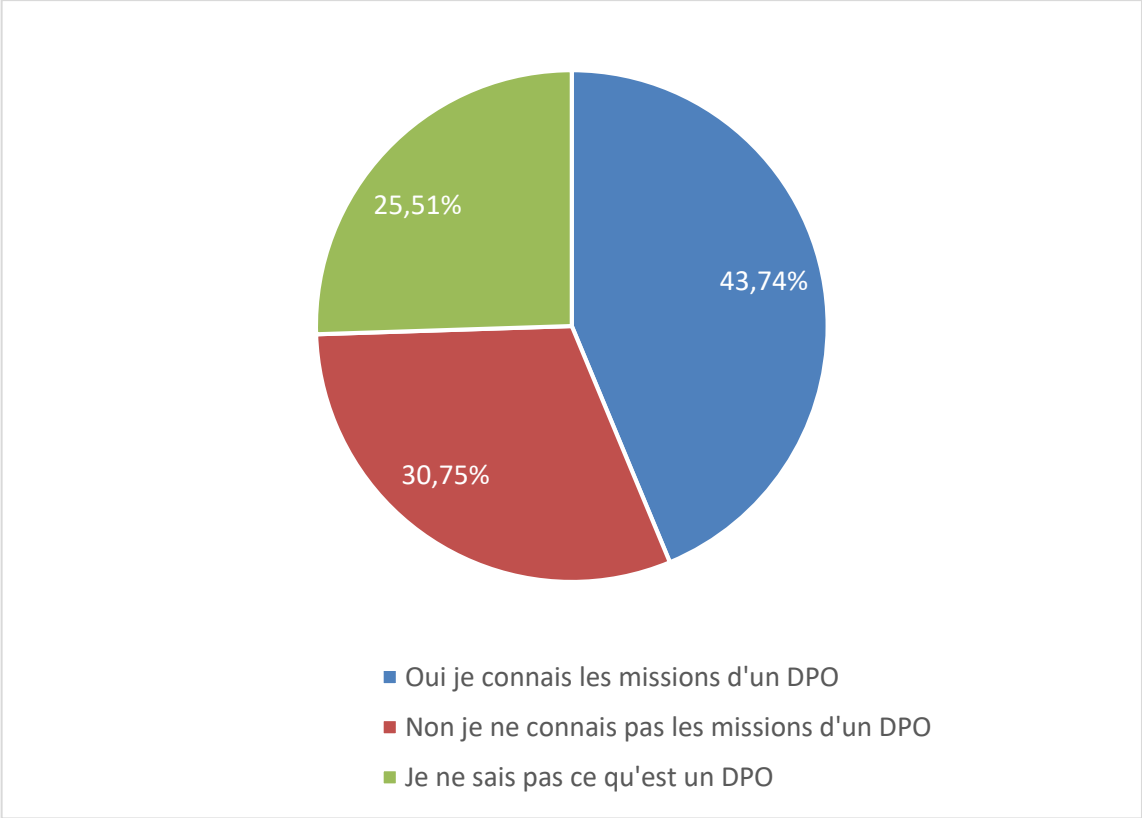
autre. pas de communication

Pas de communication à ma connaissance

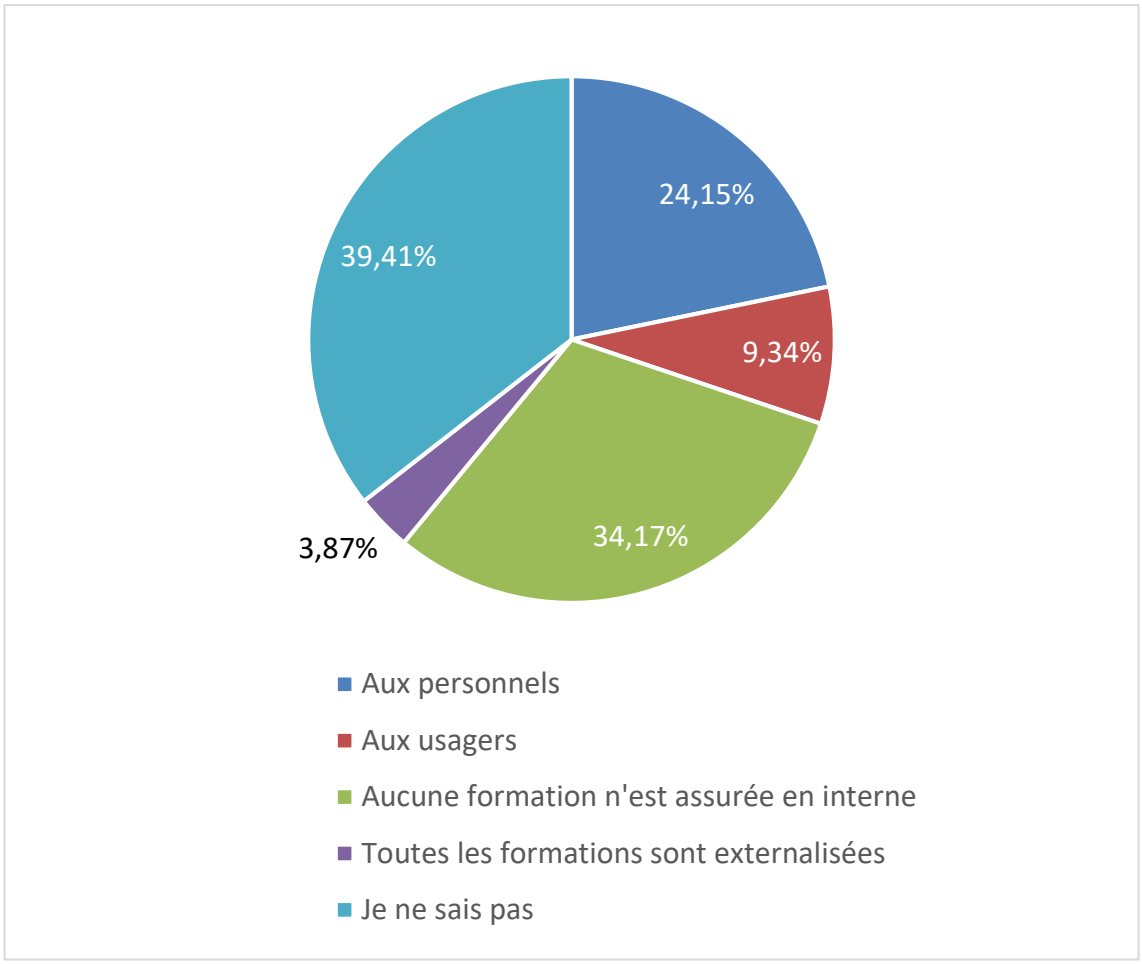
Avez-vous une procédure pour répondre à une demande d'usager au sujet de ses données à caractère personnel ?



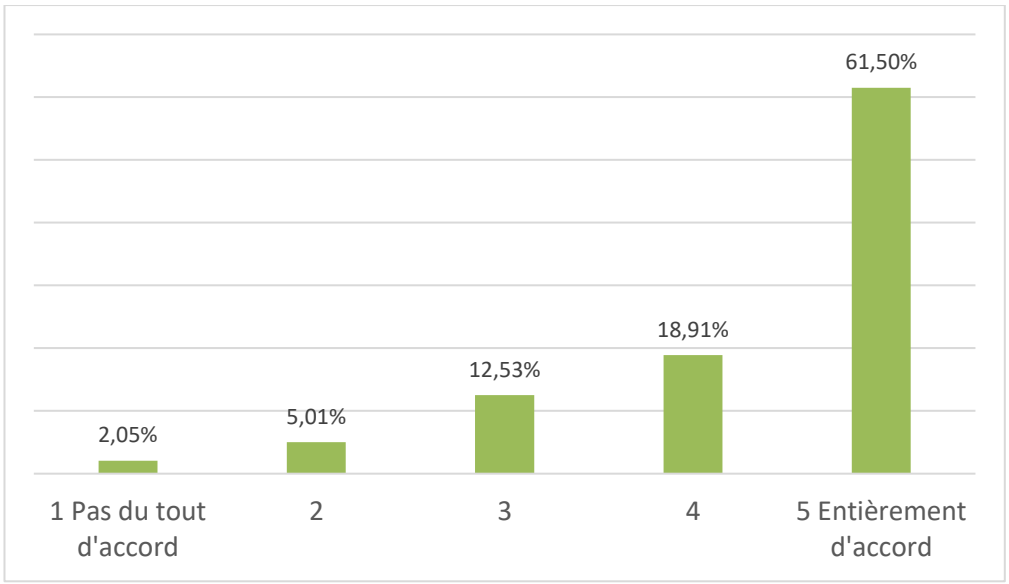
Connaissez-vous les missions du Délégué à la protection des données (DPO) de votre établissement ?



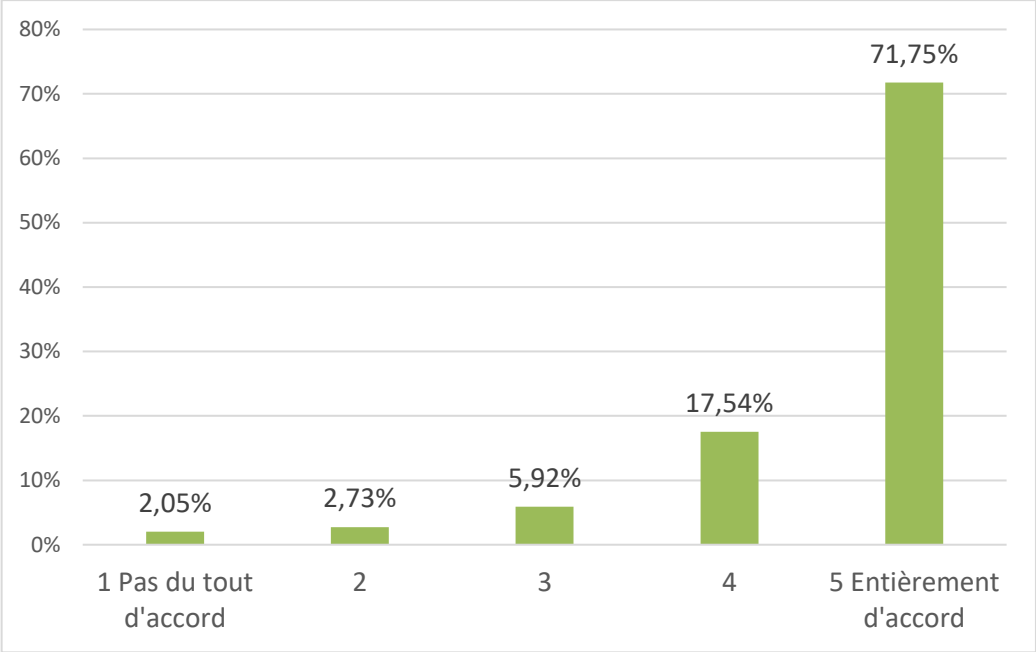
Des formations sur la protection de la vie privée des utilisateurs sont-elles proposées (ou en projet pour 2018/2019) ?



Selon vous, est-il important de proposer des formations sur la protection de la vie privée aux usagers

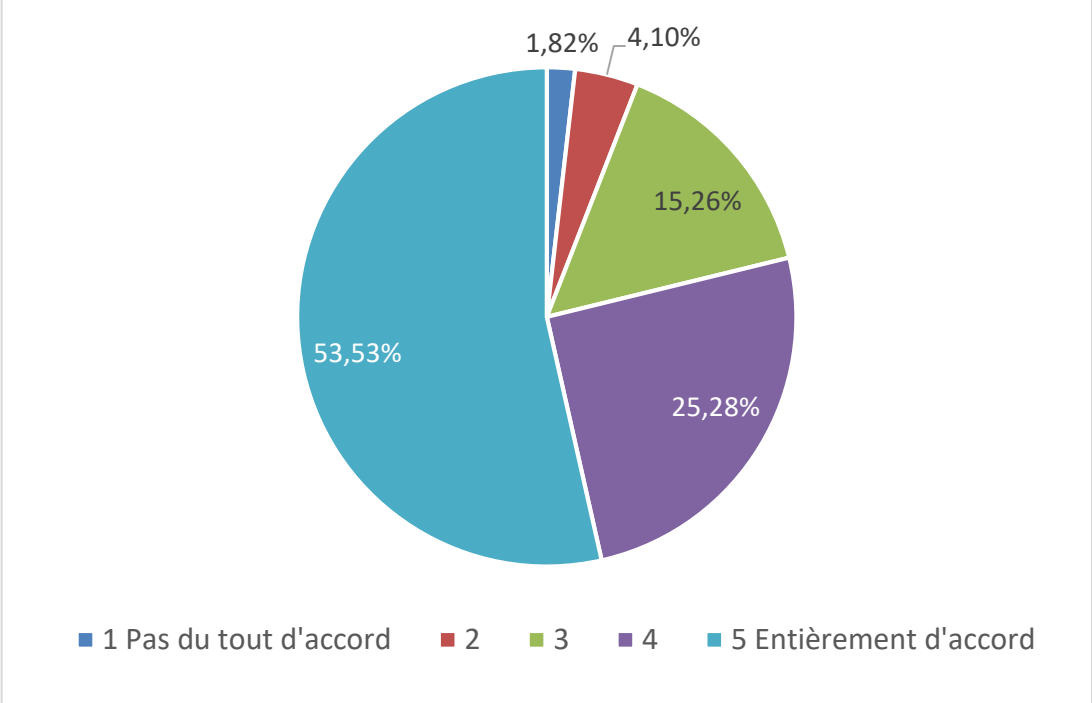


Selon vous, est-il important de proposer des formations sur la protection de la vie privée aux personnels ?

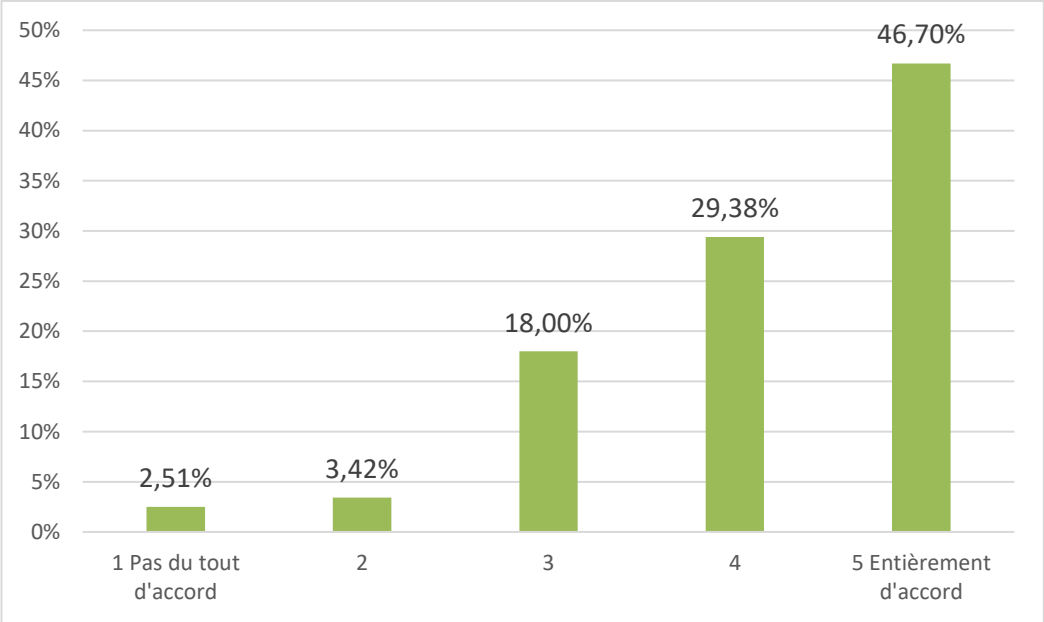


Votre avis

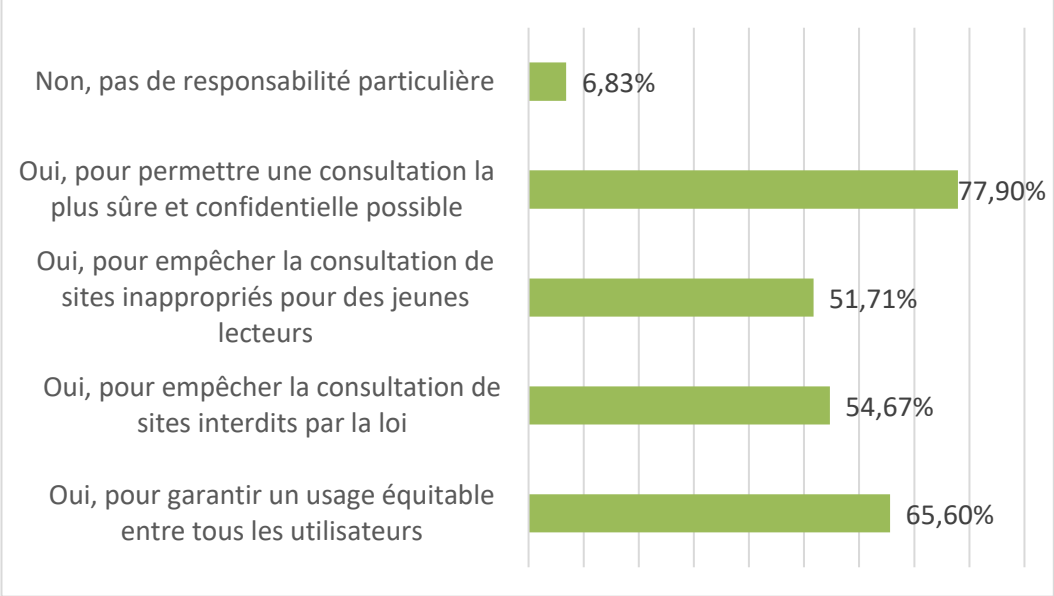
Les bibliothécaires doivent jouer un rôle dans la protection de la vie privée de leurs usagers



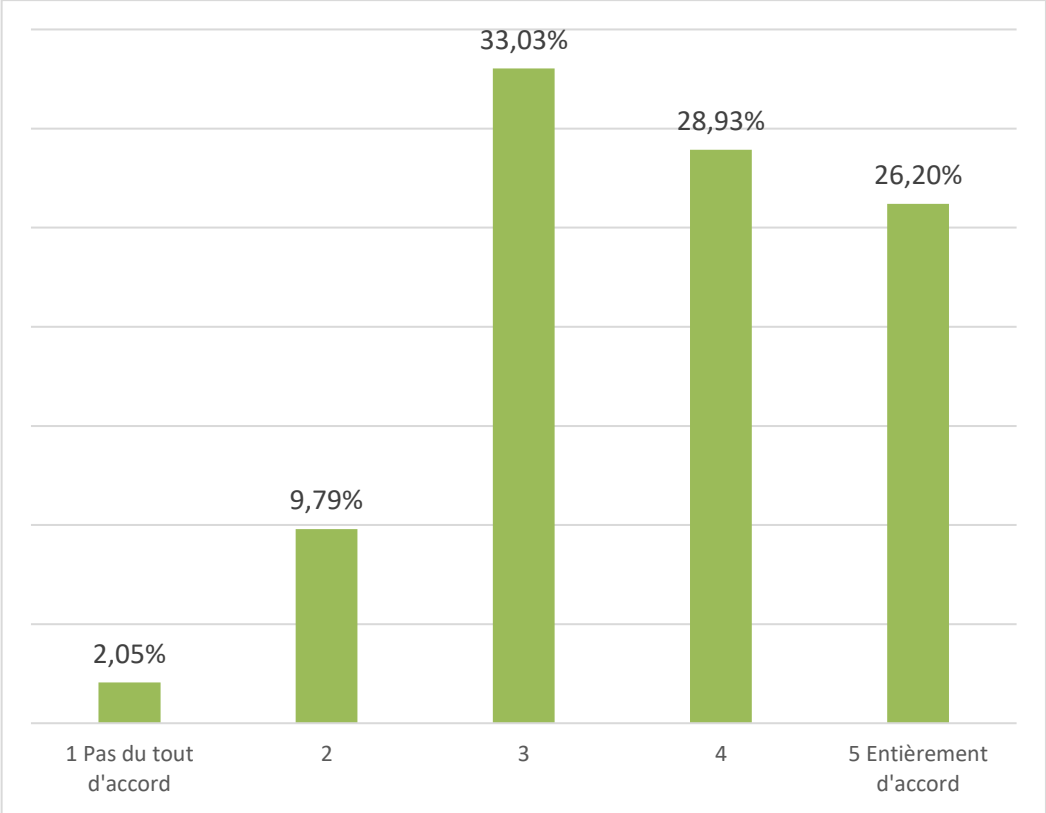
La protection des données à caractère personnel doit être un élément décisif dans le choix des outils ou services (abonnement à des bases de données, applications de réservation, livres électroniques ...) mis à disposition des usagers



Estimez-vous avoir une responsabilité quant à l'usage des ordinateurs publics de la bibliothèque ?



A titre personnel, êtes-vous particulièrement vigilant sur la surveillance électronique de masse, et la protection de vos données à caractère personnel ?



Si vous souhaitez rajouter quelques éléments qui vous semblent manquer dans ce questionnaire, vous pouvez vous exprimer ici.

Sélection de verbatim

« Sur la question des formations, vous pouvez recontacter mon service. Nous avons des formations destinees en priorité aux masters sur la question de l'identité numérique ou la question des données personnelles est abordée. Nous avons egalement créé et scénarisé cette année une murder party pedagogique en partenariat avec Legifrance, dont le sujet central n'etait pas la protection des données, mais qui abordait la question des gafam, et les licences CC. Par ailleurs, nous avons egalement crée un serious escape game sur la question des fake news, et l'une des fake news qu'il faut invalider dans notre escape game concerne une usurpation d'identité sur les réseaux sociaux (dans ce cas precis, le sujet de la protection des données personnelles est évoqué en marge d'autres sujets, mais nous espérons vraiment pouvoir diversifier et etendre nos propositions sur ces sujets dans l'avenir). Ces différents thèmes sont également abordés dans Hellink (jeu vidéo sur les compétences informationnelles et l'esprit critique créé au sein de mon équipe l'an dernier). Une question problématique qui va se poser à nous dans un avenir tres proche est celui des Learning Analytics, et de la collecte de données afférentes. Si ces données sont bien entendu anonymisées, je constate depuis environ 5 ans que la question de la collecte des données pédagogiques se pose avec accuité, dans un moment ou le recours desormais devenu massif au blended learning et aux LMS ne peut malheureusement pas toujours s'accompagner par une sensibilisation systematique de l'ensemble de la communauté etudiante et des equipes enseignantes aux questions de protection de la vie privée. Nous mêmes, bibliothécaires devons nous former et exercer une veille sur ces questions. Les bibliotheques vont certainement etre amenées a jouer un role de plus en plus grand sur ces questions. »

« Il serait intéressante d'ajouter des questions sur le rôle des services informatiques qui ont souvent la main sur un certain nombre de données, les mises à jours des logiciels etc... et pas les bibliothécaires malheureusement. »

« Malgré ma présence à plusieurs journées d'information à ce sujet, je me rend compte qu'il me manque encore des connaissances. Je pense que le rôle des bibliothèques dans ce domaine est primordial car la grande majorité de la population n'a pas conscience de l'importance des enjeux et implications de ce sujet. Nous devrions être une institution irréprochable en terme de protection des données personnelles, ainsi que le fer de lance de la sensibilisation du public. Sinon qui d'autre le fera ?“

« En tant de personnels de bibliothèque universitaire, nous sommes souvent tributaires des décisions des services informatiques de l'Université (exemple : suppression des comptes lecteurs à une date donnée, utilisation du wifi) . Je me suis informée à titre personnel sur le RGPD mais dans le cadre du travail nous n'avons pas encore de procédure, cela viendra sans doute. »

« Je trouve que malgré la richesse et la complétude des données personnelles que nous collectons auprès de nos usagers, ceux-ci nous font montre d'une grande confiance à ce sujet. Ceci est même vrai pour les lecteurs les plus fragiles psychologiquement qui nous avouent se croire surveillés (ils sont moins rares qu'on pourrait le penser) alors que , paradoxalement, nous sommes parmi les agents publics ayant le plus d'informations les concernant. »

« En ce qui concerne les BU, seule la gestion de la base lecteurs et la non-divulgation d'infos personnelles à un tiers revient vraiment à la BU. Pour le reste (charte informatique, utilisation d'ordinateurs et impression de façon systématiquement identifiée, etc.) tout cela est géré au niveau du service informatique de l'établissement et "redescend" vers les bibliothèques ».

« Ayant évolué dans des fonctions administratives depuis plusieurs années, je ne suis plus "bibliothécaire" depuis longtemps. Néanmoins, il apparaît indispensable que les professionnels des bibliothèques soient à jour de ces connaissances là, qui font partie du socle des connaissances professionnelles, qu'ils puissent en être porteurs et médiateurs auprès des publics, dans une perspective d'éducation citoyenne informelle. »

« Les bibliothèques étant municipales ou communautaires, la problématique du RGPD ne peut être initiée qu'au plus haut niveau décisionnaire. Une seule structure ne peut pas se rendre conforme au RGPD, sans un projet global à tous les services de toute la collectivité. En clair : si ça ne bouge pas en haut, ça ne bougera pas en bas. »

« Pour compléter ma réponse à la question des formations internes à la protection des données : notre "DPO", très engagé sur ce sujet, organise des formations, rencontres,... en dehors des heures ouvrées sur ce sujet et un festival sur ce thème (je ne donne pas son nom dans un soucis d'anonymat du questionnaire) dont la bibliothèque est partie prenante. »

« Dans ma collectivité, je sais que la question de la protection des données personnelles est prise en compte, mais elle est traité par le DPO sans que les agents n'aient trop d'infos sur le sujet (ce qui me semble plutôt normal au vu des multiples tâches que nous avons à assurer déjà en tant qu'agent). Par contre les documents demandés pour un accès Internet pour les non-abonnés est une question d'actualité chez nous, avec des tendances différentes au sein des équipes (tolérance si pas de CI car il faut privilégier un accès à l'information et au numérique vs application stricte du règlement : CI obligatoire). Même s'il semble que les directives européennes aillent dans le sens de plus de souplesse et donc de ne pas systématiquement demander la CI. On est donc en plein débait et aussi en pleine confusion dans ma collectivité car selon les équipements on n'applique pas les mêmes procédures. Excusez les raccourcis mais l'essentiel est là... »

« La formation des bibliothécaires et avant tout leur sensibilisation à ces questions est un véritable enjeu. La protection des données personnelles est souvent perçue comme étant le domaine réservé de quelques spécialistes. Il est nécessaire que la profession s'empare réellement de ces questions, en explicitant, vulgarisant, en faisant que ce thème soit inclus dans le quotidien des bibliothécaires. »

« Je suis une petite bibliothèque avec un seul ordinateur mis à disposition. Je n'ai pas de formation pour mes usagers mais nous en parlons de manière individuel et le fab-lab voisin (10 km) en fait beaucoup, je n'ai donc pas le temps et les connaissances suffisante pour assurer le même service. »

« en l'occurrence je suis chargée à la BU d'un module pour lequel les données étudiantes sont communiquées à une entreprise extérieure gérant le logiciel. Analogue au TOEIC. Un professeur de droit de la fac nous a interrogés là-dessus. j'en ai référé à mon Directeur. Nous lui avons communiqué le contrat signé avec l'entreprise. il comportait un alinéa précisant que les parties s'obligeaient à ne pas diffuser les données personnelles transmises, et ne les conserveraient que pour la bonne marche du service rendu. Nous savons qu'ils les conservent au moins 4 ans, car ils donnent

à l'étudiant un code, que celui-ci peut retransmettre à son recruteur ou qui il veut, de manière que ce dernier vérifie le score affiché dans son CV (ou ailleurs). Le professeur de droit s'est satisfait de la réponse. Néanmoins je ne suis pas en mesure de vérifier ce que l'entreprise fait de ces données. Aucun étudiant ne s'est plaint de la publicité certainement liée. »

« Je pense que pour les usagers provenant de pays où il y a une dictature en place, et donc où les usagers sont susceptibles d'être fichés, voire dénoncés à tout moment par les autorités de leur pays, pour tel ou tel motif d'ordre intellectuel ou politique, il est important de protéger la vie privée de ces dits usagers. Sinon, si les pays ne sont pas menacés par des dictatures, il ne faut pas sombrer dans la paranoïa, mais rester quand même vigilants ! »

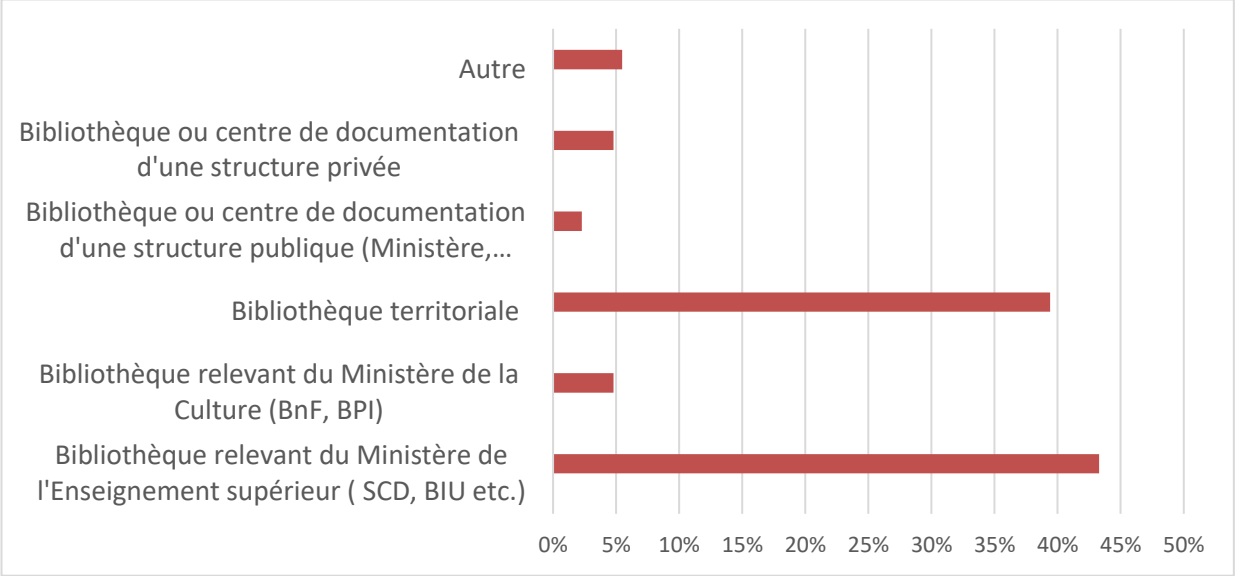
« nous sommes en train de programmer 2 journées pour les usagers à ce sujet, en janvier/février 2019 ; toutefois nous n'avons pas fait de démarche pour sensibiliser particulièrement l'ensemble des agents de la bibliothèque. L'idée sera de former aussi les agents du pôle numérique à cette occasion. le sujet est complexe et il faut vraiment bien le maitriser pour pouvoir en faire la vulgarisation raison pour laquelle nous ferons appel aux intervenants de l'association Nothing2Hide pour animer ces ateliers. L'enjeu étant bien de rester dans un discours équilibré à ce sujet et de ne pas verser dans le militantisme. »

« Dans le cadre de certaines actions de coopération, il nous est indispensables de recourir à des outils proposés par Google et Facebook, alors même que dans les services culturels de la municipalité où je travaille nous faisons le maximum pour avoir recours à des alternatives libres (type Framasoft, Chatons, etc.). Donc même en essayant d'être vertueux et pédagogues, nous ne pouvons faire l'économie de travailler en nous appuyant sur certaines grandes entreprises du capitalisme numérique. »

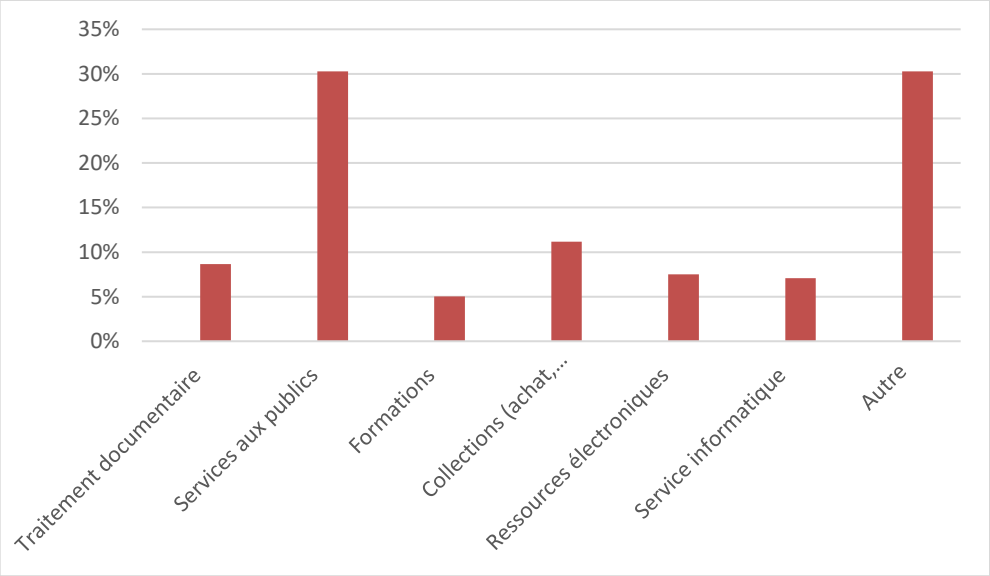
Vous pouvez également me laisser votre adresse mail, dans cette zone, pour que je puisse vous contacter.

Mieux vous connaître

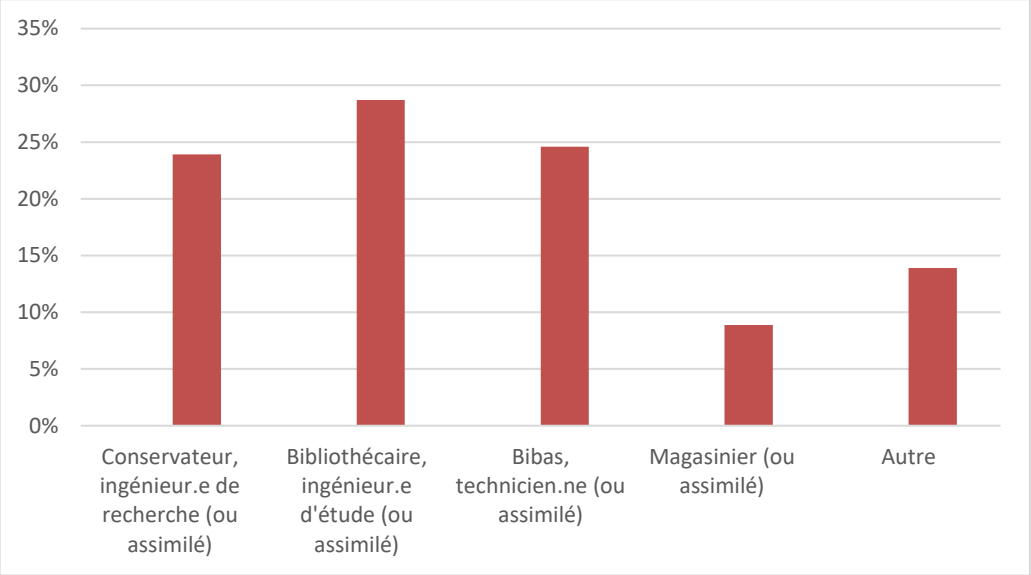
Vous travaillez dans une bibliothèque



Vous travaillez dans un service de



Vous êtes



Quelle est votre tranche d'âge ?

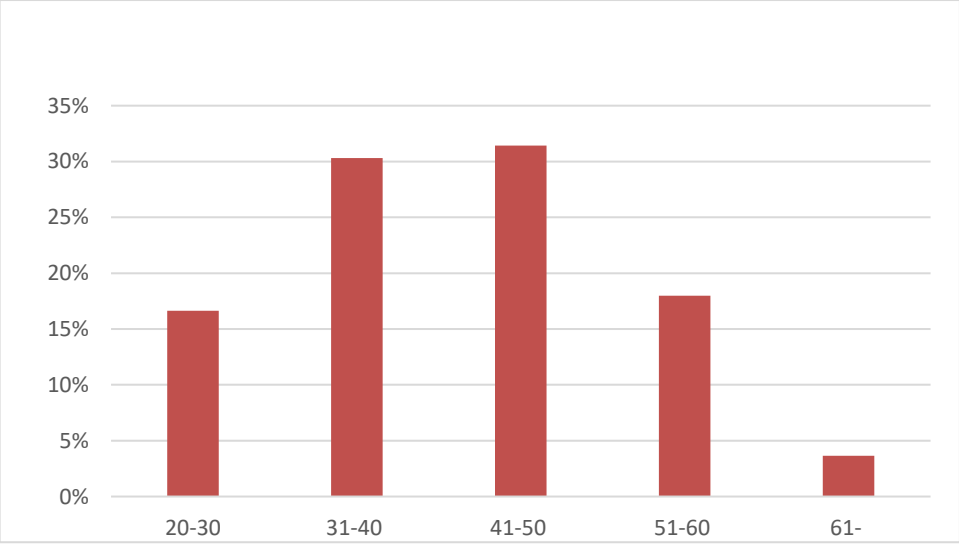


TABLE DES MATIERES