

LA GOUVERNANCE DES DONNÉES D'USAGE

ENJEUX ÉTHIQUES ET
PERCEPTIONS DES PUBLICS
DANS LES BIBLIOTHÈQUES ET ARCHIVES

Synthèse de la littérature



Institut national
de la recherche
scientifique

Institut national de la recherche scientifique
Centre Urbanisation Culture Société

Date : Août 2021

Direction scientifique

Nathalie Casemajor, PhD
Institut national de la recherche scientifique
Centre - Urbanisation Culture Société
nathalie.casemajor@inrs.ca

Co-chercheur

Guillaume Sirois, PhD
Université de Montréal
Département de Sociologie

Recherche et rédaction

Lily-Cannelle Mathieu et Alexis Morin
Stagiaires de recherche, INRS

Recherche bibliographique

Louis Melançon
Stagiaire de recherche, INRS

Diffusion :

Institut national de la recherche scientifique
Centre - Urbanisation Culture Société
385, rue Sherbrooke Est
Montréal (Québec) H2X 1E3

Téléphone : (514) 499-4000
Télécopieur : (514) 499-4065

www.ucs.inrs.ca

Révision linguistique : Carole Bourbonnais.

ISBN 978-2-89575-420-6
Dépôt légal : Bibliothèque et Archives nationales du Québec, 2021

© Les Auteurs

SOMMAIRE

RÉSUMÉ	1
INTRODUCTION	11
Contexte du projet	11
Méthodologie.....	13
1. LES DONNÉES D’USAGE : MOYEN DE CONNAISSANCE ET OBJET DE RECHERCHE..	17
Éléments de définition générale	17
La valorisation des données d’usage	18
Le champ des études de public : renouvellement par les usages numériques	20
Le champ des <i>critical data studies</i>	22
2. LA VIE PRIVÉE EN CONTEXTE NUMÉRIQUE	24
Données personnelles et données sensibles	24
La protection de la vie privée.....	25
Enjeux pour le secteur des bibliothèques et archives	28
3. GOUVERNANCE DES DONNÉES D’USAGE EN CULTURE	33
Éléments de définition générale	33
Gouvernance culturelle.....	35
Gouvernance dans le secteur des bibliothèques et archives.....	36
Gouvernance numérique.....	38
Principes éthiques en données massives, algorithmes et intelligence artificielle	39
Enjeux pour le champ culturel.....	45
Gouvernance participative et inclusive.....	46
Agir pour la littératie numérique des publics	50
Inclusion numérique : le rôle des bibliothèques.....	52

4. ENQUÊTES SUR LA PERCEPTION DES DONNÉES D'USAGE ET DE LA PROTECTION DE LA VIE PRIVÉE EN CONTEXTE NUMÉRIQUE	55
Facteurs d'influence de la perception de la vie privée	55
Le paradoxe de la vie privée dans les comportements.....	66
Enquêtes au Canada et au Québec.....	69
Enquêtes dans le contexte des bibliothèques et archives	72
Sur la perception des publics.....	72
Sur la perception des professionnels.....	74
CONCLUSION	77
ANNEXES	79
Lois, règlements et documents d'orientation pour l'encadrement de la vie privée et du droit à l'information au Québec et au Canada.....	80
BIBLIOGRAPHIE.....	91

LISTE DES TABLEAUX

Tableau 1 : Liste des mots-clés pour la recherche bibliographique	14
Tableau 2 : Extrait des résultats de recherche dans la base JSTOR.....	14
Tableau 3 : Thématiques d'analyse préliminaire du corpus bibliographique	16
Tableau 4 : Sélection de principes recommandés dans la littérature pour une gouvernance numérique éthique	42
Tableau 5 : Facteurs d'influence sur la perception de la protection de la vie privée des usagers et usagères dans le contexte numérique.....	65
Tableau 6 : Facteurs d'influence sur le comportement des usagers et usagères vis-à-vis la protection de leur vie privée dans le contexte numérique	66

RÉSUMÉ

Ce rapport présente les résultats d'une revue de la littérature menée en 2020-2021 dans le cadre du développement d'un projet de recherche partenariale avec Bibliothèques et Archives nationales du Québec. Il porte sur la gouvernance des données d'usage et ses enjeux éthiques dans le secteur des bibliothèques et archives. Plus particulièrement, il s'intéresse aux enquêtes menées auprès des usagers et usagères pour connaître leurs perceptions au sujet de la collecte, l'exploitation, le partage et l'archivage des données qui les concernent.

La première partie offre des éléments de définition des données d'usage en situant leur émergence et leur place actuelle dans les pratiques professionnelles du secteur culturel, mais aussi dans divers domaines de la recherche académique (études sur les publics de la culture, études critiques des données). La seconde partie présente les enjeux soulevés par les données d'usage relativement à la protection de la vie privée en contexte numérique, incluant les données personnelles et leur potentiel sensible. La troisième partie dégage des principes de gouvernance des données d'usage en croisant les coordonnées du secteur des bibliothèques et archives et du secteur de l'intelligence artificielle. Enfin, la quatrième partie identifie les principales variables à retenir pour mener l'enquête sur la perception des publics au sujet de la gouvernance des données d'usage, en soulignant le paradoxe qui existe entre les perceptions déclarées et les comportements effectifs des usagers et usagères en contexte numérique.

Les pages ci-dessous résument les principaux éléments à retenir, dont on trouvera une explication détaillée dans les différentes sections du rapport.

CONTEXTE – Les données d’usage



Générées par l’activité des usagers d’un service informatisé

SOURCES : compte usager, historique de recherche dans le catalogue, parcours de navigation sur le site web, médias sociaux



Les données d’usage sont constituées par les **traces d’activité** des utilisateurs et utilisatrices de services numériques, tel l’historique de recherche sur un portail documentaire. Elles permettent de connaître le comportement des publics dans les environnements numériques, incluant leurs goûts et préférences en matière de contenus culturels.

Ces données peuvent servir aux organisations qui les collectent pour :

- **mieux connaître leurs publics** : identifier des profils d’usage, repérer des modes d’engagement avec les contenus ;
- **améliorer les services de prescription culturelle** : contribuer aux stratégies de découvrabilité, de recommandation et de personnalisation des contenus ;
- **développer les publics** : cibler de nouveaux publics, fidéliser la clientèle existante.

Mais leur valorisation soulève aussi des enjeux liés à :

- la **représentation des publics**, car les données d’usage ne sont pas des traces objectives de l’activité humaine ; elles peuvent comporter des manques ou des biais, et construisent ainsi une image incomplète des publics et de leurs pratiques ;
- la **diversité des contenus** prescrits et la sérendipité (ou libre exploration) dans la découverte de nouveaux contenus culturels, sachant que la recommandation algorithmique offre au contraire des choix déjà présélectionnés ;
- la **protection de la vie privée** des usagers et usagères, étant donné la confidentialité des données personnelles qui doit être préservée, et les craintes liées à la surveillance numérique.

LA VIE PRIVÉE EN CONTEXTE NUMÉRIQUE

Un concept obsolète ?

« prendre le risque d'essayer de vivre avec l'idée que la vie privée n'existe plus »

(Thompson dans Manach, 2010)

Une définition **mouvante** et **contextuelle**

Azzaria et Zimmermann (2019)

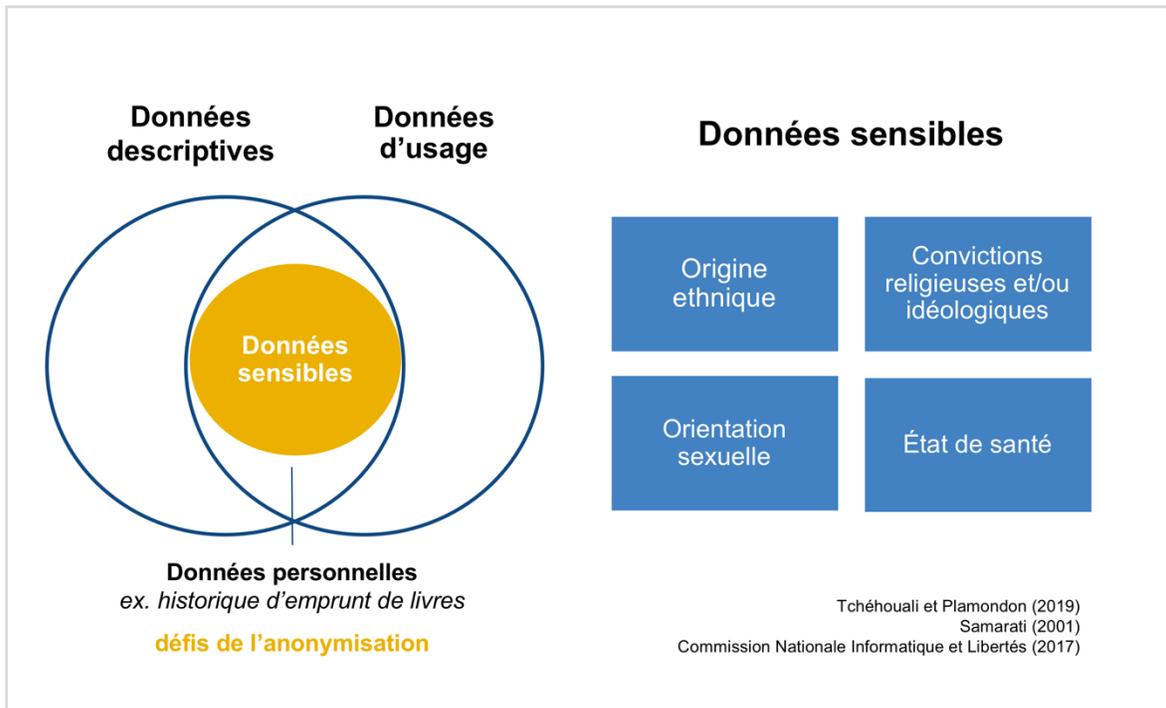
REDÉFINITION

(et non abandon) du concept de vie privée en contexte numérique

- > Capacité à **soustraire** des informations à l'**observation**
- > Possibilité de **choisir** quels renseignements personnels partager, avec qui, dans quel but, pour combien de temps.

Avec le développement des environnements numériques tels, les blogues puis les réseaux sociaux où les usagers et usagères peuvent rendre publique une part de leur intimité, **la notion de vie privée a été remise en cause.**

- Plusieurs spécialistes insistent plutôt sur la nécessité de redéfinir cette notion pour **l'adapter au contexte présent.**
- Si la notion de vie privée a évolué dans le temps, sa compréhension varie aussi entre les différentes sociétés. **Les valeurs sociales et les cultures politiques influencent la conception de la vie privée.** Ainsi, dans un pays démocratique comme le Canada, doté de lois encadrant la protection de la vie privée dans un large nombre de secteurs d'activité, les citoyen.ne.s sont plus exigeant.e.s quant à la protection de leurs données personnelles.
- Cependant, **il n'existe pas encore au Canada de réglementation spécifique encadrant les données d'usage.** Des réformes en cours sur les lois sur la protection de la vie privée au Québec et au Canada pourraient combler cette lacune.
- Plus largement, la protection de la vie privée soulève **des enjeux politiques et sociaux**, et plusieurs spécialistes plaident pour que toute nouvelle réglementation des données d'usage soit soumise au débat public.

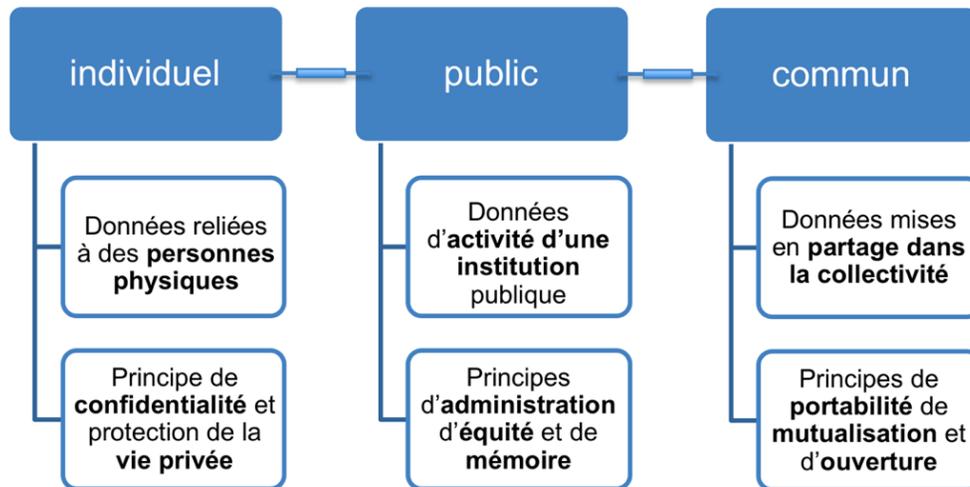


Sont considérées personnelles les données qui se rapportent à une personne physique en permettant de l'identifier.

- Par exemple, l'historique d'emprunt de documents d'un.e abonné.e de bibliothèque ayant un compte enregistré à son nom contient des informations personnelles. Cet historique est constitué par le croisement de deux types de données : des données d'usage qui décrivent les transactions (ex. date, lieu, durée de l'emprunt) et des données descriptives des documents empruntés (ex. titre, auteur).
- L'identification de la personne peut être **directe (par son nom) ou indirecte (par recoupement de plusieurs autres informations**, ce qui rend la confidentialité difficile à garantir).

Les données sensibles sont un type particulier de données personnelles qui, lorsque révélées, peuvent contraindre l'exercice des libertés fondamentales de l'individu identifié, le rendre vulnérable à la discrimination ou compromettre son intimité. Les données sensibles peuvent avoir trait, entre autres, à l'état de santé, à l'origine ethnique, aux convictions religieuses ou philosophiques ou à l'orientation sexuelle d'un individu.

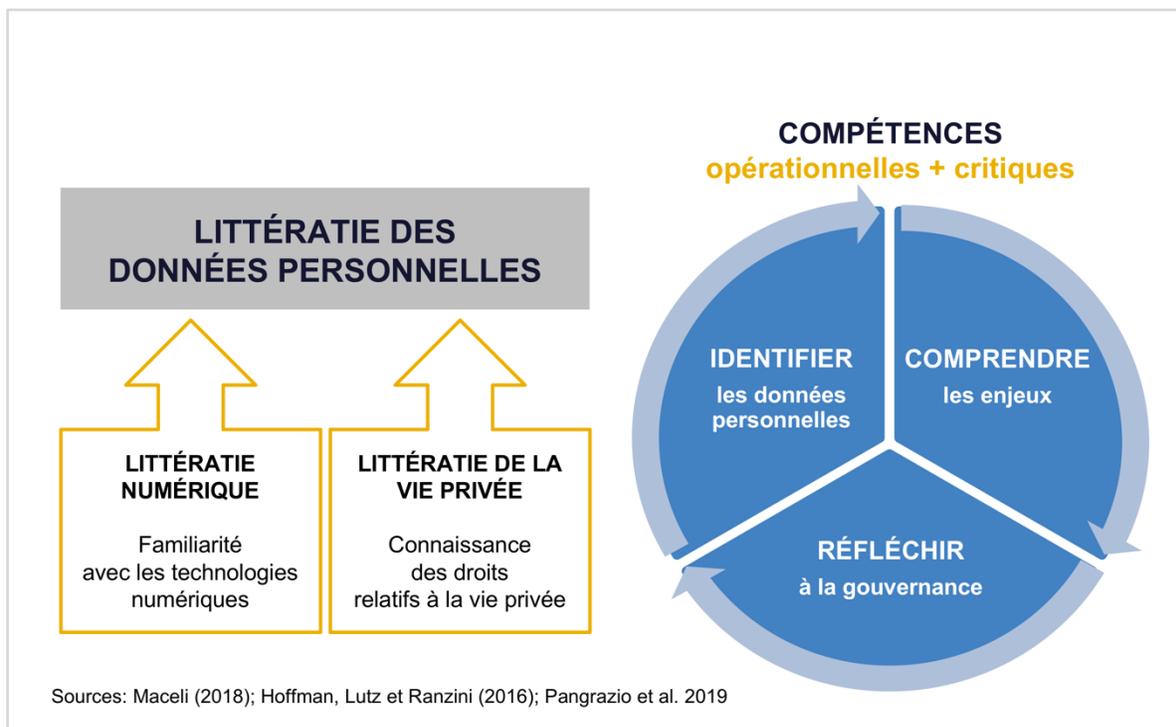
TENSION DANS LA DÉFINITION DES DONNÉES D'USAGE



Source: Cavoukian (2006); Dilhac et al. (2018); Calimaq (2018); ACEI (2020)

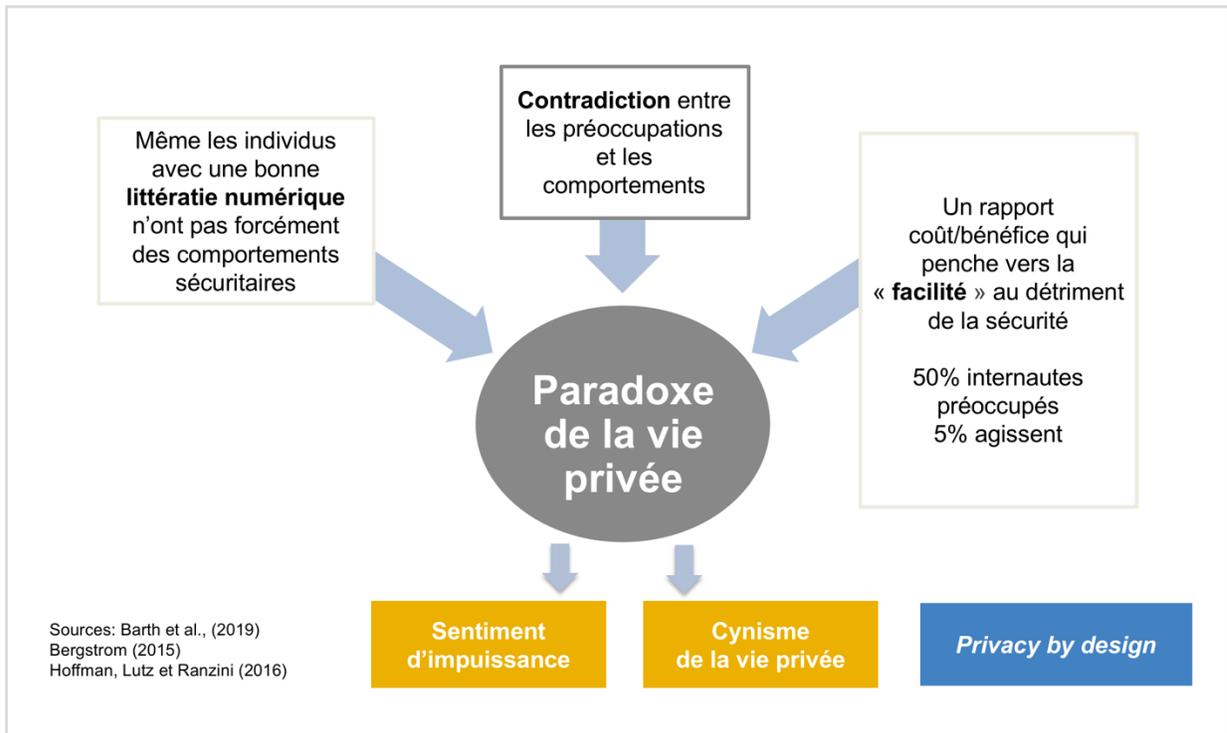
Dans le contexte d'un service public tel qu'une bibliothèque ou un centre d'archives, les données d'usage doivent être envisagées au croisement de **trois conceptions qui engagent différentes normes et manières de faire pouvant entrer en contradiction** les unes avec les autres :

- considérées **sur le plan individuel**, relativement à la personne identifiée dans ces données, elles sont soumises aux principes de protection de la vie privée ;
- considérées comme un **produit et une ressource de l'activité courante d'une organisation** fournissant un service d'intérêt général, ces données sont régies par des principes d'administration publique, d'équité dans l'offre d'accès aux services et de mémoire organisationnelle ;
- considérées comme un **bien commun qui devrait être partagé** pour enrichir la connaissance et soutenir l'innovation, les données d'usage devraient satisfaire aux principes de portabilité (capacité à être déplacées d'un système à un autre), de mutualisation dans des portails collectifs et d'ouverture à des degrés divers à la réutilisation par des tiers.



Il existe une **asymétrie d'information** entre les **organismes culturels et leurs publics** au sujet de la gouvernance des données personnelles. C'est-à-dire que les usagers et usagères sont peu au courant de la manière dont leurs données personnelles sont collectées, exploitées, partagées et archivées par ces organisations.

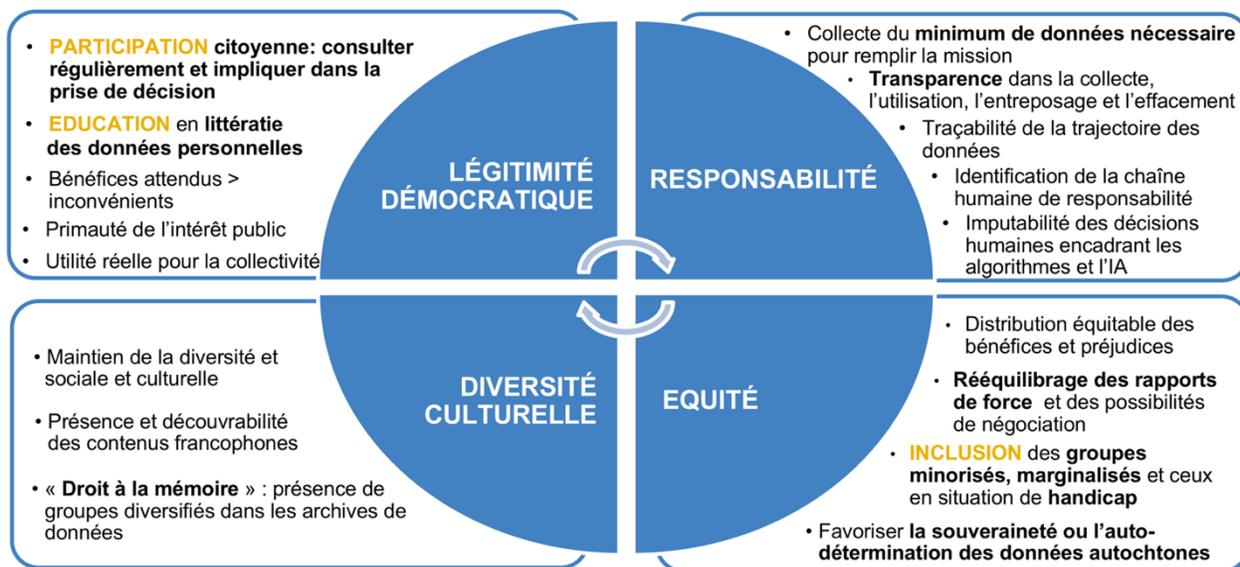
- La notion de **littératie des données personnelles** désigne les connaissances et compétences utiles pour comprendre et utiliser l'information relative à la gestion de ses données personnelles dans les environnements numériques.
- Cette notion se situe au point de rencontre entre la **littératie numérique** et la **littératie de la vie privée**.
- Les compétences visées par cette littératie sont à la fois opérationnelles (utiles pour agir) et critiques (utiles pour discerner les risques) : elles concernent la capacité à identifier la nature des données personnelles, à comprendre leurs enjeux et à réfléchir à leur gouvernance en contexte numérique.



Un haut niveau de littératie des données personnelles chez les publics **ne garantit pas qu'ils adopteront des comportements prudents** dans les environnements numériques, et ce même s'ils déclarent un fort niveau de préoccupation.

- Il s'agit d'**un paradoxe** entre les perceptions déclarées (le fait de se dire préoccupé par la gestion de ses données personnelles sur le Web) et les comportements effectifs (peu d'utilisateurs et d'utilisatrices agissent à la hauteur de leurs préoccupations).
- Cette tendance est aussi qualifiée de **cynisme**, au sens où les membres du public ressentent un sentiment d'impuissance face aux risques d'interférence dans leur vie privée, qui semblent dépasser leur capacité à se protéger.
- Face à cette contradiction, plusieurs spécialistes recommandent une approche de **protection de la vie privée en amont, dès les premières étapes de conception des services numériques (privacy by design)**, plutôt que d'essayer de mettre en place des mesures de protection en aval, une fois le service créé avec des failles potentielles.

PRINCIPES ÉTHIQUES DE LA GOUVERNANCE NUMÉRIQUE

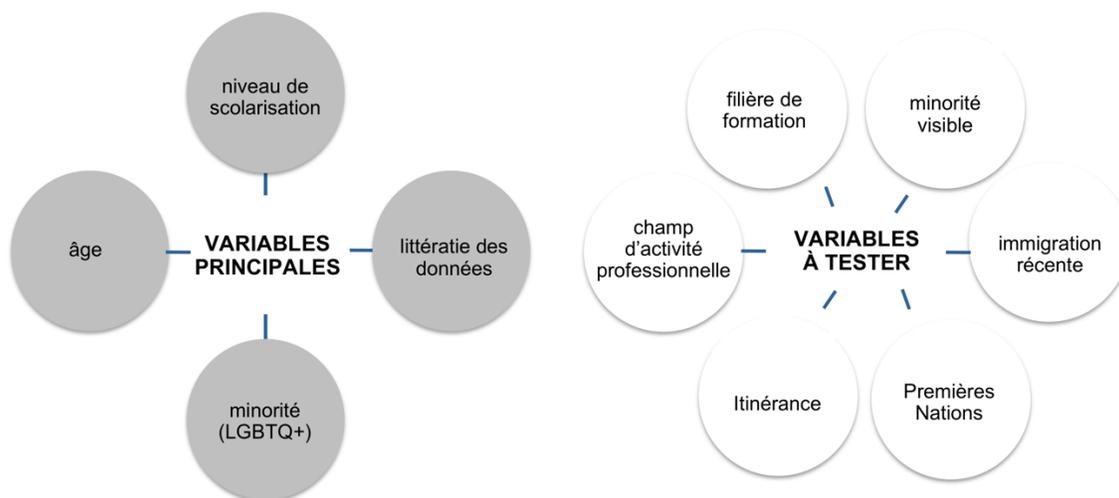


Sources: Gams (2020); Déziel et al. (2020); Tchéouali et Plamondon (2019); Dilhac et al. (2018); McDermott (2017).

Dans le tableau ci-dessus, nous proposons une **synthèse des principes éthiques à retenir** pour la gouvernance des données personnelles dans le secteur des bibliothèques et archives. Plusieurs de ces principes s'appliquent plus largement à d'autres organisations dans le secteur culturel.

- Ils ont été sélectionnés en croisant les travaux sur la **gouvernance culturelle** (en tenant compte de son virage vers la démocratie culturelle) et sur la **gouvernance numérique** (notamment dans le domaine des données massives, des algorithmes et de l'intelligence artificielle).
- Dans le cadre des travaux menés avec BAnQ, une institution publique dotée d'un mandat de diffusion et de promotion du savoir, nous avons souligné en particulier les principes de **participation citoyenne** dans la gouvernance des données d'usage, d'**éducation des publics à la littératie** des données personnelles, et d'**inclusion des populations souvent laissées en marge** des processus de gouvernance participative de par leur situation socioéconomique, leur situation de handicap ou leur appartenance à un groupe minorisé.

FACTEURS D'INFLUENCE DE LA PERCEPTION DE LA VIE PRIVÉE EN CONTEXTE NUMÉRIQUE



Diverses **enquêtes** ont été menées ces dernières années sur la perception des usagers et usagères concernant la vie privée sur Internet.

- Au Canada, on constate une **hausse des préoccupations** à ce sujet : 88 % des Canadiens.ne.s craignent que des organisations utilisent leurs données personnelles numériques pour prendre des décisions à leur sujet (Phoenix SPI, 2019).
- **Au Québec**, 50,3 % des personnes sondées estiment avoir une bonne ou très bonne connaissance du droit en matière de vie privée et ses implications sur Internet (Azzaria et al., 2019).

Notre synthèse de ces enquêtes permet d'identifier une série de **facteurs qui influencent de manière significative la perception des usagers** et usagères : le niveau de scolarisation, l'âge, le niveau de littératie numérique, l'appartenance à un groupe minoritaire (les enquêtes ont notamment porté sur des groupes LGBTQ+). Globalement, ces études montrent que les usagers plus éduqués, de plus de 35 ans, appartenant à un groupe minoritaire et familiers avec le numérique tendent à réclamer plus de protection de leur vie privée et ont des attentes plus élevées quant à la gouvernance des données d'usage.

D'autres facteurs restent à tester davantage dans le contexte des bibliothèques et archives au Canada : la filière de formation professionnelle, le champ d'activité professionnelle, l'appartenance à une minorité visible, le statut d'immigration récente (ex. réfugié.e.s), l'appartenance à une Première Nation et le statut d'itinérance (sachant que les itinérant.e.s fréquentent régulièrement les bibliothèques publiques).

INTRODUCTION

Contexte du projet

Les organismes culturels québécois ont multiplié, au cours des dernières années, les projets numériques visant à recueillir un grand nombre de données d'usage, c'est-à-dire les données générées par l'activité des usagers et usagères de leurs services (données de billetterie, données sociodémographiques, données comportementales), ce qui leur permet de connaître leurs publics de manière sans cesse plus approfondie. Le développement d'une expertise professionnelle sur les données numériques dans le domaine culturel a été fortement encouragé par les gouvernements fédéral et provincial au cours des dernières années grâce à plusieurs programmes de financement et d'accompagnement. Au Québec, le ministère de la Culture et des Communications (MCCQ) a déployé un plan d'action concernant les données sur les contenus culturels dont plusieurs mesures visent spécifiquement les données sur les publics de la culture. Cette volonté gouvernementale s'est traduite par un grand nombre de projets innovants menés par les organisations culturelles de toutes tailles. Parmi eux, l'organisme Synapse C est dédié au développement de ce que plusieurs intervenants et intervenantes culturels nomment désormais « une culture de la donnée » au service de « l'intelligence d'affaires ».

Or, si les données d'usage sont devenues l'épine dorsale des modèles d'affaires des géants du Web (Google, Apple, Facebook, Amazon, etc.), leur collecte et leur exploitation comportent un ensemble de défis pour les organismes culturels québécois. Plusieurs affaires largement médiatisées, par exemple celle de Cambridge Analytica, ou des caisses Desjardins au Québec, ont d'ailleurs sensibilisé la population aux risques du partage des données personnelles. Dans ce contexte, les organismes culturels québécois cherchent à

adopter des pratiques éthiques et responsables. Tout en profitant des possibilités offertes par les avancées technologiques, plusieurs d'entre eux souhaitent que la valorisation des données d'usage s'accorde avec la relation de confiance bâtie de longue haleine au cours des années avec leurs publics. Ainsi, les organismes culturels québécois sont de plus en plus préoccupés par la mise en place de pratiques de gouvernance des données d'usage pour mieux encadrer la collecte, l'exploitation et le partage des données d'usage.

À l'origine de ce projet se trouve l'idée que les publics sont rarement consultés au sujet de leur « mise en données », alors qu'ils sont les principaux concernés. Dans cette perspective, nous avons mené une revue de la littérature avec l'objectif de **synthétiser les travaux existants sur la gouvernance éthique des données d'usage, avec un accent particulier sur les travaux d'enquête auprès des usagers et usagères des services informatisés, et plus précisément dans le contexte des bibliothèques et archives**. Notre démarche est aussi inspirée par les travaux de Kennedy et Moss (2015) qui suggèrent de transformer les « publics connus » grâce aux données d'usage en des « publics connaissants », réflexifs et actifs, qui puissent se prononcer et agir sur leur mise en données. À ce titre, nous nous sommes intéressé.e.s aux démarches de gouvernance participative et inclusive, ainsi qu'aux enjeux de littératie des données du point de vue des publics.

Cette revue de la littérature a été menée dans le cadre d'un développement de partenariat de recherche avec Bibliothèque et Archives nationales du Québec. C'est pourquoi le secteur des bibliothèques et archives prend une place importante dans le rapport, mais plusieurs des constats tirés de la littérature peuvent s'appliquer plus largement à l'ensemble du secteur culturel. Les bibliothèques et archives se trouvent en effet à l'avant-poste de la gestion des données : d'une part, il peut compter sur une longue tradition de collecte et de gestion de l'information, d'autre part, son rôle se trouve aujourd'hui renouvelé alors qu'il est engagé dans un « virage citoyen » (Derbas, Thibodeau et Poirier, 2019). Or, au Québec, la réflexion sur les données d'usage dans les milieux culturels s'est jusqu'à présent surtout concentrée sur le secteur des arts de la

scène et sur les plateformes de diffusion en continu, en musique notamment. Il est donc urgent de réfléchir aux opportunités et défis de cette « mise en données » des publics dans d'autres secteurs tel celui des bibliothèques et archives, afin d'établir des principes éthiques et durables qui guideront le développement dans ce champ de pratiques.

Méthodologie

La collecte de données initiale a été menée en avril 2020. Une recherche systématique par mots-clés a été effectuée dans les bases de données SocINDEX, Web of Science, JSTOR et Lisa (Library and Information Science Abstracts) en ciblant les travaux publiés dans les cinq dernières années. Les mots-clés utilisés, listés ci-dessous, ont été choisis en lien avec l'objectif de recherche énoncé plus haut. Nous avons privilégié l'anglais dans un premier temps pour avoir accès aux travaux internationaux. Les requêtes dans les bases de données ont été faites par combinaison de mots-clés en utilisant des opérateurs booléens (AND, OR, * pour les lettres manquantes, guillemets pour les expressions exactes). De plus, nous avons procédé à une recherche par mots-clés dans les sites web d'une série de revues scientifiques et professionnelles en anglais et en français dans le domaine des sciences de l'information et de la bibliothéconomie : *Argus*, *Documentation et bibliothèques*, *Balisages*, *Archimag*, *Canadian Journal of Library and Information Science*.

Tableau 1 : Liste des mots-clés pour la recherche bibliographique

Thèmes	Mots-clés
PRATIQUES DE DONNÉES	big data; data; data collection; datafication; data infrastructures; data mining; data practic*; metrics; usage data
CHAMP CULTUREL	archiv*; audience; cultur* ; librarian; librairie(s);
APPROCHES DE RECHERCHE SCIENTIFIQUE	critical data studies; data studies
ENJEUX ETHIQUES ET GOUVERNANCE	audience profiling; data justice; data politics; data privacy; ethics; governance; personal data; profiling; stakeholder; privacy;

Le tableau 2 présente un extrait des résultats dans la base JSTOR. Il fait apparaître que l'enjeu de la gouvernance des données est largement documenté dans la littérature, celui de la vie privée l'est dans une moindre mesure, et encore moins dans le domaine plus précis des données personnelles et de la vie privée relative aux données. Enfin, l'expression « culture des données » est très peu répandue dans la littérature anglophone sur les bibliothèques, tout comme l'approche de l'étude critique des données, alors qu'elle est centrale dans les travaux généraux au sujet des données d'usage.

Tableau 2 : Extrait des résultats de recherche dans la base JSTOR

Mots-clés	Résultats
librar* AND data AND governance	1 848
librar* AND data AND privacy	865
librar* AND "data mining"	356
librar* AND "personal data"	156
librar* AND "data privacy"	54
librar* AND "data studies"	38
librar* AND "data culture"	2
librar* AND "critical data studies"	2

Description du corpus – Dans un premier temps, nous avons trié les résultats à partir des titres et sommaires, pour retenir une sélection restreinte de références pertinentes. Leurs bibliographies ont été analysées pour recueillir davantage de références par effet boule neige. Ainsi 250 références ont été colligées dans le logiciel Endnote. S’y sont ajoutées environ 100 références tirées de notre connaissance du champ, avec une attention particulière aux travaux francophones, ainsi qu’une trentaine de travaux publiés entre mai 2020 et juin 2021, recueillis par veille via des listes de diffusion.

Au final, **180 références ont fait l’objet d’une lecture et d’une analyse plus détaillée** dans le cadre de la rédaction de ce rapport. Ce corpus est constitué en majorité d’articles scientifiques. Il inclut également des ouvrages et chapitres scientifiques, ainsi que des compte-rendus de colloques et des rapports publiés par des agences gouvernementales ou des groupes d’intérêt au Québec, au Canada, en France et dans l’Union européenne. Les travaux universitaires proviennent en majorité des champs de spécialisation suivants : études des publics de la culture ; sciences de l’information ; bibliothéconomie ; sociologie de la culture numérique ; études des médias numériques ; études critiques des données.

La principale limite du corpus est que la recherche dans la base de données n’a pas été faite systématiquement avec des mots-clés en français. Nous nous sommes plutôt appuyé.e.s sur notre connaissance du champ et sur une veille documentaire pour couvrir ce volet de la littérature. De plus, certains thèmes de recherche ont émergé ou se sont précisés lors de l’analyse des références, tels ceux de la « perception » des publics relativement à la vie privée, du « paradoxe de la vie privée » ou de la « littératie des données ». A posteriori, ces termes auraient pu figurer dans la liste des mots-clés. La synthèse de la littérature menée par Kennedy et al. (2020c) sur un sujet connexe (la gouvernance des données dans le domaine de la santé en Grande-Bretagne) est utile à consulter en complément pour obtenir une liste détaillée de mots-clés au sujet de la perception des usagers et usagères.

Analyse des références – Lors de l’opération de triage et de consultation des résumés, les références pertinentes ont été classées par thématique, selon une première catégorisation reproduite ci-dessous, et selon un ordre de pertinence (prioritaire ; classique incontournable ; complémentaire). Les lectures prioritaires ont été divisées entre les membres de l’équipe et leur contenu discuté collectivement à partir de fiches de lecture. Le processus nous a amené à raffiner nos thématiques d’analyse, et le sommaire du rapport montre la réorganisation des contenus en lien avec ces thématiques. Nous nous sommes tout particulièrement attaché.e.s à comparer les résultats des enquêtes quantitatives et qualitatives menées auprès des publics pour sonder leurs perceptions de la vie privée. Cette analyse comparative nous a permis de faire ressortir les principales variables qui font significativement varier cette perception, dans l’optique de mener nous-mêmes une enquête à ce sujet.

Tableau 3 : Thématiques d’analyse préliminaire du corpus bibliographique

DONNÉES D’USAGE : Définition, utilisation et perception du public

- Les publics des bibliothèques et archives : en ligne et *in situ*
- Définir les données d’usage
- Utilisation des données d’usage : mesures d’impact et optimisation des pratiques professionnelles
- Mutualisation des données et données ouvertes
- Limites des données d’usage (méthodologiques, épistémologiques, pratiques)
- Risques liés aux données d’usage en bibliothèque et archives
- Perceptions du public relatives aux données d’usage et à la protection de la vie privée

GOUVERNANCE DES DONNÉES D’USAGE

- Définition et enjeux généraux
- Gouvernance dans le secteur culturel
- Enjeux spécifiques pour les bibliothèques et archives
- Participation citoyenne, fossé numérique et littératie numérique
- Gouvernance numérique
- Gouvernamentalité algorithmique
- Identité numérique, vie privée et surveillance
- Critiques de la notion de gouvernance

1. LES DONNÉES D'USAGE : MOYEN DE CONNAISSANCE ET OBJET DE RECHERCHE

Éléments de définition générale

Dans le champ de l'information numérique, on distingue habituellement deux types de données : les données dites « descriptives » ou « d'usage ». Alors que les données descriptives correspondent à de l'information de catalogage des contenus et des publics, les données d'usage (ou données transactionnelles) sont issues de l'activité numérique des usagers et usagères, c'est-à-dire de l'interaction entre un individu, l'interface d'un système et ses contenus (Tchéhouali et Plamondon, 2019).

Les données descriptives, souvent techniques ou administratives, réfèrent par exemple au numéro d'identification, à l'année de parution ou au nombre de pages d'un livre listé dans un système électronique (OCCQ 2017). Elles peuvent référer, du côté d'un.e membre du public, à un nom, un identifiant ou une adresse IP, par exemple. Les données descriptives concernant les usagers et usagères peuvent aussi s'apparenter à des données socio-démographiques telles que l'âge, le revenu ou l'activité professionnelle. On parle aussi de « métadonnées » pour désigner les informations de classification servant à caractériser d'autres données et à en faciliter la gestion. Elles sont utilisées pour décrire, enrichir et trouver d'autres données et objets culturels et médiatiques numériques (Office québécois de la langue française, 2019 ; Vaillancourt et Bisailon, 2020).

Les données d'usage, quant à elles, reposent sur des traces d'activité qui caractérisent le comportement numérique des publics et, dans le contexte de consommation culturelle tout particulièrement, leurs goûts et préférences. Le discours ambiant présentant les données d'usage comme des « mines d'or » non exploitées suscite aujourd'hui un regain d'intérêt pour ces données, non seulement de la part d'organismes commerciaux, mais aussi de la part des organismes culturels, qui auront été plus tardifs à

s’y intéresser (Moore, 2016). C’est dans cette optique que notre étude s’oriente spécifiquement sur les données d’usage, tout en considérant leur interrelation étroite avec les données descriptives.

Enfin, le terme « **données massives** » (ou « **mégadonnées** ») (*big data*) réfère aux **ensembles de très grandes quantités de données** — descriptives et d’usage — que des technologies algorithmiques permettent aujourd’hui de traiter et d’analyser en de très courts délais, notamment via des systèmes d’intelligence artificielle (apprentissage profond). Ces ensembles de données, qui ne peuvent pas être gérés avec des outils classiques de bases de données, se distinguent par leur volume, leur variété et la rapidité de leur traitement (Office québécois de la langue française, 2019). À cause de leur volume considérable, les données massives et leur traitement algorithmique sont souvent perçus comme des indicateurs fiables de la réalité, quoique la véracité de la représentation qu’ils font du monde soit contestée par certaines critiques (Gillespie, 2014).

La valorisation des données d’usage

Les données d’usage recèlent d’une grande richesse informationnelle, richesse que certaines compagnies — citons par exemple YouTube, Facebook et Netflix — ont su exploiter commercialement. Un modèle d’affaires basé sur le profilage d’usage et la recommandation algorithmique de contenus et/ou de publicités peut en effet se révéler très fructueux : **la valorisation des données d’usage permet aux organisations ayant une composante numérique de personnaliser leur offre, de cibler de nouvelles clientèles, de fidéliser leur clientèle existante et d’améliorer leurs services**. Il s’avère ainsi que la valorisation des données d’usage est une opportunité manifeste pour les organisations culturelles. Mais l’abondance de ces données d’usage confronte les organismes culturels au défi d’analyse des données massives (Amar et al., 2016).

Dans le secteur des bibliothèques et archives, la valorisation des données d’usage est envisagée comme un moyen d’améliorer les services aux publics. Une série d’études

partenariales menées avec la Bibliothèque nationale de France¹ sur l'exploitation des sessions de connexion (*logs*) et des séquences de clics (*clickstreams*) montrent que **ces données contribuent à identifier des profils d'utilisateurs et d'utilisatrices (Rollet et al., 2017) et à repérer des types d'usage et d'engagement avec les contenus** (thèmes de consultation, types de documents consultés, temps passé sur chaque document, type d'action entreprise telle que le prêt; Beaudouin et al., 2016). Ces informations permettent aussi de mieux comprendre les parcours des publics sur les sites web des institutions (Nouvellet et al., 2017; d'Alché-Buc et al., 2017; Beck, 2018) de façon à mettre en adéquation l'offre avec les différents profils d'usage.

Les données d'usage permettent également de connaître les différents niveaux de popularité des contenus des collections, et d'éventuellement repérer des effets de « longue traîne » (Benghozi et Benhamou, 2008), **contribuant ainsi aux stratégies de découvrabilité, de recommandation et de personnalisation des contenus**. Par exemple, à partir de l'historique des documents empruntés par un utilisateur ou une utilisatrice, il est possible de suggérer d'autres contenus similaires. Les bibliothèques pourraient imprimer ces recommandations sur les relevés de prêts des abonné.e.s ou leur faire parvenir par courriel lors d'un rappel d'échéance d'emprunt (Beck, 2018).

Le développement du profilage des audiences par les données est aussi alimenté par les approches marketing de segmentation des consommatrices et consommateurs culturels, orientées vers le développement de marché. Enfin, **dans une perspective managériale, les données d'usage sont aussi envisagées comme un outil de mesure d'impact des activités des organismes culturels pour évaluer et optimiser leur performance organisationnelle**. Ces nouvelles avenues de développement de public et de gestion

¹ Ce partenariat avec Télécom Paris-Tech a démarré en 2013 dans le cadre du Bibli-Lab, Laboratoire d'étude des usages du patrimoine numérique bibliothèques de la BnF.

organisationnelle sont aujourd'hui présentées comme faisant partie d'une nouvelle « culture des données » qui offrirait un avantage concurrentiel aux organisations qui fondent leurs décisions sur l'analyse des données massives (Legoux, 2019).

Toutefois, il existe des freins ou une certaine résistance au développement d'une telle « culture des données » dans les organismes culturels. Les réticences de certain.e.s bibliothécaires et archivistes face à la valorisation des données d'usage sont-elles un simple obstacle au développement d'une « culture des données » avantageuse pour tous et toutes ? Une expression de valeurs politiques liée au refus de considérer les arts comme un simple commerce ? Une « panique morale » (Moore 2016) ? Une réticence face à des pratiques managériales jugées envahissantes ? Ou sont-elles la manifestation d'une prudence historique du secteur des bibliothèques et archives (Travis et Ramirez, 2020) face à des risques pour la protection de la vie privée des publics ? Nous détaillerons dans les sections suivantes les différents enjeux de la valorisation des données d'usage tels qu'ils se dégagent dans la littérature scientifique.

Le champ des études de public : renouvellement par les usages numériques

Outre son développement dans les pratiques professionnelles, du côté de la recherche, **l'analyse des données d'usage a stimulé la curiosité scientifique et transformé les modes d'enquête dans le champ des études d'usage en bibliothèque et archive** (Jauréguiberry et Proulx, 2011 ; Souchier et al., 2013), suscitant par là même un renouvellement de ce champ établi de longue date (Jahjah, 2017). Plus largement, l'étude des usages numériques et des nouveaux rapports entre publics en ligne et *in situ* a fait évoluer le champ des études des publics de la culture (Donnat, 2016 ; Beaudoin et Denis, 2016). Remarquons par ailleurs que les nouveaux outils numériques de connaissance des publics permettent aux institutions culturelles d'inventer une relation nouvelle avec leurs publics, guidée par des principes d'ouverture, d'échange et d'adaptation aux publics,

délaissant la traditionnelle posture institutionnelle de « sachant » qui fonde maintes accusations d'élitisme envers les structures culturelles (Caillet, 2016).

En Grande-Bretagne, les données compilées par Audience Finder, qui mutualise les données d'usage et les données démographiques des publics de plus de 800 organismes culturels à travers le pays, ont donné lieu à une série d'études sur le potentiel des données massives pour les études de public (Hadley et al., 2019). Par exemple, l'analyse des données de billetterie en ligne peut apporter une compréhension plus fine de pratiques culturelles « de niche » et compléter ainsi les informations tirées des grandes enquêtes nationales sur les pratiques culturelles (Hanquinet et al., 2019). **La granularité dans l'analyse des comportements permise par les données d'usage a même conduit certains auteurs à évoquer une nouvelle approche « post-démographique » des pratiques culturelles** pour souligner les limites des catégories traditionnelles construites à partir des groupes démographiques (Rogers, 2009 ; Ashton et Gowland-Pryde, 2019).

L'approche algorithmique de ces études de public comprend pourtant elle aussi certaines limites, notamment le fait que les bases de données sur lesquelles se basent les algorithmes ne sont pas complètes. **Gillespie (2014) critique d'ailleurs le mythe de la représentation algorithmique objective des publics en parlant de « publics construits ».** Additionnellement, l'auteur remarque l'impact de la présentation algorithmique du public sur le sens du soi des membres le constituant. Soulignons à ce propos que l'utilisation des données numériques inspire maintes critiques, les plus significatives étant synthétisées dans la section suivante.

Dans un autre ordre d'idées, le rapide développement des travaux critiques et empiriques à propos des données d'usage comme source d'information sur la participation numérique suscite de nouveaux croisements entre le champ des études des pratiques culturelles et celui des audiences médiatiques (Das et Brita, 2018). Ytre-Arne et Das (2019) notent qu'au sein de ces champs d'études croisés, **plus d'attention devrait être portée aux inégalités de pouvoir entre les plateformes médiatiques et leurs publics, aux**

nouvelles littératies et stratégies d'adaptation de ces derniers face à un quotidien culturel devenu numérique et, enfin, aux expériences d'usage fondamentales, telle que la lecture ou le visionnement d'une vidéo, plutôt qu'à la singulière expérience de production de données (souvent nommée *produsage*).

Le champ des critical data studies

Si les nouvelles possibilités ouvertes par l'analyse des données massives suscitent l'enthousiasme de nombreux spécialistes, divers travaux ont néanmoins pointé un ensemble de limites et de critiques concernant les données massives, les algorithmes et les applications en intelligence artificielle, donnant naissance à un nouveau champ d'étude baptisé *critical data studies* ou études critiques des données (Crawford et al., 2014 ; Kitchin et Lauriault, 2014).

Dans ce nouveau champ, un premier ensemble de travaux concerne les limites méthodologiques et épistémologiques des données d'usage. Plusieurs études soulignent que les données d'usage en bibliothèque ne captent qu'une partie limitée des pratiques du public, et recommandent dès lors de combiner l'analyse statistique des données d'usage avec une démarche qualitative d'entretiens individuels ou collectifs afin d'obtenir un portrait plus global des publics et de leurs usages (Jamali et al., 2005 ; Beaudouin et al., 2016). Plus généralement, face à un engouement pour l'analyse des données massive qui cède parfois le pas à une fétichisation des données comme représentation objective du monde, **il est important de rappeler que les données d'usage ne sont pas des traces objectives de l'activité humaine : elles sont toujours construites par l'intermédiaire d'un dispositif de collecte, de traitement et d'information pouvant induire des biais** (Gitelman, 2013). Une autre confusion entretenue par le comportementalisme algorithmique tient au glissement entre corrélation de variables et causalité, confusion qui teinte certains travaux d'analyse statistique des données massives (Cardon, 2015). C'est-à-dire qu'un lien apparent entre deux types de données (ex. le lieu d'habitation d'un

usager ou d'une usagère et son historique d'emprunt de documents) ne veut pas nécessairement dire qu'il y a un lien de cause à effet entre les deux.

Un second ensemble de travaux dans le champ des *critical data studies* pertinent pour notre démarche se penche sur les conséquences socio-politiques d'un monde gouverné par les données et leurs métriques. Les dispositifs de collecte et de valorisation des données y sont envisagés comme des assemblages techno-culturels qui produisent de nouvelles formes culturelles contemporaines (Beer et Burrows, 2013 ; Kennedy, 2015), suscitant l'émergence d'une nouvelle « culture algorithmique » (Striphas, 2015 ; Dourish, 2016 ; Seyfert et Roberge, 2016). Du côté des analyses politiques, la littérature académique a abondamment documenté les risques d'une surveillance accrue des citoyens et citoyennes sur Internet via la collecte et l'analyse des données personnelles (Bennet et Parsons, 2013), un phénomène qualifié de « *dataveillance* » (Van Dijck, 2014). **Les applications de surveillance, tout comme les dispositifs de prédiction et de prescription des choix dans les environnements numériques, véhiculent des normes sociales sous-jacentes qui peuvent mener à des biais d'interprétation, voire à la reproduction d'inégalités et de discriminations** (Pasek et al., 2019 ; Apprich et al., 2018).

Le profilage des consommateurs et consommatrices par les données personnelles a aussi été décrit comme un processus instrumental et économique qui institue de nouveaux modes de capture, de régulation et de gouvernement des comportements quotidiens (Elmer, 2003). **Plusieurs travaux suggèrent que les données massives contribuent ainsi à une « gouvernamentalité algorithmique » où les décisions politiques sont fondées non sur des débats publics, mais sur des corrélations de données et des modélisations de comportements** (Rouvroy et Berns, 2013 ; Cardon, 2015 ; Badouard et al., 2016). Considérant leur tendance à orienter la prise de décision vers la performance quantifiable, ces modes de gouvernance fondés sur l'analyse de données massives ont été qualifiés de nouvel ordre de pouvoir biopolitique et néolibéral (Beer, 2015 ; Beer, 2016).

2. LA VIE PRIVÉE EN CONTEXTE NUMÉRIQUE

Données personnelles et données sensibles

Parmi les différents enjeux soulevés par la valorisation des données d'usage, notre projet s'intéresse en particulier à ceux qui ont trait aux données personnelles et à la protection de la vie privée. Au Québec, la *Loi sur la protection des renseignements personnels dans le secteur privé (L.R.Q. P-39.1)* définit les données personnelles comme « tout renseignement qui concerne une personne physique et permet de l'identifier ». Ainsi, **tant les données descriptives que les données d'usage associées à un usager ou une usagère identifiable peuvent être qualifiées de « personnelles ».**

La confidentialité des données personnelles est protégée par diverses lois à l'échelle provinciale et fédérale (voir l'annexe « Lois, règlements et documents d'orientation pour l'encadrement de la vie privée et du droit à l'information au Québec et au Canada »). Certaines institutions, comme Bibliothèque et Archives nationales du Québec (BAnQ), se sont également dotées d'une politique de protection des renseignements personnels (*Politique d'accès à l'information et protection des renseignements personnels*), mais la portée de celle-ci est centrée sur la protection des renseignements personnels de ses employés.e.s.

Le Parlement européen et la Commission nationale française de l'Informatique et des Libertés (CNIL) spécifient que **l'identification de la personne physique peut être directe comme indirecte et qu'elle peut être effectuée par recoupement de plusieurs informations** telles qu'un nom, un numéro d'identification, une localisation géographique, un identifiant électronique et d'autres informations plus spécifiques à l'identité sociale ou physique d'une personne. Par exemple, si l'historique de recherche d'un usager ou d'une usagère dans le catalogue numérique d'un centre d'archive peut être associé à son nom via un compte d'abonné, les données de l'historique sont considérées comme personnelles. Compte tenu de l'existence de divers moyens

techniques d'identification des données numériques et de l'absence d'une technique d'anonymisation universelle, **la confidentialité des données personnelles s'avère très difficile à maintenir, d'où la demande que formulent certain.e.s analystes de minimiser la génération et la collecte de données** (Gambis, 2020 ; Bowers, 2006).

L'enjeu de la confidentialité des données personnelles est particulièrement grand en ce qui a trait aux **données sensibles, un type de données personnelles qui, lorsque révélées, peuvent contraindre l'exercice des libertés fondamentales de l'individu identifié ou le placer dans une situation indésirable** (Samarati, 2001). La CNIL explique que **les données sensibles peuvent avoir trait, entre autres, à la santé, à l'origine ethnique, aux convictions religieuses ou philosophiques ou à l'orientation sexuelle d'un individu**. La collecte, la génération, l'utilisation, la communication et l'entreposage de données sensibles — descriptives ou d'usage — pouvant être associées à un usager ou une usagère numérique sont donc, selon plusieurs travaux, des activités qui devraient être hautement sécurisées (Déziel et al., 2020).

La protection de la vie privée

Alors que la protection des données personnelles est assurée par la loi, la protection de la vie privée est identifiée comme un « droit fondamental » et une « valeur de base » au Canada et au Québec (Commissariat à la protection de la vie privée du Canada [CPVPC], 2019 ; Charte québécoise des droits et libertés de la personne, 1975). Or, très peu de mesures y assurent la confidentialité et la protection des données d'usage. Cette absence de réglementation encadrant les données d'usage semble être due à une combinaison de facteurs.

Soulignons tout d'abord que les données d'usage étant un type d'information et une source potentielle de violation de la vie privée très spécifique dont le développement est relativement récent, il est compréhensible qu'elles ne soient pas ciblées par les cadres législatifs préexistants. Notons à cet égard que la Commission d'accès à l'information du

Québec cherche à repenser la protection des renseignements personnels à la lumière des défis soulevés par l'intelligence artificielle (Déziel et al., 2020) et que **le Commissaire à la protection de la vie privée du Canada « réclame depuis plusieurs années une réforme fondamentale des lois sur la protection des renseignements personnels dans les secteurs privé et public au Canada »** (CPVPC, 2019 : 2).

Toutefois, certaines voix critiques notent que bien que la surveillance, ou la *dataveillance*, soit aujourd'hui généralement exercée à des fins commerciales plutôt qu'à des fins de sécurité publique, plusieurs incidents récents ont révélé de proches connexions entre l'industrie de l'information et certains gouvernements, dont celui des États-Unis. Selon Peacock (2014), cette affinité d'intérêt entre les acteurs étatiques et privés serait une des raisons pour lesquelles l'industrie des données est peu réglementée.

Notons de plus que la manière dont les données d'usage peuvent se qualifier comme « personnelles » — et ainsi requérir une protection légale — est peu définie et vraisemblablement peu comprise. En effet, il semblerait que le caractère « personnel » de certaines données d'usage soit contextuel plutôt que définitif, une caractéristique rendant leur légifération ardue. De plus, les mécanismes technologiques permettant de relier directement des données d'usage à une personne physique sont multiples et leur compréhension requiert des habiletés techniques avancées. Ceci a pour effet que les données d'usage sont, de manière générale, très peu reconnues comme des données personnelles et, conséquemment, peu protégées comme telles. Déziel et al. (2020) suggèrent à ce titre que **la loi québécoise devrait établir un critère précis permettant d'établir selon quelles spécificités un renseignement est personnel ou dépersonnalisé, et, additionnellement, que la loi devrait explicitement reconnaître les évaluations, inférences et prédictions comme des renseignements pouvant être « personnels »**.

Enfin, nous relevons que **la notion de « protection de la vie privée », comme le confirme le Commissariat à la protection de la vie privée du Canada (2019), est difficile à définir et relève de valeurs normatives établies de manière contextuelle par une société et ses**

individu.e.s. Ainsi, et bien que ce même Commissariat affirme que la protection de la vie privée est une « valeur de base » de la société canadienne, la littérature scientifique démontre que l'étendue et les modalités de l'encadrement de la vie privée sont des enjeux normatifs devant être sujets à débat public. La législation de la vie privée repose en outre sur des décisions orientées par des idéaux politiques et des valeurs culturelles plutôt que par des principes universellement acceptés (Dilhac et al., 2018).

L'utilité même des débats tenus autour de la protection de la vie privée est cependant remise en question par certains spécialistes internationaux et dirigeants d'entreprises technologiques, qui proclament qu'au 21^e siècle, le concept de la vie privée n'aurait plus lieu d'être — qu'il s'agirait d'un concept obsolète. Ainsi Thompson (cité dans Manach, 2010) est de l'opinion qu'il faut « prendre le risque d'essayer de vivre avec l'idée que la vie privée n'existe plus », Bloche et Verbère (2011) observent quant à eux que la protection de la vie privée ne semble plus être un « élément essentiel au bien-être des peuples ». Mark Zuckerberg, président et directeur général de Facebook, a également affirmé que la vie privée n'est plus « une norme sociale » (Johnson, 2010).

Azzaria et Zimmermann (2019) relativisent toutefois ces déclarations, qu'ils jugent être subjectives et teintées d'une perspective idéologique. Selon eux, **un changement épistémologique s'est effectivement opéré autour de la notion de la vie privée, mais il s'agirait d'une redéfinition, plutôt que d'un abandon du concept.** Ils soutiennent que la vie privée ne peut plus être perçue comme une notion fixe et univoque et qu'une telle conceptualisation de la vie privée cède naturellement à une définition plus contemporaine. Dans cette perspective, **plusieurs proposent de redéfinir la protection de la vie privée comme un droit collectif, et non individuel, afin d'insister sur le statut de la donnée comme bien commun plutôt que sur les bénéfices individuels que les membres du public ou les organisations peuvent en tirer** (CNIL, 2017 ; Villani, 2018 ; Calimaq, 2018).

Ainsi, le concept de vie privée est sujet à une négociation incessante qui est alimentée par la multiplicité sociale et la complexité technologique caractérisant notre époque. Il apparaît donc que la définition de la vie privée est variable et que les mesures à établir pour la protéger ne font pas consensus. **Nous remarquons toutefois une tendance publique favorisant un renforcement de la protection des données numériques** (Phoenix SPI, 2016 ; Azzaria et Zimmermann, 2019), tendance très vraisemblablement alimentée par l’affaire Cambridge Analytica en 2018, les débats actuels en lien aux applications de traçage du virus COVID-19 et, au Québec, la fuite de données de Desjardins en 2019. **Ces observations nous mènent au constat que tout encadrement réglementaire ou légal des données d’usage devrait être soumis à débat public.**

Enjeux pour le secteur des bibliothèques et archives

Outre les enjeux généraux de la valorisation des données d’usage mentionnés dans la section précédente, certains enjeux sont plus spécifiques au milieu des bibliothèques et archives. Ces enjeux concernent : **une asymétrie d’information entre les bibliothèques et leurs publics ; une tension entre la liberté de s’informer et la surveillance des usagers et usagères à des fins de sécurité publique ; une opposition normative entre la donnée comme propriété individuelle, institutionnelle ou commune ; le contraste entre la valorisation algorithmique des données d’usage et un accès à l’information plurielle et au choix non prédéterminé.**

Larson (2019) souligne que la plupart des bibliothèques ayant implanté des bornes d’emprunt de livres en libre-service (*self check-out*) au début des années 2000 n’avaient pas sondé les membres du public avant d’implanter cette technologie, ce qui a soulevé des craintes quant à la protection de la vie privée des usagers et usagères (Sturges et al. 2003; Mathson et al., 2007 ; Bowers, 2008). De plus, Affonso et Sant’Ana (2018) démontrent que **la collecte de données en ligne dépasse généralement ce qui est annoncé dans les politiques de confidentialité des bibliothèques** — quand celles-ci

existent et qu'elles sont publiques. Au moment de l'étude d'Affonso et Sant'Ana en 2017, la majorité des bibliothèques n'affichaient pas de politique de confidentialité sur leur site. Les auteurs remarquent aussi qu'en plus de ne pas rendre publique une description exhaustive de leurs processus de collecte de données, les bibliothèques n'organisent généralement pas leurs interfaces d'usage numérique de manière à rendre l'information ayant trait à ces collectes intelligible et facilement accessible. Ajoutons que l'opacité et l'abstraction des réseaux de télécommunication et des systèmes de production et d'analyse des données d'usage contribuent à ce manque de transparence général des bibliothèques et autres institutions culturelles envers leurs publics.

Il existe ainsi une asymétrie d'information entre les bibliothèques et leurs publics concernant la collecte des données d'usage, avec en corollaire une perte de contrôle de la protection de la vie privée pour les usagers et usagères. Alors que le concept d'« asymétrie informationnelle » est généralement utilisé en référence à un déséquilibre de capital informationnel entre les plateformes internationales telles les GAFAM et les acteurs gouvernementaux ou privés ayant moins de ressources informationnelles que les « géants » de l'industrie (Tchéhouali et Plamondon, 2019 ; Cliche, 2017), nous faisons ici référence à l'asymétrie entre les organisations ayant une présence numérique — qui disposent des données de leurs publics *et* des informations ayant trait à la collecte de ces données — et les membres du publics, qui ne comprennent ou n'ont souvent pas accès à ces mêmes informations et savoirs. La question se rapporte ainsi à un manque de transparence organisationnelle et à l'enjeu citoyen du manque de littératie numérique.

Dans un autre ordre d'idées, nous relevons une tension entre la liberté de s'informer et la surveillance d'usage employée sous le couvert de la sécurité publique. Suite à l'arrestation, en septembre 2016, d'un homme ayant consulté des sites djihadistes à partir de l'ordinateur d'une bibliothèque publique de Marseille, l'Association des Bibliothécaires de France a émis une prise de position déclarant que les bibliothèques devaient rester un espace de liberté où tous et toutes ont le droit de s'informer librement (Association des bibliothécaires de France [ABF], 2017). Bien que le « délit de lecture » de

cet homme fût finalement annulé par le Conseil Constitutionnel au nom de la protection des droits fondamentaux de *liberté de conscience* et de *liberté d'expression et de communication* (Le Figaro, 2017), cet incident a mis en relief **un enjeu d'utilisation des données d'usage propre aux bibliothèques, qui, remarquons-le, se veulent de prime abord être une porte d'accès à l'information libre et sans discrimination** (ABF, 2018).

D'autres cas mettant en relation la surveillance étatique et les bibliothèques publiques s'additionnent aux États-Unis depuis la promulgation, en 2001, du **USA Patriot Act, qui, en réponse aux événements terroristes de 2001, permet au gouvernement états-unien de surveiller les lectures et activités des publics des bibliothèques du pays à des fins de sécurité publique** (Shaffer, 2014). Bien que plusieurs bibliothécaires rapportent avoir refusé de collaborer, au temps de la Guerre Froide, aux activités de surveillance étatique au nom de la liberté intellectuelle et de l'accès libre à l'information, le *Patriot Act* de 2001 a renforcé les pouvoirs de l'État en ce sens et empêche même les usagers et usagères de savoir qu'ils ont été soumis à une surveillance d'usage (Bowers, 2006). Plus récemment, plusieurs bibliothèques, dont les administrateurs et administratrices craignaient un élargissement de la politique de surveillance nationale suite à l'élection du républicain Donald Trump à la Maison Blanche, ont accru de manière préventive leurs politiques de protection de la vie privée (Thielman, 2016).

Le Canada n'a pas été à l'abri avec le dépôt du projet de loi C-51 ou Loi antiterroriste en 2015 (Beck, 2018). Mise en place par le gouvernement majoritaire conservateur, cette loi visait à protéger les Canadiens et Canadiennes en facilitant le partage d'information entre les institutions gouvernementales pour une surveillance accrue. L'Association canadienne des bibliothèques avait commenté cette décision par l'entremise d'une déclaration publique (Beck, 2018). Sans nier l'importance de la sécurité intérieure, l'association avait des préoccupations à l'égard des risques pour la vie privée et la liberté d'expression des citoyens et citoyennes. Elle souhaitait donc des consultations et des audiences pour qu'une plus grande diversité de perspectives et d'opinions soient entendue (CLA, 2015), mais cet appel n'a pas été entendu par le gouvernement.

Comme l'illustrent ces exemples, **la surveillance des usages numériques des citoyens et citoyennes réalisée à des fins de sécurité publique peut entrer en conflit avec le droit à l'information, droit qui constitue un des principes fondamentaux de la bibliothèque publique.** De là émerge une problématique questionnant les rapports entre sécurité publique et liberté. À ce sujet, certain.e.s proposent qu'augmenter l'un rogne nécessairement sur l'autre – plus de liberté signifierait moins de sécurité, et vice-versa (Chouet, cité dans Boisselet, 2018). Les bibliothèques se retrouvent donc au cœur d'un débat politique requérant un positionnement sociétal sur l'importance relative de la liberté et de la sécurité publique. Une réflexion de fond s'impose donc sur l'utilisation qui peut être faite des données d'usage de leurs publics.

Un autre enjeu ayant trait aux données d'usage dans le secteur des bibliothèques et archives concerne **l'opposition normative entre la donnée comme bien individuel dont la confidentialité doit être protégée, la donnée comme bien institutionnel qui sert à des fins administratives pour fournir un service public, et la donnée comme bien commun devant répondre aux principes d'ouverture et de transparence.** Puisque les données d'usage peuvent être reliées à des personnes physiques par diverses techniques qui sont peu comprises par le public et par les décideurs, **plusieurs experts réclament la primauté du principe de confidentialité et de protection de la vie privée** dans la collecte et le traitement des données d'usage (Cavoukian, 2006; Dilhac et al., 2018 ; Autorité canadienne pour les enregistrements Internet (ACEI), 2020). *A contrario*, **plusieurs archivistes soulignent que la donnée, comme l'archive, est un bien collectif dont l'ouverture et l'authenticité contribuent au « droit à la mémoire » et à l'évitement d'une « amnésie collective »** (Calimaq, 2018).

Ainsi s'opposent un paradigme individualiste du droit aux données personnelles et un paradigme collectiviste du droit « social » aux données ouvertes et à l'information publique. Notons à ce propos que dans le secteur de la culture, au Québec, et tout particulièrement dans le contexte actuel de pandémie forçant les institutions culturelles à renouveler leur approche du public, plusieurs acteurs soulignent les bénéfices de la

mutualisation et du partage des données d'usage provenant de différentes organisations culturelles (Wylie, 2021; Legoux et Duceppe, 2020; Lefebvre et Bélanger, 2020). Il apparaît donc que les développements technologiques se rapportant aux données d'usage et à leur valorisation provoquent une mutation de certains paramètres de l'accès à l'information dans le secteur des bibliothèques et archives, qui se voient complexifiés par la tension entre bénéfices publics et droits individuels.

Enfin, nous remarquons que la **promesse d'un accès libre et non-discriminant à un Internet neutre et à une information plurielle que font les bibliothèques (Association des bibliothèques publiques du Québec [ABPQ], 2019; ABF, 2018)** ne peut pas nécessairement être tenue si les algorithmes de recommandation fondés sur l'analyse des données d'usage enferment les membres du public dans des profils d'usage architecturant l'offre du contenu culturel leur étant faite et, ultimement, pré-formulant leurs choix (Dilhac et al., 2018). Une valorisation exacerbée des données d'usage en bibliothèque pourrait en effet faire entrave au principe de sérendipité qui caractérise, pour Umberto Eco (cité dans Dilhac et al., 2018), l'expérience de la bibliothèque; ces découvertes fortuites, faites par hasard dans la bibliothèque, se révèlent souvent des plus intéressantes.

La valorisation des données d'usage, dans le secteur des bibliothèques et archives, soulève donc de nombreux enjeux devant être analysés pour une meilleure compréhension des paramètres de gouvernance qui encadrent la prise de décision concernant ces données ainsi que la mise en débat de leurs potentiels et limites.

3. GOUVERNANCE DES DONNÉES D'USAGE EN CULTURE

Éléments de définition générale

La gouvernance des données d'usage réfère aux processus décisionnels entourant la collecte, l'exploitation, le partage et l'archivage des données issues de l'activité des utilisateurs d'un système informatisé au sein d'une organisation. Elle établit les rôles et responsabilités des différentes parties prenantes concernées (telles l'organisation elle-même, les fournisseurs de services tiers, les usagers) en formalisant des politiques, des normes et des procédures de gestion des données et en surveillant leur conformité dans la durée (Abraham et al., 2019). Les divers acteurs impliqués collaborent pour définir un ensemble d'objectifs, de valeurs et de moyens pour organiser la prise de décision.

Différents paliers d'encadrement et de régulation sont impliqués dans la gouvernance des données d'usage (voir en annexe pour une liste plus exhaustive) :

- 1) **les procédures et règlements internes** propres à l'organisation (par exemple, à BanQ, la *Politique de confidentialité* pour les services fournis sur place et en ligne);
- 2) **les documents de référence professionnels** qui établissent des codes, chartes ou meilleures pratiques pour l'ensemble du secteur (tel le *Code d'éthique de la Fédération Canadienne des associations de bibliothèques*);
- 3) **les lois provinciales et fédérales** (dont la *Loi sur la protection des renseignements personnels* au Canada).

De plus, la littérature souligne **l'importance d'inclure la société civile dans les mécanismes de gouvernance des données** (Micheli et al., 2020; Godinho et al., 2021) : à l'interne, en sollicitant les usagers d'une organisation, et à l'externe, en suscitant des occasions de débat public.

Dans le secteur des bibliothèques et archives, la valorisation des données d'usage croise **les enjeux de la gouvernance culturelle** (qui concerne notamment les institutions publiques dans le secteur de la culture) **et ceux de la gouvernance numérique**. Cette dernière caractérise les relations entre acteurs engagés dans le développement des pratiques et infrastructures numériques et dans les débats publics entourant ces technologies. Les principes à retenir dans ce contexte devraient donc tenir compte de cette double affiliation.

D'un point de vue plus général, la littérature montre que **le terme de gouvernance s'est imposé au cours des deux dernières décennies pour caractériser un tournant dans les processus décisionnels traditionnels**. Sous l'effet de changements sociopolitiques, un certain « déplacement de l'autorité » (Rosenau et Czempiel, 1992) a entraîné une extension des manières de gouverner, privilégiant le passage de rapports hiérarchiques à des processus horizontaux (Schmitter, 2001), mais aussi le fait de varier les formes de processus décisionnels (Kooiman, 2003) et de considérer une multitude de niveaux décisionnels entremêlés (Marks, Hooghe et Blank, 1996). Au Québec, le développement de la gouvernance a été marqué par le dynamisme communautaire et la « citoyenneté active », qui se sont développés dans le contexte de la construction de l'État québécois dans les années 1970 (Hamel et Jouve, 2006). **La littérature documente aussi plusieurs critiques de la gouvernance en tant que démarche décisionnelle** : elle est décrite comme fortement associée au tournant néolibéral (Brown, 2015), à l'envahissement de la doxa managériale (Offe, 2009) et à la production d'un espace dépolitisé qui annihile les rapports conflictuels (Fawcett et al., 2017).

Bien qu'il existe de multiples définitions du terme gouvernance, certains éléments communs peuvent être identifiés (Padovani et Pavan, 2011) : **il s'agit de processus décisionnels dans lesquels une multiplicité d'individus et de groupes — dont les niveaux de pouvoir, d'autonomie et de légitimité varient — interagissent de manière formelle et informelle pour tenter d'influencer le résultat du processus**.

Ainsi, la notion de gouvernance permet de penser la variété des processus, des acteurs, des actrices et des objets impliqués dans les processus décisionnels, tout en soulevant l'enjeu des rapports de pouvoir entre les différentes parties prenantes impliquées (ou non-impliquées) dans une démarche de gouvernance. Dans l'analyse des processus de gouvernance, **une attention particulière doit donc être portée à la manière dont l'influence et le pouvoir décisionnel sont distribués entre des individus et des groupes positionnés à des niveaux d'autonomie et de légitimité différenciés, voire inégaux.**

En résumé, nous définissons la gouvernance des données d'usage à BAnQ comme **la mise en œuvre de processus décisionnels qui incluent la perspective et l'engagement de multiples acteurs issus de groupes diversifiés, la mise en œuvre d'un encadrement des données d'usage et la mise en débat des pratiques liées à ces données au sein de l'institution et dans la sphère publique.**

Gouvernance culturelle

Dans la littérature francophone, le terme de gouvernance culturelle est souvent associé à l'étude des politiques culturelles dans leur rapport à différentes échelles territoriales (Saez, 2004 ; Négrier et Tellier, 2020). Par contre, comme dans d'autres domaines, la gouvernance culturelle ne connaît pas de définition stabilisée (Valentine, 2017). Or, **l'application du concept de gouvernance au domaine culturel pose un certain nombre de questions reliées aux enjeux identitaires qui marquent les rapports à la culture.** En effet, puisque la gouvernance implique l'apport d'un ensemble de parties prenantes dans les processus décisionnels, elle vient compliquer les processus de définition de la « culture légitime », alors que plusieurs groupes minoritaires revendiquent désormais la légitimité de leur identité (Sirois, 2018) et leur droit à participer à l'élaboration des politiques culturelles locales (Marx, 2019).

Ainsi, la gouvernance culturelle est le corollaire du passage d'une démocratisation de la culture, qui impliquait d'amener la culture légitime déterminée par les élites au plus

grand nombre, à une démocratie culturelle qui implique pour sa part une redéfinition même de la culture en prenant en compte les apports de tous et toutes (Hadley et Belfiore, 2018). Le champ des politiques culturelles a par conséquent été marqué dans les dernières années par un « tournant participatif » (Bonet et Négrier, 2018), alors que se développe le concept d'une citoyenneté culturelle (Poirier, 2017) qui suggère que la participation culturelle dépasse désormais les cadres institutionnels pour s'établir comme une contribution à l'espace civique.

Gouvernance dans le secteur des bibliothèques et archives

La littérature sur le secteur des bibliothèques a documenté la mise en place de cadres internes de gouvernance dès les années 1970 (Stevens, 1977). Dans les travaux plus récents au Canada, **l'implication de membres issus de la société civile dans les conseils d'administration des bibliothèques publiques est présentée comme un facteur de proximité avec les besoins et les intérêts de la communauté desservie (Irwin, 2012). Mais la diversité des membres du public et les multiples conceptions du « public » lui-même viennent complexifier l'adoption de processus décisionnels et de politiques internes** qui puissent répondre aux différents besoins d'une communauté hétérogène, comme l'ont montré Freeman et Blomley dans le cas de la bibliothèque publique d'Edmonton (2019).

Ce défi de représentation des divers groupes d'utilisateurs et d'utilisatrices soulève une réflexion socio-politique plus large sur le rôle des bibliothèques comme sphères publiques de participation citoyenne (Widdersheim, 2015). Cette orientation rejoint le modèle en expansion de la bibliothèque comme tiers lieu, dédié à la vie sociale de la communauté et ouvert sur la mixité sociale, qui lui confère une fonction politique d'accueil de débats publics et démocratiques (Servet, 2010 ; Jacquet, 2017). Ce modèle a d'ailleurs suscité la mise en place de laboratoires d'innovation publique autour des technologies numériques dans plusieurs bibliothèques au Québec, en misant sur l'approche de membres du public actifs et engagés dans le développement technologique

(Martel, 2017, 2018). Toutefois, pour permettre l'activation d'une sphère publique réellement démocratique, certaines conditions doivent être mises en place, telles que la participation d'individus et de groupes diversifiés positionnés à différents niveaux de légitimité et de pouvoir, capables d'influencer la prise de décision, ainsi que la possibilité du conflit, sans présupposer l'atteinte d'un consensus (Fraser, 1990).

Outre les documents de politique interne, plusieurs cadres de référence professionnels guident les pratiques de gouvernance des bibliothèques publiques au Québec. Les *Lignes directrices pour les bibliothèques publiques du Québec* (2019), copubliées par l'Association des bibliothèques publiques du Québec, BAnQ et le Réseau BIBLIO du Québec, incluent une série de recommandations en ce qui concerne la gouvernance des bibliothèques publiques et la relation aux publics. La « bonne gouvernance » y est caractérisée par « la clarification des rôles et des responsabilités entre les différents acteurs, la concertation avec ses partenaires, la participation et la prise en compte de la communauté, la transparence et l'évaluation » (p. 131). **Ces lignes directrices recommandent explicitement de consulter et d'impliquer les citoyens et les citoyennes dans la gouvernance pour alimenter la planification stratégique des programmes et « assurer l'adéquation des services et des activités avec les attentes de tous les groupes de la communauté »** (p. 25).

L'examen de la littérature sur la gouvernance culturelle et le secteur des bibliothèques montre que la notion de gouvernance est bien implantée dans la culture institutionnelle des bibliothèques publiques, y compris au Québec. La consultation des publics et l'implication de groupes diversifiés sont identifiées comme des facteurs de « bonne gouvernance ». Ces orientations témoignent plus largement d'une volonté d'adaptation aux transformations contemporaines du champ culturel, en lien avec l'inclusion de groupes minoritaires, dans une approche de démocratie culturelle et de participation civique. Par contre, il reste du libre ressort de chaque institution de mettre en œuvre ces recommandations : en résultent des niveaux variables de participation et d'engagement des publics et des défis d'inclusion sociale qui perdurent.

Gouvernance numérique

La gouvernance des données s'inscrit plus largement dans le champ de la gouvernance numérique. Notons que l'apparition des technologies numériques a suscité une importante littérature sur la gouvernance puisque les processus décisionnels dans ce domaine impliquent des actrices et acteurs variés, tant privés que publics et communautaires, ainsi que de nouvelles agentivités techniques (Musiani et Schafer, 2018).

Le champ d'études de la gouvernance numérique s'est notamment développé autour des travaux portant sur la gouvernance d'Internet (Goldsmith et Wu, 2006 ; Bygrave et Bing, 2009 ; Badouard et al., 2012), qui documente les relations entre institutions publiques, acteurs commerciaux et société civile. Selon Laprise et Musiani (2015), **la gouvernance d'Internet met en jeu une pluralité d'acteurs, une coordination technique, le développement de standards et l'établissement de politiques publiques à différentes échelles (domestique et supranationale)**. Pour ces deux auteurs, les enjeux de gouvernance se cristallisent autour du contrôle des infrastructures technologiques, qui sont une entrée clé pour comprendre la « politique matérielle » du numérique.

Le champ d'étude de la gouvernance numérique est aussi marqué par un ensemble de travaux sur des collectifs auto-organisés, telles les communautés du logiciel libre (Proulx et Couture, 2006) ou les contributeurs et contributrices à l'encyclopédie Wikipédia (Cardon et Levrel, 2009), qui ont développé des modes de production, de gestion et de partage de la propriété inspirés de la philosophie des communs. Dans ces cas de figure, les modes de gouvernance tendent à être horizontaux et décentralisés, sans toutefois être dénués de dynamiques conflictuelles.

Les processus de gouvernance concernant les données massives ont particulièrement retenu l'attention d'organismes de la société civile et de chercheurs sous les angles de la protection de la vie privée et de la capacité des usagers et usagères à débattre de ces

technologies, à influencer leur développement et à les gouverner (Elmer et al., 2015). Plus récemment, **la notion de « gouvernamentalité » a contribué à renouveler le champ de la gouvernance numérique en mettant l'accent sur les formes de rationalités (a)politiques qui sous-tendent l'analyse des données massives et la politique des algorithmes** (Rouvroy et Berns, 2013). Ces enjeux croisent de plus en plus ceux du développement de l'intelligence artificielle, qui prend une place croissante depuis plusieurs années dans les débats animant la sphère publique médiatique, notamment autour de ses enjeux éthiques.

Selon Gillespie (2014), **l'idée que les algorithmes utilisés pour l'analyse des données massives sont libres de subjectivité, d'erreurs ou de biais est une fiction**. L'auteur souligne ainsi que les résultats des algorithmes ne sont pas des produits entièrement techniques : ils relèvent aussi de décisions humaines et institutionnelles. Pour Peacock (2014), le marché des données numériques s'apparente à un contrat injuste puisque ce sont les usagers et usagères qui portent tout le poids et les conséquences du manque d'alternatives et du manque de régulation. L'auteur déclare que l'industrie de l'information ne réussira pas à s'autoréguler puisque le déséquilibre profite aux acteurs commerciaux. Ainsi le besoin d'établir des normes éthiques pour la gouvernance des données numériques se fait toujours plus pressant.

Principes éthiques en données massives, algorithmes et intelligence artificielle

Les données massives, les algorithmes et l'intelligence artificielle sont gouvernés par des individus et des organisations dont les décisions ayant trait aux modalités de ces technologies peuvent avoir des répercussions importantes sur la vie des usagers et usagères dont les données sont compilées (ou exclues), utilisées et entreposées. De là l'importance d'établir, dans un contexte de technologies omniprésentes appelées à s'imposer de manière croissante dans notre quotidien, des normes et bonnes pratiques

fondées sur des principes éthiques, ainsi que d'assurer que le cadre réglementaire en vigueur.

D'un rapport rédigé par la Commission de l'éthique en science et technologie du Québec (Cliche, 2017), **nous retenons trois principes éthiques. Le premier est d'assurer la primauté de l'intérêt public**, ou, en d'autres mots, de maximiser les bénéfices sur le plan du bien commun plutôt que de laisser certains individus ou organisations profiter de la majorité des bénéfices découlant des développements technologiques. **Le second est d'assurer une distribution équitable des bénéfices et préjudices potentiels entre toutes les parties concernées. Le troisième veut que les bénéfices attendus soient toujours supérieurs aux inconvénients qui pourraient résulter d'un projet numérique.** Il est recommandé que les modalités d'application de ces principes soient soumises à réflexions et débats spécifiques à toutes itérations. En effet, **la nécessité de maintenir un débat continu est soulignée par plusieurs spécialistes**, qui notent qu'une vigilance constante doit être exercée face à l'évolution rapide des technologies de l'information (Déziel et al., 2020 ; Ylipulli et Luusua, 2019 ; Dilhac et al., 2018).

Selon la Commission de l'éthique en science et technologie, ces principes devraient être reflétés dans le cadre législatif. Notons à ce propos que les cadres légaux en place au Québec et au Canada (dont les principaux documents sont listés en annexe, accompagnés de leurs points saillants) promettent une certaine protection aux usagers et usagères qui sont incorporés, de par leur production de données d'usage en contexte numérique, dans l'industrie de l'information. Notamment, **la loi certifie aux citoyennes et citoyens que les organisations collectant leurs données doivent se pourvoir de leur consentement — qui doit être retirable — ; que tous et toutes ont droit à la rectification des erreurs ; que la collecte ne doit pas être une condition pour l'obtention d'un produit ou d'un service ; que l'objet de collecte doit avoir des fins spécifiques et identifiées ; que la collecte soit nécessaire ou « raisonnablement acceptable » dans les circonstances ; que la protection des données, une fois collectées, soit proportionnelle à leur sensibilité** (Laboratoire de Cyberjustice, 2019).

Pourtant, cette protection légale, à bien des égards, n'est pas satisfaisante : entre autres carences, elle manque souvent de précision, n'impose pas assez de transparence aux organisations, n'assure pas assez d'autonomie aux publics dont les données sont collectées, et n'assure définitivement pas la primauté de l'intérêt public et une distribution équitable des bénéfices et préjudices potentiels entre toutes les parties concernées (Laboratoire de Cyberjustice, 2019 ; Tchéhouali et Plamondon, 2019 ; Déziel et al., 2020 ; ACEI, 2020 ; Cliche, 2017). Il s'avère donc que les gouvernements canadien et québécois doivent actualiser leurs dispositions légales et juridiques. **Les institutions cherchant à entreprendre de bonnes pratiques devraient assurer une protection des usagers et usagères beaucoup plus élaborée que ce qui est requis par la loi si elles veulent correspondre aux normes de gouvernance éthique se dégageant de la littérature.**

Outre les principes proposés par la Commission de l'éthique en science et technologie du Québec, plusieurs spécialistes ont émis des recommandations pour établir les normes d'une gouvernance éthique des données massives, des algorithmes et de l'intelligence artificielle. Le Tableau 4 en propose une synthèse non exhaustive, bien qu'elle se veuille représentative, et ciblée sur les principes pertinents à la gouvernance des données numériques en milieu culturel. Ainsi, certains principes s'adressant spécifiquement à la gouvernance de la technologie dans d'autres domaines d'expertise, par exemple en urbanisme ou en ressources humaines, sont omis de notre synthèse.

Nous avons identifié quatre catégories de recommandations et avons associé ces catégories à des principes éthiques généraux : **la légitimité démocratique, la responsabilisation des organisations, l'équité et la diversité culturelle**. Nous remarquons que le principe de diversité culturelle est relativement peu discuté dans la littérature portant sur la gouvernance numérique et que peu de recommandations s'y apparentent.

Tableau 4 : Sélection de principes recommandés dans la littérature pour une gouvernance numérique éthique

PRINCIPES	DÉCLINAISONS
Légitimité démocratique	<ul style="list-style-type: none"> • Esprit d’inclusion et de participation ; • Dialogue démocratique continu ; • Consultation et implication citoyenne dans la prise de décision ; • Primauté de l’intérêt public ; • Formation pour toutes et tous en littératie numérique afin d’habiliter le dialogue démocratique ; • Accessibilité des données collectées en un format intelligible et anonymisé (principe des données ouvertes) ; • Publication de codes source ou profils de calculs afin de permettre des évaluations externes et un contrôle démocratique ; • Utilité réelle pour la collectivité de la mise en œuvre de projets de collecte et d’utilisation de données ; • Bénéfices attendus toujours supérieurs aux inconvénients potentiels.
Responsabilisation des organisations	<ul style="list-style-type: none"> • Collecte du minimum de données nécessaire pour remplir la mission de l’organisme ; • Transparence quant à la collecte, l’utilisation, l’entreposage et l’effacement de données ; • Traçabilité de la trajectoire des données ; • Fardeau du consentement imposé aux organisations collectant les données et non aux usagers et usagères (privacy by default) ; • Consentement intelligible, continu et facile d’accès en tout temps ; • Imputabilité des décisions humaines encadrant les algorithmes et l’intelligence artificielle ; • Obligation d’avoir une supervision humaine à toutes les étapes des processus technologiques ; • Identification de la chaîne humaine de responsabilité.
Équité	<ul style="list-style-type: none"> • Distribution équitable des bénéfices et préjudices ; • Équité envers les individus issus de communautés minorisées et ceux en situation de handicap ; • Équité envers les non-publics (qui sont nécessairement sous-représentés quantitativement et qualitativement) ;

	<ul style="list-style-type: none"> • Rééquilibrage des rapports de force et des possibilités de négociation entre les organisations et les individus, et entre les organisations privées et les institutions publiques (ex. entre Google Analytics et BAnQ) ; • Offre d'un plus grand éventail de choix aux individus (au lieu d'un choix dichotomique) pour paramétrer la navigation individuelle des technologies ; • Stratégies techniques : enlever le biais à l'origine, modifier ou modeler les algorithmes, adapter ce qui en sort pour faire prévaloir l'équité plutôt que l'égalité.
Diversité culturelle	<ul style="list-style-type: none"> • Maintien de la diversité sociale et culturelle et de la diversité des expressions culturelles ; • Présence et découvrabilité des contenus francophones ; • Favoriser la souveraineté ou l'auto-détermination des données autochtones ; • « Droit à la mémoire » : présence de groupes diversifiés dans les archives de données ; • Éviter d'imposer des normes sociales dominantes et des hiérarchies ethnoculturelles de par la collecte ou l'analyse de données.

Références : McDermott, 2017; Cliche, 2017; Gambs, 2020; Direction générale de l'action contre le racisme du gouvernement de l'Ontario (DGACR), 2018; Kukutai et Talor, 2016; Tchéhouali et Plamondon, 2019; Dilhac et al., 2018; Ville de Montréal, 2012; Déziel et al., 2020; Ytre-Arne et Das, 2019; Bowers, 2006.

En parallèle de ces principes, plusieurs études proposent des dispositions légales, juridiques, et d'infrastructures concrètes que les gouvernements du Canada et du Québec devraient entreprendre. Notamment, **la plupart des experts et expertes recommandent aux instances étatiques d'établir le droit à la vie privée comme un droit fondamental et remarquent qu'il est important de spécifier les contours légaux de ce qui est considéré comme « vie privée »**². D'autres suggèrent aussi de contraindre les organisations

² Pour plus de détails à ce propos, voir la section *Enquêtes sur la perception des données d'usage et de la protection de la vie privée en contexte numérique* du présent document.

recueillant les données à fournir les renseignements créés et obtenus à une autorité désignée (par exemple, Statistiques Canada ; Tchéhouali et Plamondon, 2019), de rendre ces renseignements publics après anonymisation (DGACR, 2018 ; Gambs, 2020), et de localiser leurs infrastructures ou sous-traitances de stockage de données afin que les données canadiennes restent au Canada (Tchéhouali et Plamondon, 2019).

Parmi d'autres suggestions concrètes destinées aux gouvernements, nous retrouvons aussi la recommandation de prendre des mesures législatives contre les comportements anti-concurrentiels des entreprises privées telles les GAFAM afin de réduire l'asymétrie informationnelle qui crée un déséquilibre entre les plateformes internationales et les acteurs du milieu de la culture canadienne (Maceli, 2018 ; Tchéhouali et Plamondon, 2019). De plus, **la recommandation d'établir une instance gouvernementale (composée d'un appareil judiciaire et de scientifiques indépendants, par exemple) s'occupant de la certification, de la vigilance et du contrôle de l'industrie des données et de l'intelligence artificielle semble faire consensus** (Dilhac et al., 2018). Enfin, l'établissement de mécanismes éducatifs assurant une littératie numérique commune à tous les citoyens et citoyennes est fortement recommandé aux gouvernements par la plupart des études ayant trait à la gouvernance numérique. Cette recommandation est discutée en plus amples détails dans une section subséquente du présent document.

À partir des principes présentés dans le Tableau 4, certaines études proposent aussi des dispositions concrètes que pourraient (ou devraient) prendre les organismes cherchant à assurer une protection des publics plus élaborée que ce qui est requis par la loi. Parmi ces recommandations, nous retrouvons celle de **maintenir pour toute la durée des projets de collecte et d'utilisation de données numériques une diversité de modes de consultation et de participation citoyenne** (Dilhac et al., 2018), celle de minimiser au maximum les collectes de données (Laboratoire de Cyberjustice, 2019 ; Bowers, 2006), et celle de rendre public un mécanisme intelligible de traçabilité de la trajectoire des données récoltées (Déziel et al., 2020 ; Dilhac et al., 2018). De plus, certains experts et expertes suggèrent de concevoir les outils numériques utilisés par les publics selon le

principe du *privacy by design* (protection de la vie privée par conception/par défaut) (Cavoukian, 2006 ; ACEI, 2020), tandis que d'autres proposent que ces institutions adoptent, comme la Ville de Montréal, une politique d'ouverture par défaut contraignant l'organisation à publier toutes les données qu'elle détient (sous un format anonymisé) afin de contribuer à la construction d'un savoir démocratique et à une mutualisation du savoir sur les publics de la culture québécoise (Ville de Montréal, 2012 ; Legoux et Lord, 2019 ; Legoux et Duceppe, 2020). Certain.e.s recommandent aussi aux organisations qui utilisent l'intelligence artificielle pour améliorer l'expérience numérique des publics d'établir une supervision humaine des processus technologiques modulant l'expérience des usagers et usagères (Gambs, 2020 ; Déziel et al., 2020 ; Dilhac et al., 2018). Enfin, pour les institutions sensibles au désir de souveraineté des communautés autochtones, nous relevons la recommandation d'établir des conventions d'échange de données avec des représentant.e.s de ces communautés afin de contribuer à leur indépendance statistique (Kukutai et Taylor, 2016).

Enjeux pour le champ culturel

Outre les principes transversaux mentionnés ci-dessus, certains concernent plus spécifiquement les mécanismes de recommandation algorithmique utilisés dans le secteur culturel. Notons tout d'abord qu'**un dualisme s'est établi dans la littérature entre la vision optimiste des médias numériques comme outils de démocratisation et la vision négative de ces mêmes médias comme entraves à la réflexion profonde autonome et comme outils de surveillance continue**. Afin de surmonter ce dualisme, Langlois (2012) propose de s'intéresser à l'attribution de valeur culturelle et de degrés de signification aux contenus proposés par les mécanismes de recommandation algorithmique.

Dans une optique critique envers les mécanismes de recommandation, Caillet (2016) écrit que « la prédiction de l'intérêt affinitaire abîme définitivement le désir de la culture et de la possible découverte de l'expérience et de la différence », et Donnat (2016) ajoute que les algorithmes mènent le combat à la curiosité, à l'ouverture d'esprit et à la diversité du

goût. Ainsi, **les algorithmes et l'intelligence artificielle sont critiqués comme des obstacles au maintien de la diversité sociale et culturelle**, et certain.e.s proposent que, afin d'équiper les publics de demain pour l'exercice d'une autonomie intellectuelle et culturelle, il ne faut pas laisser aujourd'hui les acteurs et actrices d'Internet et du numérique façonner les goûts des publics via les algorithmes (Donnat, 2016 ; Gillespie, 2014). Encore une fois, cet appel à l'action ne semble pas avoir généré de littérature constructive suggérant des solutions concrètes à l'enjeu en question.

Gouvernance participative et inclusive

Plusieurs auteurs insistent sur le fait qu'une gouvernance éthique des données d'usage est nécessairement modulée par la participation citoyenne et par une approche décisionnelle inclusive. Dans cette section, des éléments de définition de la « gouvernance participative » et de la « gouvernance inclusive » sont discutés en relation aux enjeux de gouvernance des données d'usage.

Selon McLaverty (2011), le développement de démarches participatives telles que les consultations publiques et les processus de coconstruction des savoirs résulte de la capacité des groupes issus de la société civile — du « troisième secteur », qui est opposé aux secteurs public et privé — de générer une opposition efficace aux politiques publiques. Le secteur public aurait ainsi commencé à intégrer divers groupes d'intérêts du troisième secteur dans les processus politiques afin de permettre aux processus en question de bénéficier du savoir, de l'expérience et du soutien de ces groupes issus de la société civile. Alors que le niveau de satisfaction des citoyens et citoyennes des démocraties euro-américaines par rapport aux modalités d'application du principe démocratique avait diminué, au début du 21^e siècle, en comparaison aux décennies précédentes (Dalton, 2004), de nouvelles opportunités pour les citoyens et citoyennes de s'impliquer politiquement ont été proposées comme promesse d'un regain de légitimité politique (McLaverty, 2011). Ainsi, l'idéal démocratique transcende aujourd'hui la notion

de représentativité et les institutions libérales pour intégrer les voix de la société civile via les approches participatives — ascendantes et pluralistes — employées par les organisations du troisième secteur. Les opinions recueillies par Dilhac et al. (2018) dans le cadre de la rédaction de la *Déclaration de Montréal pour un développement responsable de l'Intelligence Artificielle* expriment toutefois **une crainte que le déterminisme technologique et le besoin urgent de gouverner les nouveaux développements technologiques ne jouent en la défaveur d'une gouvernance participative**. Le rapport de ladite déclaration suggère à ce propos que le développement d'une littératie numérique chez l'ensemble des citoyens et citoyennes — un des chantiers que le rapport identifie comme prioritaires — permettrait le développement d'une pensée citoyenne critique et d'une motivation pour la société civile de participer à la gouvernance de l'intelligence artificielle et des données massives.

D'une manière analogue, l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA) a rédigé un mémoire en lien avec la Stratégie québécoise de la recherche et de l'innovation 2022. Il soutient dans ses recommandations qu'**il convient d'appuyer des initiatives et « des projets d'amélioration de la littératie numérique des usagers » et usagères, et d'« augmenter leur sens critique et [d']accroître leur capacité à tirer le maximum des technologies d'information »** (OBVIA, 2021 : 23). Selon l'OBVIA, ces trois énoncés ont un rôle pour promouvoir une meilleure inclusion sociale et donner la chance à toute personne de s'impliquer et d'avoir un rôle de « citoyen actif » dans la société. Le mémoire suggère par ailleurs que le gouvernement soutienne les propositions qui favorisent la participation citoyenne de façon à « recueillir de l'information sur les obstacles à l'implantation de l'IA et du numérique, de réfléchir dans une dynamique de coconstruction aux solutions susceptibles de permettre la résolution des problèmes rencontrés » (OBVIA, 2021 : 23). En somme, le mémoire insiste sur l'importance de ne pas négliger les enjeux sociaux, politiques, économiques et culturels relatifs aux technologies de l'IA.

Au-delà de ces déclarations de principe, Couldry et Powell (2014) remarquent toutefois que **les études portant sur la gouvernance numérique et algorithmique devraient porter plus d'attention à l'agentivité et à la réflexivité des membres du public et de la société civile, qui sont souvent victimisé.e.s et décrit.e.s par la littérature scientifique comme impuissant.e.s face à la technologie.** Les données numériques ont pourtant un potentiel habilitant pour les membres de la société civile ayant une littératie numérique avancée : Milan et Van der Velden (2016) étudient d'ailleurs un phénomène qu'ils appellent « **l'activisme de la donnée** » (*data activism*), qui se décline en versions réactives (réaction à la menace algorithmique et efforts menés dans l'objectif d'ébranler le système établi de collecte de données massives) et en versions proactives (mobilisation et appropriation des données dans l'objectif de créer des narrations alternatives de la réalité sociale). C'est donc en (re)prenant le contrôle des technologies du quotidien que les activistes de la donnée et d'autres groupes du troisième secteur confronteraient l'élitisme d'expertise et une version de la démocratie qui ne leur sied pas.

Outre ces pratiques politisées, la participation des publics peut aussi être conçue dans l'optique de cocréation qui est à la base des pratiques de valorisation des données d'usage, où les membres du public deviennent des « pro-sommateurs » ou « pro-sommatrices » - cette expression signifie qu'ils et elles agissent autant du côté de la consommation que de la production des biens et services numériques. Beaudouin et Denis (2016) remarquent ainsi que **les institutions culturelles, du fait que les publics y sont fortement attachés émotionnellement, disposent d'un potentiel de participation remarquable, mais que s'il se veut durable, l'engagement participatif ne doit pas s'apparenter à une forme d'exploitation.** Les publics, selon les auteurs, doivent effectivement recevoir des incitatifs valables et être satisfaits de contribuer à la gouvernance des expériences numériques offertes par les institutions culturelles.

Pour ce qui est de la « gouvernance inclusive », elle a trait aux enjeux de composition sociale des groupes d'acteurs et actrice.s impliqué.e.s dans les processus de gouvernance. Une telle gouvernance peut se matérialiser, par exemple, grâce à des

efforts visant à renforcer les compétences numériques de groupes traditionnellement sous-représentés dans le domaine de l'intelligence artificielle et des données massives, tels que les femmes ou les Premières Nations, ou par le développement de standards techniques d'inclusion et de non-discrimination à intégrer dans les algorithmes de décision et de recommandation. Les expert.e.s et citoyen.ne.s consulté.e.s dans le cadre de la rédaction du rapport de la *Déclaration de Montréal pour un développement responsable de l'Intelligence artificielle* font d'ailleurs **consensus quant au fait que l'inclusion passe par l'équité plutôt que par la neutralité algorithmique** (Dilhac et al., 2018). Le fonctionnement algorithmique devrait selon eux être corrigé par l'action humaine afin d'éviter que l'intelligence artificielle ne reproduise ou n'amplifie des discriminations existantes.

Dans un autre ordre d'idées, Koikkalainen (2011) remarque que les politiques contemporaines d'inclusion sociale ne reposent plus uniquement sur le secteur public, mais laissent plus de responsabilités au troisième secteur. Selon lui, cette nouvelle distribution de la gouvernance sociale serait l'œuvre des partisans et partisanses de la théorie néo-institutionnelle, qui, en réponse à un mécontentement face au modèle de l'état providence (le *welfare state*), propose de stimuler la participation civique, les réseaux informels et volontaires, et le « capital social ». Ainsi, **selon les modalités politiques contemporaines, la gouvernance inclusive serait indissociable de la gouvernance participative**. Bien que la société civile se montre résiliente et que des initiatives réagissant à l'omniprésence des technologies de la donnée dans nos vies quotidiennes émergent du troisième secteur, maints enjeux de pouvoir, d'autonomie et de légitimité restent à adresser pour assurer une gouvernance éthique de la donnée.

En effet, si le principe de diversification des parties prenantes (*multistakeholderism*) dans la gouvernance implique que chaque acteur ou actrice concerné.e puisse s'exprimer, Laprise et Musiani (2015) observent cependant que dans les faits, en ce qui concerne la gouvernance d'Internet, ce sont généralement les compagnies et les gouvernements qui

prennent les décisions, tandis que **la société civile, si elle s'exprime, ne se voit déléguée aucun pouvoir décisionnel.**

À la lumière de cette réalité, **dans son étude sur l'implantation de nouvelles technologies en bibliothèque, Larson (2019) recommande les stratégies de sondage et de *focus groups*, ainsi que l'intégration des divers groupes de parties prenantes (*stakeholders*) dans les processus décisionnels ayant trait à l'implantation de ces technologies, de façon à anticiper les problèmes et à reconnaître l'apport des groupes qui pourraient s'opposer à de tels changements. Selon lui, le dialogue ne devrait pas se limiter à la phase initiale d'implantation de la technologie, mais devrait se poursuivre de manière régulière tout au long d'un projet.** Il recommande à cet effet de mettre en place des groupes de discussion, des séminaires éducatifs et des occasions régulières de dialogue avec les parties prenantes.

En plus d'élaborer de tels mécanismes participatifs, il apparaît nécessaire non seulement **d'approcher les différents groupes de publics avec une sensibilité à leurs spécificités culturelles, mais aussi d'intégrer des acteurs et actrices issu.e.s de communautés diversifiées à toutes les étapes des processus décisionnels ayant trait à la « mise en données » des publics.** Une telle approche pourrait par ailleurs permettre aux segments du public qui sont issus des communautés autochtones de se diriger vers leurs objectifs d'auto-détermination ou de souveraineté des données (Kukutai et Taylor, 2016).

Agir pour la littératie numérique des publics

Afin que la gouvernance des données soit réellement participative et inclusive, **il est nécessaire de prendre en compte les fossés numériques dans la population, dont celui qui concerne la littératie numérique, et plus précisément la littératie des données personnelles.** Notons au passage que la littératie de la vie privée (*privacy literacy*), souvent comprise dans la notion de littératie numérique (*digital literacy*), est pour Maceli (2018) une catégorie de savoirs distincte. Ainsi, la **littératie numérique** est une catégorie

plus ample de connaissances et savoir-faire ayant trait à toutes les facettes de l'univers numérique, par exemple la capacité de lire ses courriels sur un appareil digital. Cette notion définie par l'UNESCO comme « l'habileté à accéder, gérer, comprendre, intégrer, communiquer, évaluer et créer de l'information de façon sécuritaire et appropriée par les outils numériques et les technologies en réseau » (définition de l'agence GAML de l'UNESCO, traduite librement par Dilhac et al., 2017 : 272).

La **littératie de la vie privée en contexte numérique** implique quant à elle une compréhension quant à l'utilisation des renseignements personnels en ligne, la capacité de reconnaître quand des données sont collectées, la compréhension des conséquences de cette collecte, et l'habileté de juger quand la collecte de données est appropriée et bénéfique et quand elle ne l'est pas. Pour mettre l'accent sur l'enjeu des données massives, Pangrazio et Selwyn (2019) utilisent **l'expression de littératie des données personnelles (*personal data literacies*)**. Celle-ci permet d'appréhender les niveaux de **compétences opérationnelles et critiques des membres du public concernant les données collectées à leur sujet**. Ces compétences se déclinent dans les domaines de l'identification des données personnelles, de la compréhension de leurs enjeux et de la réflexion sur leur gouvernance en contexte numérique. Ainsi ce type de littératie a pour visée d'aider les individus à s'investir de manière critique dans la gouvernance de leurs données, en favorisant un sentiment de compréhension, de contrôle et d'agentivité (Pangrazio et Selwyn, 2019).

La plupart des travaux s'entendent sur le fait qu'avec l'évolution constante et l'omniprésence du numérique dans notre quotidien, **la littératie numérique se place au cœur de la participation et de l'engagement social et citoyen** (Dilhac et al., 2018) **et devient une habileté civique essentielle au bien-être de la société démocratique** (Ylipulli et Luusua, 2019). En effet, Redden (2015) soutient que la capacité de critiquer et d'évaluer les décisions prises dans le cadre des gouvernances numériques dépend de la capacité des citoyens et citoyennes à comprendre les modèles et technologies utilisés, et Maceli (2018) remarque la profonde asymétrie des savoirs entre les publics et les fournisseurs

de services numériques rendent le consentement éclairé et la réflexivité très difficiles chez les usagers et usagères. Trottier (2018) estime pour sa part que la protection de la vie privée en contexte numérique est davantage une affaire de privilège que de droit, puisqu'elle nécessite du temps et la mise en application de certaines connaissances, ce qui n'est pas donné à tout le monde.

Ainsi, le besoin d'encapaciter et d'autonomiser les citoyens et citoyennes dans la sphère numérique, de transformer les « publics connus » saisis par les données (*known publics*) en des « publics connaissant » (*knowing publics*), réflexifs et actifs (Kennedy et Moss, 2015), est jugé primordial. Effectivement, de notre revue de la littérature se dégage le fait que les citoyens et citoyennes doivent comprendre leur rapport aux données et aux technologies numériques afin d'avoir les capacités de critiquer les modèles utilisés, d'imaginer des régimes alternatifs, de poser des actions politiques au niveau « micro » et de connecter ces actions à la gouvernance se déroulant au niveau « macro » (Brites et al., 2018). Ces compétences, celles de la « citoyenneté numérique » (Dilhac et al., 2018), doivent être développées et promues par des moyens éducatifs accessibles à tous les membres de la société.

Inclusion numérique : le rôle des bibliothèques

Les bibliothèques publiques, qui offrent, pour la plupart, une connexion gratuite à Internet et un accès non payant à des ordinateurs et autres outils numériques, représentent une portion significative des efforts publics d'inclusion numérique. Ce paramètre d'inclusivité, qui est défini par Bertot et al. (2016) comme l'accès à toutes les ressources nécessaires pour participer à la société moderne et à ses itérations numériques est mis en relation par ces auteurs et autrices à la littératie numérique, qui se définit quant à elle en termes de capacités et d'habiletés.

Pour plusieurs spécialistes, le rôle d'éduquer les citoyens et citoyennes à propos des technologies numériques incombe aux bibliothèques publiques (Shaffer, 2014 ; Ylipulli

et Luusua, 2019), puisque ces dernières procurent déjà un accès libre à ces technologies, promeuvent déjà la notion de pensée critique, qui est étroitement reliée à la littératie numérique (Wissinger, 2017), et représentent déjà une présence soutenue dans le quotidien des citoyens et citoyennes, contrairement aux OBNL (organisations à but non lucratif) qui sont actives dans le domaine de l'éducation numérique (Maceli, 2018). De plus, étant donné que la bibliothèque publique se veut être un lieu d'éducation continue (ABPQ, 2019) et que cette institution est identifiée comme un tiers lieu idéal à la démocratisation du savoir (Servet, 2010 ; Jacquet, 2017 ; Dilhac et al., 2018), il semble très approprié qu'elle devienne l'un des vecteurs principaux d'une littératie numérique citoyenne. **Ainsi, un croisement entre la notion d'éducation citoyenne — cruciale à une gouvernance participative des données numériques — et le positionnement social de la bibliothèque fait surface pour suggérer le rôle central de cette institution dans le développement de la littératie numérique et de la littératie de la vie privée.** Ylipulli et Luusua (2019) soutiennent par ailleurs que les acteurs et actrice.s institutionnel.le.s de niveau « meso », telles les bibliothèques publiques, permettent d'établir des ponts entre des activités de niveau « micro » (par exemple le développement d'une perspective critique à l'endroit des technologies « mises en pratique » à la bibliothèque) et le niveau « macro » de la gouvernance numérique. Ainsi, cette approche reflète le principe de gouvernance participative et inclusive tel qu'il a été décrit dans une section précédente de ce document.

Les bibliothèques auraient donc un positionnement idéal (Maceli, 2018), et même, selon certain.e.s, l'obligation morale (Wissinger, 2017 ; Ylipulli et Luusua, 2019) d'offrir des services visant à accroître la littératie numérique de leurs publics et des citoyen.ne.s qu'elles desservent. À ce propos, il est intéressant de constater qu'un recensement analysé par Bertot et al. (2016) démontre que la plupart des bibliothèques publiques, aux États-Unis, offrent des formations, formelles comme informelles, pour habiliter leurs publics dans leurs compétences numériques. L'étude souligne aussi que ces bibliothèques

manquent de ressources pour mettre en œuvre tous les services d'inclusion et d'éducation numérique qu'elles aimeraient offrir.

Concernant la littératie des données personnelles, Beck (2018) soutient que la formation des usagers et usagères concernant la gestion et la confidentialité des données est fondamentale. En effet, **même si les bibliothèques suivent des normes en matière de protection de la vie privée, il est encore difficile d'appliquer ces normes aux données récoltées par les fournisseurs tiers. Cependant, il est possible de mieux renseigner les publics à propos de ces services tiers, de leurs facteurs de risque et de leurs conséquences potentielles.** La formation du personnel sur ces questions est donc centrale et elle doit être considérée dans une politique générale de gestion des données.

Pour autant, très peu d'information existe à ce jour sur les efforts d'inclusion et d'amélioration de la littératie des données personnelles déployés dans les bibliothèques canadiennes et québécoises : il s'agit d'un manque important dans la littérature scientifique.

4. ENQUÊTES SUR LA PERCEPTION DES DONNÉES D'USAGE ET DE LA PROTECTION DE LA VIE PRIVÉE EN CONTEXTE NUMÉRIQUE

Facteurs d'influence de la perception de la vie privée

Une multiplicité de facteurs, souvent intersectionnels, peuvent influencer la perception des individus en ce qui a trait au respect de leur vie privée en contexte numérique. L'examen de la littérature existante en termes d'enquêtes quantitatives et qualitatives à ce sujet montre que **les principaux facteurs sociodémographiques qui influencent cette perception sont : 1) le niveau de scolarité complété ; 2) l'âge ; et 3) le niveau de littératie numérique**. Toutefois, le degré d'influence de chacun de ces facteurs ne fait pas toujours consensus dans les études consultées. D'autres facteurs sociodémographiques moins déterminants sont aussi étudiés dans la littérature, tels que l'appartenance à un groupe marginalisé ou racisé, le revenu familial et la situation de handicap. Des facteurs psychologiques, collectifs, idéologiques, situationnels et méthodologiques sont aussi relevés dans les travaux consultés.

Premièrement, une forte tendance parmi les enquêtes consultées suggère que le niveau de scolarisation fait varier les perceptions de manière significative. Selon plusieurs études, **les usagers et usagères ayant fait des études postsecondaires ont un niveau de préoccupation plus élevé au regard de la protection de leur vie privée en ligne que ceux n'ayant pas de diplôme postsecondaire** (Phoenix SPI, 2019 ; Pasquier, 2018 ; Bergstrom, 2015). De plus, il s'avère que les usagers et usagères sans diplôme postsecondaire sont plus susceptibles d'être convaincus d'avoir d'assez bonnes connaissances pour prévoir l'incidence que les nouvelles technologies pourraient avoir sur la protection de leur vie privée, ce qui expliquerait leur niveau plutôt bas de préoccupation par rapport à la confidentialité de leurs données d'usage (Phoenix SPI, 2019). L'étude de Bergstrom (2015) vient toutefois nuancer cette affirmation. À contre-courant des autres études existantes,

ses résultats montrent que la recherche d'information, le traitement des courriels et l'utilisation de cartes de débit en ligne suscitent plus d'inquiétudes auprès des individus avec moins d'éducation. L'autrice suggère qu'il est difficile d'établir des comparaisons entre les études existantes, car la variable de la scolarisation y est traitée selon des catégories non uniformes.

Deuxièmement, la manière dont l'âge influence la perception de la vie privée en contexte numérique ne fait pas consensus, même si ce facteur est identifié comme étant très significatif par la plupart des études. Alors que le sondage réalisé pour le Commissariat à la protection de la vie privée au Canada (CPVPC) en 2018-2019 note que ce sont les usagers et usagères âgés de 25 à 55 ans qui sont les plus préoccupé.e.s par la protection de leur vie privée (en comparaison avec les citoyen.ne.s âgé.e.s de moins de 25 ans et de plus de 55 ans ; Phoenix SPI, 2019), une étude québécoise réalisée en 2019 rapporte plutôt que plus les répondant.e.s sont âgé.e.s, plus ils tendent à prioriser la confidentialité et la protection de leur vie privée en contexte numérique (Azzaria et Zimmermann, 2019), une observation corroborée par McStay (2020) dans un sondage réalisé auprès de 2000 citoyen.ne.s en Grande-Bretagne. De plus, selon ces deux études, **plus les publics sont jeunes, plus ils semblent avoir une conception ouverte de la vie privée et un niveau de préoccupation moindre à l'égard de la protection de leurs données numériques** (Azzaria et Zimmermann, 2019), sans toutefois se montrer ouvertement favorables à la surveillance (McStay, 2020).

Il se pourrait toutefois que la disparité entre l'étude du CPVPC et celles d'Azzaria et Zimmermann sur le facteur de l'âge ne traduise pas une différence significative entre les perceptions des Québécois.e.s et celles des Canadien.ne.s des autres provinces, mais qu'elle s'explique plutôt par des différences dans la formulation des questions de sondage de ces deux enquêtes, qui ne sont pas strictement comparables. Par ailleurs, Azzaria et Zimmermann (2019) soulignent que **les écarts d'opinions liés à l'âge s'illustrent par un continuum lié au cycle de vie plutôt que par des différences générationnelles.**

Quoi qu'il en soit, **il y a consensus sur le fait que ce sont les publics plus âgés qui adoptent le moins de comportements visant à sécuriser la confidentialité de leurs usages numériques** (Phoenix SPI, 2019 ; Bergstrom, 2015 ; Courmont, 2018 ; Azzaria et Zimmermann, 2019, Kennedy et al., 2020a), **probablement par manque de familiarité d'usage avec les technologies numériques**. Des données récoltées aux États-Unis par le Pew Research Center à propos de la relation entre âge et comportement de protection de la vie privée (Perrin, 2018) corroborent cette observation. En effet, suite à l'affaire Cambridge Analytica, ce sont les jeunes Américain.e.s qui ont le plus agi pour renforcer leurs paramètres de protection de la vie privée en ligne : « 44 % des usagers de 18 à 29 ans, soit le plus jeune groupe d'âge sondé, avaient supprimé l'application Facebook de leur téléphone, contre seulement 12 % des utilisateurs 65 ans et plus. De plus, alors que seulement 33 % des usagers de 65 ans et plus avaient revu leurs paramètres de confidentialité, 64 % des plus jeunes utilisateurs ont rapporté l'avoir fait » (Perrin, 2018). Il faut toutefois noter que ces comportements visant à protéger la vie privée ont été observés par rapport aux réseaux sociaux seulement, et non de manière généralisée dans la sphère numérique. Dans cette optique, il est important de souligner que **les jeunes, comme beaucoup d'autres membres du public, semblent plus préoccupés par la confidentialité des données qu'ils laissent sur les réseaux sociaux que celles qu'ils laissent sur d'autres types de plateformes** (Azzaria et Zimmermann, 2019 ; Bergstrom, 2015).

Troisièmement, pour ce qui est de la littératie numérique, elle est définie par Hoffman, Lutz et Ranzini (2016) comme une combinaison de connaissance des enjeux de surveillance, de familiarité technique avec les technologies numériques et de connaissance de la réglementation encadrant la vie privée. Il s'avère que ces trois déclinaisons de la littératie numérique influencent de manière différente la perception qu'ont les publics de la confidentialité de leurs données d'usage. Ainsi, **les usagers et usagères ayant une connaissance développée des enjeux de surveillance et des dangers que courent leurs données d'usage s'en disent très préoccupés** (Barth et al., 2019). À

cela, il est toutefois important d'ajouter que, selon Hoffman, Lutz et Ranzini (2016), **la majorité des membres du public n'ont pas une bonne connaissance des menaces encourues en lien avec leurs données d'usage**. En ce qui a trait au facteur de la familiarité technique avec les technologies numériques, la causalité est moins nette. Tandis que l'acquisition d'une familiarité d'usage de base tend à réduire les préoccupations des usagers, cette corrélation ne tient pas au-delà de cette acquisition de compétences numériques élémentaires. En effet, **les usagers ayant des compétences d'usage moyennes et élevées avec les technologies numériques savent entrevoir qu'ils ne sont pas capables de comprendre les mécanismes techniques de violation de la confidentialité des données d'usage, ce qui cause chez eux un sentiment d'impuissance et de préoccupation** (Barth et al., 2019). Enfin, la perception de bien connaître la réglementation encadrant la vie privée dans le secteur numérique donne un sentiment de confiance si la réglementation est jugée suffisante, mais cause des préoccupations si elle est jugée insuffisante (Phoenix SPI, 2019 ; Barth et al., 2019). Pour leur part, **ceux qui ne pensent pas bien connaître la réglementation encadrant la vie privée ont plutôt un sentiment d'incertitude, qui est souvent la cause de préoccupations** (Hoffman, Lutz et Ranzini, 2016). À cet égard, il est intéressant de souligner qu'environ deux tiers des Canadiens estiment avoir une bonne connaissance de leurs droits en matière de vie privée (Phoenix SPI, 2019).

Concernant les enquêtes qui traitent plus précisément de la littératie des données personnelles, elles suggèrent des variations du niveau de littératie selon l'âge, mais aussi dans un même groupe d'âge en lien avec une situation de handicap. Par exemple, l'étude de Kennedy et al. (2020b) qui s'intéressait à la perception des individus sur les pratiques de données du radiodiffuseur public BBC, montre que les 16 à 34 ans possèdent une compréhension et une sensibilisation plus grande à ces enjeux que les participants âgés de 65 ans et plus. Cependant, au sein des participants plus jeunes, ceux et celles

avec des troubles d'apprentissage légers³ ont eu aussi des difficultés à comprendre les pratiques en matière de données lors des groupes de discussion. D'autre part, Kennedy et al. (2020a) invoquent une étude de Digital Catapult en 2015 qui relatait que 96 % des personnes interrogées lors de l'enquête pensaient bien comprendre le terme « donnée personnelle ». Pourtant, seul 64 % d'entre elles ont sélectionné la bonne définition dans un questionnaire à choix multiples. **Il semble donc que certaines personnes surestiment leur compréhension de notions reliées à la littératie des données personnelles.** Dans une étude plus récente de Kennedy et al. (citée dans 2020a), le taux de réussite était plus élevé vis-à-vis de la définition du mot « donnée personnelle ». Il est donc possible de penser que le terme se démocratise de plus en plus.

Quatrièmement, l'appartenance à un groupe marginalisé ou racisé est un autre facteur d'influence relevé dans la littérature, mais dans une moindre mesure et dans des études plutôt qualitatives (Direction générale de l'action contre le racisme du gouvernement de l'Ontario (DGACR), 2018 ; Kukutai et Taylor, 2016 ; Redden, 2018). Marwick et al. (2017) se sont intéressés lors de leur étude auprès de jeunes adultes avec un faible statut socio-économique à la perception du partage d'information en ligne. Les participant.e.s étaient majoritairement racisé.e.s et plusieurs avaient déjà eu une expérience avec les services policiers et la surveillance physique. Les résultats montrent que les participant.e.s utilisent des stratégies et des outils de protection de la vie privée très variés. En effet, certain.e.s utilisent des pseudonymes pour avoir une présence en ligne, mais d'autres ont pris la décision d'éviter les réseaux sociaux. Par ailleurs, plusieurs percevaient les risques du partage des données en ligne puisqu'ils et elles avaient subi de la surveillance hors-ligne (Marwick et al., 2017). Par ailleurs, **l'identification à une orientation sexuelle non-normative (LGBTQ+) et l'invisibilisation sociale, telle qu'expérimentée par les usagers**

³ Les auteurs incluent dans les troubles d'apprentissage légers l'hyperactivité, le trouble déficitaire de l'attention, le trouble du spectre autistique et le syndrome d'Asperger. Ce groupe représentait 10 personnes dans un échantillon de 68. Deux personnes sourdes étaient également dans l'échantillon et 14 d'entre elles non pas précisé leur situation relativement aux handicaps (Kennedy et al., 2020b).

et usagères sans-abris, semblent augmenter le niveau de préoccupation relatif à la vie privée en contexte numérique, notamment dans le cadre des services de bibliothèque (Campbell et Cowan, 2016 ; Mathson et Hancks, 2007 ; Richter et al., 2019).

Cinquièmement, le revenu familial d'un individu semble avoir une certaine incidence sur sa perception de la protection de la vie privée en contexte numérique, les individus ayant un revenu familial modeste déclarant beaucoup moins d'inquiétude par rapport à la confidentialité de leurs données que les autres (Barth et al., 2019 ; Pasquier, 2018). Kennedy et al. (2020) soulignent également l'intérêt d'intégrer une variable sur le revenu des ménages dans leur enquête au Royaume-Uni. Ceci dit, cette variable n'apparaît pas centrale dans le reste de la littérature. Quant au genre, il ne semble pas être un facteur d'influence déterminant, bien qu'il soit mentionné dans plusieurs travaux⁴.

Au-delà des facteurs sociodémographiques, diverses analyses ancrées dans la psychologie individuelle révèlent d'autres facteurs ayant une influence majeure sur la perception des publics vis-à-vis de la protection de leur vie privée en contexte numérique, notamment la propension d'un individu à souffrir d'anxiété et à se méfier des autres (Bergstrom, 2015) et l'expérience d'un état psychologique d'impuissance face aux menaces numériques (Hoffman, Lutz et Ranzini, 2016), propensions qui tendent à maximiser le niveau de préoccupation lié à la protection de la vie privée en ligne. Bergstrom (2015) relève aussi l'influence des orientations politiques et idéologiques des individus sur leur perception de la vie privée, les personnes se déclarant de gauche étant par exemple plus méfiantes, sceptiques et préoccupées par rapport à la protection de leur vie privée en contexte

⁴ Même si le genre ne semble pas être un facteur déterminant, certaines études se sont penchées sur la variation du niveau de confiance dans la gestion de la sécurité des données personnelles entre les hommes et les femmes, notamment en ce qui a trait au partage d'information sur les réseaux sociaux. Toutefois, il n'y a pas de consensus dans la littérature sur cette question. Une enquête de Ofcom (2016; cité dans Black et al., 2018) suggère que les hommes sont plus confiants que les femmes en ce qui a trait à la sécurité de leurs données personnelles. Cependant, Nurse et Williams (2016) ont obtenu un résultat différent dans une étude par entrevues. Sur ce sujet, voir aussi Pedersen et Frances, 1990 ; Black et al., 2018.

numérique. Quant aux personnes se déclarant de droite et déclarant soutenir les stratégies étatiques de surveillance numérique, elles tendent à être moins préoccupées par la confidentialité de leurs données personnelles.

L'influence de certaines valeurs collectives est aussi mentionnée par la littérature scientifique : **l'idéologie euro-américaine du « droit à la vie privée » (Yao et al., 2007) ainsi que les cultures nationales individualistes, dont les États-Unis représentent le paroxysme, font prévaloir les préoccupations ayant trait à la protection de la vie privée et aux usages non-autorisés des données numériques** (Bellman et al., 2004 ; Pasquier, 2018 ; Calimaq, 2018). *A contrario*, les citoyen.ne.s de pays où l'acceptation de l'intrusion par d'autres membres d'une communauté, par des organisations ou par des institutions gouvernementales dans la vie privée des individus est plus élevée (en Chine, par exemple) se révèlent moins préoccupés par la confidentialité de leur vie privée. De plus, les membres de cultures nationales dont l'index d'intolérance à l'incertitude est élevé (comme la Grèce et d'autres pays européens)⁵ se révèlent désirer plus d'encadrement législatif de leur vie privée et se révèlent plus préoccupé.e.s que les autres par la protection de leur confidentialité en contexte numérique (Bellman et al., 2004 ; Potoglou et al., 2017). **Considérant ces différents facteurs collectifs, nous pouvons faire l'hypothèse que les valeurs euro-américaines qui prévalent au Canada devraient favoriser un certain niveau de préoccupation et un désir d'encadrement de la protection de la vie privée en contexte numérique.**

Concernant ce désir d'encadrement, Bellman et al. (2004) soutiennent **que la structure réglementaire encadrant la vie privée reflète et influence la perception que les**

⁵ Il est toutefois intéressant de noter qu'il y a des disparités au sein des pays de l'Union européenne. Ainsi, dans l'étude de Potoglou et al. (2017), les proportions de participants avec des « fortes préoccupations » concernant la confidentialité sur Internet se retrouvaient majoritairement en Grèce, en Espagne, au Portugal, en Lituanie et en Lettonie. À l'inverse, c'était en Slovaquie, en Slovénie, au Danemark, en Suède et en Finlande qu'ils y avaient les plus grandes proportions de participants indiquant ne pas être concernés par cet enjeu.

citoyen.ne.s d'un pays ont quant à l'importance de protéger leur vie privée. Ces chercheurs notent en effet des différences culturelles entre les pays sans réglementation gouvernementale des données numériques (comme la Chine et le Mexique), les pays à réglementation sectorielle (États-Unis, Japon), et les pays à réglementation unificatrice de type « omnibus » tels que les pays de l'Union européenne et le Canada. Il est intéressant de souligner que les individus vivant dans les pays compris par cette dernière catégorie sont les plus enclins à désirer une majoration de la protection étatique des données personnelles par leur gouvernement : il semble en effet qu'un encadrement réglementaire déjà développé influencerait les citoyen.ne.s à percevoir l'importance de la réglementation de leur vie privée en contexte numérique et, ainsi, à désirer des cadres légaux encore plus complets.

L'analyse de la littérature révèle également que plusieurs facteurs situationnels ont un impact significatif sur la perception des publics vis-à-vis du respect de leur vie privée et de leurs données d'usage. Deux études menées au Canada (Phoenix SPI, 2019 ; Dilhac et al., 2018) soulignent par exemple **que le type d'organisation recueillant lesdites données à une influence sur le niveau de préoccupation des publics : les Canadien.ne.s et Québécois.e.s déclarent en effet, en proportion assez marquée, être moins préoccupé.e.s lorsque ce sont des organismes gouvernementaux et paragonnementaux que lorsque ce sont des entreprises privées telles que les GAFAM qui utilisent leurs données d'usage.** En effet, en 2018-2019, 45 % des Canadien.ne.s ont l'impression que les entreprises ne respectent pas leur droit à la vie privée, tandis que 29 % ont l'impression que le gouvernement fédéral ne respecte pas ce droit (Phoenix SPI, 2019). Pourtant, **de nombreux organismes publics utilisent des services tiers tels que Google Analytics pour l'analyse des données récoltées sur leur site web, ce qui vient brouiller la distinction entre organismes publics et privés.** Lorsqu'une organisation n'est pas claire dans l'information qu'elle donne au sujet de ses pratiques de données, les membres du public ont tendance à réagir plus émotionnellement (Kennedy et al., 2020a).

Le contexte dans lequel les données sont collectées revêt aussi une certaine importance (Bergstrom, 2015 ; Feng et Pan, 2016). Nous notons que **l'utilisation de moteurs de recherche semble générer moins de préoccupation liée à la confidentialité que la plupart des autres types d'usage** (par exemple, l'échange de courriels ou la publication de contenus sur les réseaux sociaux). Ceci s'explique par le fait que plus les répondant.e.s jugent un type d'usage comme étant de caractère personnel, plus ils et elles sont préoccupé.e.s par la confidentialité des données y étant associées (Bergstrom, 2015) — à tort ou à raison, puisque les requêtes dans un moteur de recherche peuvent révéler de nombreux indices personnels.

De plus, les usagers et usagères moins scolarisé.e.s ou ayant une littératie numérique moins développée seraient plus préoccupé.e.s par des menaces émanant de leur environnement social direct (comme le *stalking*, le cyber-harcèlement ou l'atteinte à la réputation dans le cercle social proche) que par des menaces issues d'acteurs organisationnels tels les GAFAM ou le gouvernement, menaces leur semblant plus distantes (Hoffman, Lutz et Ranzini, 2016 ; Young et Quan-Haase, 2013 ; Pasquier, 2018). Par exemple, plusieurs sont plus préoccupés par ce que des membres de leur famille révèlent à propos d'eux à leurs « ami.e.s » par l'entremise des médias sociaux que par les données d'usage que ces médias sociaux récoltent à leur propos et l'utilisation que ces organisations en font (Pasquier, 2018).

Enfin, Preibusch (2013) démontre que **des facteurs méthodologiques peuvent aussi influencer la mesure de la perception que les membres du public déclarent avoir de la protection de leur vie privée**. Un biais de cadrage positif s'immisçant dans la construction de formulaires de sondage ou d'études comportementales peut vraisemblablement induire les participant.e.s à souscrire à la valorisation de la protection de la vie privée qui est mise de l'avant par l'étude, c'est-à-dire à déclarer avoir un niveau de préoccupation qu'ils et elles jugent désirable socialement plutôt que de répondre selon l'intensité réelle de leurs préoccupations. En effet, les travaux concluent généralement que les usagers et usagères devraient être plus préoccupés par les menaces à leur vie privée, et ils et elles

transposent leur jugement dans la construction de leurs enquêtes. Un dernier facteur d'influence à mentionner a trait au niveau de confiance que les répondant.e.s ont envers l'entité administrant l'enquête : la confiance - ou, surtout, un manque de confiance - envers l'organisation menant la cueillette des données peut effectivement influencer le niveau d'honnêteté et de véracité des déclarations des répondant.e.s.

En somme, la multitude de facteurs sociodémographiques, psychologiques, réglementaires, situationnels et méthodologiques influençant la perception et les attentes relatives à la valorisation des données d'usage soulignés par la littérature reflète la complexité de la notion de « protection de la vie privée », qui se doit d'être définie de manière contextuelle par une société et ses individus. Les variables mentionnées ci-haut, ainsi que la manière dont elles entrent en corrélation avec l'indifférence, la préoccupation ou la confiance que peuvent ressentir les usagers et usagères par rapport à la protection de leur vie privée en contexte numérique, ont été synthétisées dans le Tableau 5. Il est à noter que les variables apparaissant être les plus significatives ont été placées en haut de leur catégorie respective au sein du tableau.

Tableau 5 : Facteurs d'influence sur la perception de la protection de la vie privée des usagers et usagères dans le contexte numérique

Facteurs d'influence sur la perception de la protection de la vie privée des usagers dans le contexte numérique			Indifférence ← ————— → Préoccupation Confiance ●
Socio-démographie	Scolarisation	Sans éducation universitaire	← —————
		Éducation universitaire	————— →
	Âge	Moins de 25 ans	← —————
		25-55 ans	————— →
		Plus de 55 ans	————— →
	Littératie numérique	Connaissance des enjeux de surveillance	————— →
		Familiarité d'usage avec les technologies numériques	← - - - - - →
		Connaissance de la réglementation encadrant la vie privée	● ou - - - - - →
	Affiliation à un groupe minoritaire	Appartenance à une communauté ethno-culturelle racialisée	————— →
		Auto-identification à une identité sexuelle non-normative	————— →
Revenu familial	Modeste	← —————	
	Moyen ou élevé	————— →	
Psychologie et valeurs	Tendance de l'individu à l'anxiété		————— →
	Sentiment d'impuissance vis-à-vis la protection de sa vie privée		————— →
	Valeurs individuelles	Manque de confiance envers les autres	————— →
		Orientation politique de gauche	————— →
		Orientation politique de droite et idéologie prônant la surveillance comme outil de sécurité publique	← —————
	Valeurs collectives	Idéologie du droit à la vie privée	————— →
		Communautarisme	← ————— ●
Individualisme		————— →	
Intolérance à l'incertitude	————— →		
Réglementation	Réglementation gouvernementale de la vie privée dans le contexte numérique	Pays sans réglementation	————— →
		Réglementation sectorielle	← —————
		Réglementation « omnibus » (ex. U.E., Canada)	————— →
Contexte	Type d'organisation recueillant les données	Public	← ————— ●
		Privé	————— →
	Proximité sociale perçue de la menace à la vie privée		————— →
	Type d'usage scruté	Médias sociaux	————— →
		Courriels	————— →
Utilisation de moteurs de recherche		————— →	
Méthodologie	Biais positif de construction du sondage induisant une valorisation sociétale de la protection de la vie privée		————— →
	Confiance envers l'entité encadrant le sondage ou l'expérience		●

Le paradoxe de la vie privée dans les comportements

En ce qui concerne non pas les perceptions, mais les comportements de protection de la vie privée en contexte numérique, la littérature scientifique tend vers un consensus quant à l'existence d'un phénomène nommé le « paradoxe de la vie privée » (*privacy paradox*). Ce paradoxe, formulé pour la première fois par Barnes (2006), a évolué au fil des ans et est aujourd'hui associé à une pluralité de définitions. Celle que nous retenons, et qui semble être acceptée par plusieurs spécialistes, décrit ce paradoxe comme **l'apparente contradiction entre le fait de se déclarer préoccupé par la protection de sa vie privée en ligne et le fait d'adopter des comportements très peu sécuritaires** (Barth et al., 2019). L'importance conférée à ce phénomène dans la littérature nous a invité.e.s à nous pencher sur les facteurs influençant le comportement des publics vis-à-vis de la protection de leur vie privée dans le contexte numérique, qui ont été synthétisés dans le Tableau 6.

Tableau 6 : Facteurs d'influence sur le comportement des usagers et usagères vis-à-vis la protection de leur vie privée dans le contexte numérique

Facteurs d'influence sur le comportement des usagers vis-à-vis la protection de leur vie privée dans le contexte numérique		←	→
		Comportement numérique non sécuritaire	Comportement numérique sécuritaire
Contraintes situationnelles	Argent requis pour protéger la confidentialité des données	←	
	Efforts requis pour protéger la confidentialité des données	←	
	Temps requis pour protéger la confidentialité des données	←	
	Proximité sociale perçue du danger pouvant porter atteinte à la confidentialité		→
Psychologie	« Cynisme de la protection de la vie privée » (<i>The cynicism of privacy</i>)	←	

Notons que le caractère irrationnel et les apparentes contradictions internes du paradoxe de la vie privée sont nuancés par certains chercheurs. Notamment, Preibusch (2013) souligne de possibles biais méthodologiques qui surévalueraient dans bien des cas ce paradoxe, peut-être moins profond qu'il ne le semble. **Les répondant.e.s seraient influencé.e.s, de par le cadrage normatif des enquêtes, à gonfler leurs préoccupations déclarées.** Il semblerait aussi que la proximité sociale perçue du danger a une influence sur le comportement des publics, ces derniers adoptant des comportements plus sécuritaires à l'encontre des menaces émanant de leur environnement social direct, mais réagissant avec moins de constance pour se protéger des menaces qui leur semblent plus distantes — et ce, même s'ils perçoivent l'existence de ces menaces et s'en disent préoccupés (Hoffman, Lutz et Ranzini, 2016).

D'autres chercheurs, comme Barth et al. (2019) et Bergstrom (2015), se sont attelés à démontrer que le paradoxe entre le comportement non sécuritaire des membres du public et leurs préoccupations déclarées peut être expliqué par **une analyse coût-bénéfice favorisant souvent l'immédiateté, la simplicité et la gratuité plutôt que la sécurité.** En effet, une corrélation positive établit que plus l'investissement en temps, en efforts cognitifs et en argent requis pour protéger ses données personnelles est grand, plus les individus (même ceux ayant une très bonne littératie numérique) tendent à ignorer leurs préoccupations liées à la protection de leur vie privée, car les contraintes mentionnées ci-haut sont souvent jugées peser plus lourd que la violation de la confidentialité des données. Une étude menée par Barth et al. (2019) démontre effectivement que même si 50 % des usagers et usagères ayant une excellente littératie numérique déclarent avoir des préoccupations maximales quant à leur vie privée, seulement 5 % de ces mêmes usagers et usagères traduisent ces préoccupations en un comportement réellement sécuritaire.

L'apparente disparité entre les préoccupations déclarées et les comportements non sécuritaires de nombreux membres du public est expliquée différemment par Hoffman, Lutz et Ranzini (2016), qui dénotent une attitude cynique — ce qu'ils désignent comme le

« cynisme de la vie privée » en substitution à la notion du « paradoxe de la vie privée ». **Cette notion insiste plutôt sur le sentiment d'impuissance que beaucoup d'utilisateurs et d'utilisatrices ressentent face à l'intrusion de leur vie privée en contexte numérique. Ce cynisme est, selon ces chercheurs, un mécanisme d'adaptation cognitif visant à rationaliser la dissonance entre de fortes préoccupations et un comportement ne pouvant peut-être jamais être assez sécuritaire.** Ce mécanisme de rationalisation sert ainsi à justifier une résignation qui a pour conséquence un comportement négligent et peu sécuritaire chez les publics. Ainsi, désarmés face à des rapports de pouvoir qu'ils perçoivent être au-delà du contrôle individuel, les utilisateurs et utilisatrices cyniques abandonnent tout effort et adoptent, par défaut, des comportements non sécuritaires.

Ainsi, la mise en œuvre d'une gouvernance des données uniquement assise sur des préoccupations et désirs déclarés par les publics apparaît problématique (Barth et al., 2019). À ce propos, plusieurs experts soulignent le besoin criant qu'a notre société d'adopter une culture de la confidentialité par défaut (*data privacy by default / data privacy by design*) (Cavoukian, 2006 ; ACEI, 2020), qui devrait, grâce à une réglementation plus stricte de la vie privée en contexte numérique, faire incomber le « fardeau du consentement » aux organismes collectant les données, plutôt qu'aux publics (Quintal et al., 2018, cité dans Dilhac et al., 2018).

Campbell et Cowan (2016) relèvent par ailleurs que dans le contexte des bibliothèques, un autre type de paradoxe de la vie privée se manifeste, soit **la contradiction entre l'influence positive d'une certaine valorisation des données d'usage (pour la recommandation de lectures, par exemple) et le désir de confidentialité entretenu par les jeunes individus LGBTQ+.** Ces jeunes, qui pourraient bénéficier de recommandations de livres ou services contribuant à leur construction identitaire non normative, préfèrent souvent garder confidentiels leurs usages de contenus pouvant être jugés marginaux. Dans le cas de tels groupes minorisés, la méthode d'enquête par sondage peut se révéler insuffisante pour saisir la complexité du paradoxe de la vie privée, et le recours au format

de l'entretien collectif peut permettre d'approfondir la compréhension des enjeux spécifiques qui les concernent.

Enquêtes au Canada et au Québec

Les définitions et les perceptions concernant la vie privée peuvent grandement varier en fonction du contexte national (voir plus haut). **Il est donc crucial de documenter localement les perceptions de la vie privée afin de comprendre la spécificité du contexte québécois. Or, peu d'enquêtes sur ce thème existent à ce jour au Québec**, mises à part quelques données éparses récoltées dans le cadre des consultations réalisées pour la *Déclaration de Montréal pour une Intelligence artificielle (IA) responsable* (2018) et celles, dans une optique plus légale, collectée par Azzaria et Zimmermann (2019). Pourtant, de telles données sont essentielles pour alimenter et orienter les mécanismes de gouvernance locale sur la protection de la vie privée.

À l'échelle du Canada, une série de sondages réalisés auprès des Canadien.ne.s pour le Commissariat à la vie privée du Canada relèvent une augmentation du niveau de préoccupation des Canadien.ne.s au cours des dernières années (Phoenix SPI, 2016) : le taux actuel de citoyen.ne.s ayant des préoccupations (tous niveaux confondus) concernant la protection de leur vie privée en contexte numérique est de 92 % (Phoenix SPI, 2019). De plus, un déclin significatif du nombre de Canadien.ne.s étant prêt.e.s à partager des données personnelles en échange d'un contenu ou d'un service utile a été observé de 2019 à 2020 (ACEI, 2020). Les Canadien.ne.s sont donc résolument préoccupé.e.s par la protection de leur vie privée en contexte numérique. **Une majorité désirent d'ailleurs des mesures de protection additionnelles pour les usagers et usagères numériques (ACEI, 2020)** et les deux tiers des Canadien.ne.s pensent que le gouvernement devrait être responsable de les aider à protéger leurs renseignements personnels (Phoenix SPI, 2019). Ces résultats corroborent la théorie avancée par Bellman et al. (2004) selon laquelle les citoyen.ne.s de pays ayant un cadre réglementaire pour la

protection de la vie privée de type « omnibus » sont plus enclin.e.s à souhaiter un renforcement de la réglementation gouvernementale sur la protection de la vie privée.

Or, il est intéressant de remarquer que **le Canada, comme l’Australie et la Nouvelle-Zélande, n’a pas adopté ce type de réglementation en réponse à des aspirations citoyennes, mais afin de souscrire à des conditions commerciales imposées par l’Union européenne** (Bellman et al., 2004). L’adoption d’un cadre réglementaire canadien formulé selon les normes de l’Union européenne aurait-elle ainsi influencé la population canadienne à devenir plus préoccupée et à désirer plus encore d’encadrement étatique de la vie privée ? Quel est l’apport réel d’influence de changements réglementaires sur la perception que les individus se font de la protection de leur vie privée ? Bien qu’il soit impossible de répondre à ces questions de manière précise, les préoccupations individuelles étant complexes et multifactorielles, l’influence des changements réglementaires sur les perceptions qu’ont les individus de la protection de la vie privée devrait être creusée. Un tel phénomène pourrait en effet s’avérer significatif s’il s’appliquait aussi au niveau organisationnel : **les organisations privées et parapubliques s’appliquant à protéger la vie privée de leurs publics pourraient éventuellement nourrir de par leurs efforts des attentes grandissantes chez leurs publics.**

Une avenue potentiellement plus probante pour expliquer l’accroissement d’un désir d’encadrement étatique de la vie privée chez les citoyen.ne.s canadien.ne.s (Phoenix SPI, 2016) semble être la sensibilisation grandissante du public aux enjeux de confidentialité se rattachant aux données numériques. Il apparaît effectivement vraisemblable que **l’accumulation d’affaires médiatiques ayant trait à des violations de la vie privée, telles que celle de Cambridge Analytica en 2018, et, pour le Québec, celle de la fuite de données de la Caisse populaire Desjardins en 2019, soit un facteur d’influence majeur sur l’opinion publique.** Bien que les impacts réels de ce type de couverture médiatique restent à déterminer, nous pouvons faire l’hypothèse que la médiatisation des enjeux des données personnelles contribue, et continuera à contribuer au courant des prochaines

années, à l'accroissement des préoccupations ayant trait à la vie privée en contexte numérique.

Au Québec, la perception des citoyen.ne.s vis-à-vis de la protection de la vie privée en contexte numérique n'a pas été sondée de manière systématique comme elle l'est régulièrement au niveau pancanadien. Toutefois, il est intéressant de noter que le sondage réalisé pour le Commissariat à la vie privée du Canada en 2018-2019 relève une différence de perception entre les Québécois.e.s et les Canadien.ne.s des autres provinces. **Les Québécois.e.s déclarent en effet un niveau de connaissance plus élevé sur la manière dont leurs données sont collectées et utilisées que les autres Canadien.ne.s. Les Québécois.e.s se sentent aussi plus en contrôle de leur vie privée et semblent ainsi moins préoccupé.e.s à ce propos que les autres Canadien.ne.s** (Phoenix SPI, 2019). L'étude d'Azzaria et Zimmermann (2019) souligne par ailleurs qu'environ la moitié des Québécois.e.s jugent bien ou très bien connaître leurs droits encadrant la vie privée. Pourtant, cette étude relève aussi que le niveau de découragement face aux contrats en contexte numérique est assez élevé (et ce, pour les répondant.e.s de tous âges) et que le droit relatif à la vie privée est vraisemblablement opaque et méconnu. **L'impression que plusieurs Québécois.e.s sont d'être bien renseigné.e.s à propos de la protection de la vie privée serait ainsi trompeuse.**

En somme, la nécessité de recueillir l'opinion des Québécois.e.s sur la vie privée et la confidentialité des données personnelles en contexte numérique est évidente, car nous en savons trop peu sur les facteurs de différenciation de leurs perceptions à l'échelle de la province.

Enquêtes dans le contexte des bibliothèques et archives

Pour terminer, en ce qui concerne les enquêtes menées spécifiquement sur le secteur des bibliothèques et archives, les travaux existants portent sur diverses catégories de bibliothèques telles que les bibliothèques universitaires (Cheng et al., 2015 ; Tummon et Dawn, 2018 ; Travis et Ramirez, 2020 ; Jones et al., 2020), les bibliothèques publiques (Vitak et al., 2018) et les bibliothèques territoriales et universitaires (dont une analyse comparative par L'École nationale supérieure des sciences de l'information et des bibliothèques en France ; Chovet, 2019). Mais très peu concernent directement les usagers et usagères des bibliothèques publiques sous l'angle de leurs perceptions de la vie privée et des données d'usage.

Sur la perception des publics

Du côté des bibliothèques publiques, peu d'études récentes concernent les nouvelles modalités de valorisation des données d'usage (l'étude de Larson étant fondée sur des données de 2006), et l'on constate un manque de données d'enquête sur la perception des publics à ce sujet. Certes une étude de Affonso et Sant'Ana (2018) a porté sur la collecte de données d'usage par neuf bibliothèques nationales d'Amérique du Sud, toutefois l'étude ne s'appuie pas sur des données de sondage ou d'entretien auprès des publics, mais sur une analyse des paquets de données échangés entre serveurs, et sur une analyse des interfaces d'usage.

Par contre, plusieurs études relevées dans la revue de littérature traitent de la perception des usagers et usagères des bibliothèques universitaires (Roberts et al., 2016 ; Schumacher et Ifenthaler, 2018 ; Jones et al., 2020). **Ces travaux portent notamment sur les systèmes d'analyse de l'apprentissage des étudiant.e.s (*learning analytics*)** qui permettent de suivre leurs progrès en continu et d'offrir une forme de récompense pour les encourager à maintenir leurs efforts d'apprentissage. De tels systèmes servent aussi à développer des interventions comportementales et académiques et à justifier le « bien-

fondé » des bibliothèques auprès des utilisateurs et utilisatrices qui ont recours à ces services. L'analyse de ces données d'apprentissage soulève certains enjeux pour des bibliothécaires. Par exemple, les adeptes du *learning analytics* prétendent que certaines données devraient être mutualisées dans un système central « inter-institutions » pour faciliter le développement de projets (Jones et al., 2020), mais ce type d'initiative soulève des préoccupations liées à la protection de la vie privée des étudiants.e.s.

Roberts et al. (2016) ont mené une étude dont l'objectif était d'explorer les connaissances, attitudes et préoccupations des étudiants.e.s face aux systèmes d'analyse de l'apprentissage. Certain.e.s participant.e.s apprécient le fait que ces systèmes les encouragent à progresser, mais ils ne comprennent pas toujours leur nature et leurs implications en termes de données personnelles. En effet, toutes les activités en ligne en relation avec la plateforme de l'école sont cartographiées et liées aux profils des étudiant.e.s. De plus, selon les auteurs, les étudiant.e.s sont écarté.e.s de la prise de décision relative à ces systèmes qui pourtant les concernent directement. Certain.e.s jugeaient cette collecte de données envahissante et se déclaraient méfiant.e.s face à ces pratiques. Outre les risques liés à la vie privée, à l'accès et à la conservation de ces données, les auteurs rapportent que les étudiant.e.s sont enrôlé.e.s dans le système de facto, sans leur consentement ou sans que leur consentement soit éclairé. Les étudiant.e.s ont manifesté leur désir d'obtenir plus de transparence et d'information pour donner leur approbation d'une façon légitime.

Schumacher et Ifenthaler (2018) se sont intéressés au même sujet dans les universités américaines via des entretiens individuels. De façon générale, les répondant.e.s avaient une attitude positive à l'endroit de ces systèmes et souhaitaient les utiliser davantage. Néanmoins, les modalités pour obtenir le consentement des usagers et usagères ont suscité des préoccupations. Seuls deux étudiants ont indiqué qu'ils ne désiraient pas utiliser ces systèmes étant donné les risques liés à la confidentialité et les possibilités d'un trop grand suivi des activités éducatives par les établissements. Les auteurs montrent que

l'attitude positive face à ce système est corrélée à la perception des bénéfices que l'utilisateur ou l'utilisatrice pourra en tirer.

Les deux études (Roberts et al., 2016 ; Schumacher et Ifenthaler, 2018) démontrent ainsi une attitude globalement positive des étudiant.e.s face à la collecte de données d'usage pour des systèmes d'analyse de l'apprentissage. Mais les auteurs insistent sur l'importance d'impliquer toutes les parties prenantes quant à l'utilisation de ce système dans l'enseignement supérieur. Roberts et al. (2016) proposent des pistes de solutions détaillées pour réduire les craintes liées à la protection de la vie privée. Par exemple, **ils suggèrent d'inclure des options telles que « l'opt-in ou l'opt-out » ce qui permet aux participant.e.s de choisir d'y prendre part (ou pas) et de favoriser un consentement éclairé.**

Sur la perception des professionnel.le.s

Tummon et Dawn (2018) se sont intéressés aux attitudes et aux pratiques des bibliothécaires en lien avec la confidentialité en ligne. Leur enquête par sondage montre un consensus des bibliothécaires (97 %) autour du fait que les bibliothèques ne devraient pas partager d'informations personnelles avec des tiers à moins que l'individu en question n'ait donné son consentement, ou si un tribunal en fait la demande. En contrepartie, l'énoncé suggérant que les bibliothèques « font tout ce qu'elles peuvent pour empêcher l'accès non-autorisé aux renseignements personnels des particuliers » ne fait pas l'unanimité : près d'un quart des bibliothécaires (24 %) sont fortement en désaccord ou en désaccord, moins de la moitié (42 %) sont fortement en accord ou en accord et le reste des bibliothécaires ne sont ni en accord ou en désaccord. Ainsi, même si l'enquête de Tummon et Dawn (2018) vient démontrer la présence d'inquiétudes en matière de vie privée, il semble que dans certains cas, **les bibliothécaires ne sont pas certain.e.s des pratiques relatives à la protection de la vie privée dans leur lieu de travail, même s'ils et elles jugent qu'elles sont importantes.** Par exemple, en ce qui a trait aux politiques de confidentialité, 42 % ont mentionné ne pas être au courant si leur institution

communiquait ces informations auprès des utilisateurs et utilisatrices, et 29 % ont dit « non ». Parallèlement, la majorité des répondant.e.s soit 69 % ont aussi souligné qu'ils et elles ne savaient pas si leur bibliothèque avait un protocole ou une formation associée à la protection de la vie privée. À ce résultat, il est également possible d'ajouter le 10 % qui a indiqué « non ». Ainsi, comme le mentionnent Tummon et Dawn (2018), cela laisse sous-entendre qu'environ 79 % de ces répondant.e.s estiment qu'il n'y a pas de politique de protection des données personnelles dans leur institution ou ils et elles l'ignorent tout simplement, ce qui est considérable.

Un constat similaire est posé par Chovet (2019) en France auprès des professionnel.le.s des bibliothèques. Il a interrogé dans son enquête des employé.e.s des bibliothèques universitaires et territoriales quant à l'offre de formation sur la protection de la vie privée des utilisateurs et utilisatrices. Quelques constats ressortent. D'abord, il ne semble pas y avoir beaucoup de formations proposées dans les deux types de bibliothèques pour les membres du personnel. Seulement 25 % dans le cas des bibliothèques universitaires et 17 % pour les territoriales. En direction des publics, très peu de formations sont proposées, soit 6 % contre 13 %. Finalement, les résultats révèlent aussi que la majorité des participant.e.s ignorent l'offre de formation dans leur établissement (47 % et 34 % respectivement).

L'étude de Chovet (2019) dénote aussi que dans la majorité des bibliothèques, **il n'y a pas de procédures pour répondre aux droits des membres du public si certains d'entre eux ont des préoccupations au sujet de leurs données personnelles**. En effet, 67 % des personnes interrogées soutiennent qu'il n'y a pas de procédures dans le cas des bibliothèques universitaires et 59 % en ce qui concerne les bibliothèques territoriales. Il est donc possible d'affirmer que l'enquête de Chovet (2019) arrive à des conclusions similaires que Tummon et Dawn (2018). Dans les deux enquêtes, même si les questions étaient formulées différemment, **la majorité des répondant.e.s n'étaient pas au fait des pratiques et formations sur les questions entourant la protection de la vie privée au sein de leur institution**.

Vitak et al. (2018) se sont penchés plus largement sur les difficultés rencontrées par les bibliothécaires des établissements publics aux États-Unis. Lors de groupes de discussion, les chercheurs ont constaté que les bibliothécaires discernaient les préoccupations en lien avec le traitement des informations personnelles des membres du public. Toutefois, les bibliothécaires éprouvent malgré eux le désir d'aider certaines personnes à effectuer des transactions en ligne. Ces usagers et usagères en question dévoilent ainsi des données personnelles et sensibles parfois, pour qu'on les aide à accomplir leurs tâches. De plus, les bibliothécaires ayant participé à l'étude mentionnent qu'il n'existe pas dans leur institution de politique explicite par rapport aux scénarios auxquels ils et elles sont à l'occasion confronté.e.s. Encore une fois, il est mentionné que les bibliothécaires ne sont pas toujours formés à la gestion des affaires privées et des informations sensibles.

Dès lors, si ces questions ne sont pas toujours bien saisies par les employé.e.s, il est essentiel de se questionner sur les connaissances en matière numérique des publics qui fréquentent ces lieux. Les bibliothèques, par l'intermédiaire de leurs employé.e.s, devraient être un lieu privilégié pour aviser et renseigner ces usagers et usagères. Cela dit, la transmission de ce savoir est plus difficile quand les bonnes pratiques n'existent pas encore dans les bibliothèques, ou qu'elles sont mal comprises par le personnel.

En somme, une forme de confusion se dégage de la littérature. Si les bibliothécaires octroient une importance à la protection de la vie privée et sont d'avis qu'il est nécessaire de ne pas partager les renseignements des membres du public avec un tiers (Tummon et Dawn, 2018), ils et elles ne sont pas toujours bien renseigné.e.s sur les pratiques et formations entourant ces enjeux dans leur bibliothèque (Tummon et Dawn, 2018 ; Chovet, 2019). **Ainsi, la littérature démontre la présence d'ambiguïtés et d'un manque d'information de part et d'autre, tant du côté du personnel que du public, concernant les politiques et pratiques de données.**

CONCLUSION

La collecte, l'analyse, le partage et l'archivage responsable des données d'usage constituent un défi majeur pour les organismes culturels. Au Canada, si la protection de la vie privée est considérée comme un droit fondamental, la capacité des usagers et usagères à offrir un consentement éclairé en contexte numérique serait plus un privilège qu'un droit, car elle nécessite non seulement du temps et un niveau suffisant de littératie numérique. Plus largement, cette protection suppose des services qui prennent en compte dès leur conception une attention de la vie privée.

Du côté des bibliothèques et archives, l'équilibre entre protection des données personnelles et liberté d'accès à l'information est un enjeu documenté de longue date. Le numérique soulève toutefois de nouveaux enjeux liés à l'implantation de services collectant des données d'usage. Bien que des recommandations pour les politiques de confidentialité aient été proposées au Québec, les recherches concluent à une asymétrie d'information entre les organismes et leurs publics concernant les données collectées. Il est donc nécessaire d'enquêter sur les rapports de pouvoir entre les organismes culturels et leurs publics.

De plus, pour mettre en place des pratiques éthiques et durables de gouvernance des données, il convient de sonder les usagers et usagères au sujet de leurs préoccupations et de leurs besoins relatifs à la protection de la vie privée. De cette manière, les membres du public pourraient être davantage inclus dans la définition de ce qui constitue de bonnes pratiques de collecte, d'analyse, de partage et d'archivage des données. Cependant, il est crucial que les modalités de participation et d'inclusion des publics à cette gouvernance assurent une diversité dans la composition sociale des groupes d'intervenants impliqués.

À notre connaissance, il n'existe pas d'enquête auprès des usagers et usagères pour connaître leur perception de la vie privée dans le contexte des bibliothèques et archives au Québec. Une telle enquête permettrait de mieux comprendre le rapport entre ces perceptions et un ensemble de variables sociodémographiques qui caractérisent les différents groupes de publics. Elle cernerait aussi les besoins différenciés de chaque groupe relativement à la gouvernance des données. Plus largement, de tels travaux contribueraient à théoriser la notion de gouvernance de manière originale en croisant la perspective culturelle et la perspective de l'étude critique des données numériques.

ANNEXES

Lois, règlements et documents d'orientation pour l'encadrement de la vie privée et du droit à l'information au Québec et au Canada

LÉGISLATION CANADIENNE

Loi sur l'accès à l'information (L.C.R. (1985), ch. A-1)	<ul style="list-style-type: none">• Dernièrement modifiée en 2020.• Elle confère aux citoyen.ne.s canadien.ne.s, aux résident.e.s permanent.e.s, aux particuliers et aux sociétés présentes au Canada le droit d'accéder aux documents relevant des institutions fédérales, conformément aux principes selon lesquels les renseignements gouvernementaux devraient être accessibles au public. Les exceptions nécessaires de droit d'accès devraient être limitées et précises, et les décisions concernant la communication des renseignements gouvernementaux devrait être examinée indépendamment du gouvernement.
Loi sur la protection des renseignements personnels (L.C.R. (1985), ch. P-21)	<ul style="list-style-type: none">• Dernièrement modifiée en 2019.• Confère à toute personne le droit d'avoir accès aux renseignements personnels la concernant qui sont détenus par le gouvernement du Canada, et de demander que des corrections y soient apportées.• Elle ne s'applique qu'aux données traitées par les institutions gouvernementales fédérales énoncées dans la Loi.
Loi sur la protection des renseignements personnels et les documents électroniques (L.C. 2000, ch.5)	<ul style="list-style-type: none">• Dernièrement modifiée en 2019.• Elle vise à protéger les données et renseignements personnels dans le cadre d'activités économiques tout en effectuant la promotion du commerce en ligne.• Elle s'applique généralement aux renseignements personnels détenus par les organisations du secteur privé. Par exemple, elle s'applique aux fournisseurs tiers enclins de proposer leurs services aux bibliothèques et archives.• Toutes les entreprises qui mènent des activités au Canada et qui traitent des renseignements

	<p>personnels qui vont au-delà des frontières provinciales ou nationales sont assujetties à cette loi.</p>
<p>Projet de loi C-51 Loi antiterroriste 2015 (L.C. 2015, ch.20)</p>	<ul style="list-style-type: none"> • Projet adopté sans amendement. • Nouveaux pouvoirs élargis de collecte et de communication de l'information, admis pour les ministères et certains organismes gouvernementaux. • L'Association canadienne des bibliothèques a réagi à ce projet de loi en mars 2015. Elle avait des préoccupations sur les risques pour la vie privée des Canadiens.ne.s et pour leur liberté d'expression.
<p>Projet de loi C-58 (Sanction royale 21 juin 2019) (LC. 2019, ch.18)</p>	<ul style="list-style-type: none"> • Loi modifiant la Loi sur l'accès à l'information, la Loi sur la protection des renseignements personnels et d'autres lois en conséquence. • Le commissaire à l'information a maintenant le pouvoir « de rendre des ordonnances exécutoires à l'égard des demandes d'accès à l'information. » C'est le cas de la communication des dossiers du Canada. • Le projet de loi a entre autres ajouté un nouvel article à la <i>Loi sur l'accès à l'information</i>, soit, la publication proactive. Cet article exige que « les institutions publient de façon proactive différents types de renseignements particuliers d'intérêt pour le public. » Il n'est donc plus nécessaire de présenter une demande.
<p>Projet de loi C-11 Loi de 2020 sur la mise en œuvre de la Charte numérique</p>	<ul style="list-style-type: none"> • Première lecture le 17 novembre 2020. D'autres amendements sont possibles. • Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le Tribunal de la protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois. • Dans la section <i>Objet et champ d'application</i> para. 5, il est mentionné que « la présente loi a pour objet de fixer, dans une ère où les données circulent constamment au-delà des frontières et des limites géographiques et une part importante de l'activité économique repose sur l'analyse, la circulation et

l'échange de renseignements personnels, des règles régissant la protection des renseignements personnels d'une manière qui tient compte **du droit à la vie privée des individus** quant aux renseignements personnels qui les concernent et **du besoin des organisations** de recueillir, d'utiliser ou de communiquer des renseignements personnels **à des fins qu'une personne raisonnable estimerait acceptable dans les circonstances.** »

- Dans la section *Responsabilité des organisations* para. 7(2), il est précisé que « les renseignements personnels relèvent de l'organisation qui décide de les recueillir et établit les fins pour lesquelles ils sont recueillis, utilisés ou communiqués, qu'elle les recueille, utilise ou communique elle-même ou qu'un fournisseur de services le fasse pour elle. »
- Le para. 9(1) de la même section souligne aussi la mise en œuvre d'un programme de gestion de la protection des renseignements personnels qui doit inclure « les politiques, les pratiques, et les procédures qu'elle a mise en place afin de respecter les obligations qui lui incombent sous le régime de la présente loi. »
- Il établira un nouveau Tribunal de la protection des renseignements personnels et des données pour saisir les appels à propos des ordonnances émises par le CPVP et pour établir **et imposer aux organisations les amendes recommandées**, encore une fois par le CPVP. S'il n'y a pas de changement, il est aussi possible pour les individus de **disposer d'un droit privé d'action** pour les dommages réels subis.

Charte canadienne des droits et libertés (Loi constitutionnelle de 1982)

- L'article 8 stipule que « chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. »
- Selon la Cour suprême du Canada, l'objet de cet article « est de protéger les attentes raisonnables en matière de vie privée ».

LÉGISLATION QUÉBÉCOISE

<p>Loi sur la protection des renseignements personnels dans le secteur privé (RLRQ c P-39.1)</p>	<ul style="list-style-type: none">• Entrée en vigueur en janvier 1994 et dernièrement modifiée en 2017.• C'est la loi applicable au traitement de données personnelles opéré par les entreprises. Elle vient remplacer la <i>Loi du Canada 2000, ch. 5.</i>
<p>Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ c A-2.1)</p>	<ul style="list-style-type: none">• Entrée en vigueur en octobre 1982 et modifiée en 2020.• Concerne les bibliothèques au Québec, peu importe si le financement public représente la totalité ou seulement une partie par le gouvernement.• Elle s'applique à tous les renseignements que possède un organisme public lors de ses fonctions, et ce même si la sauvegarde de ceux-ci provient d'un tiers.• Dans le Chapitre 3 (<i>protection des renseignements personnels</i>), section I, cette loi mentionne qu'à l'origine les renseignements personnels sont considérés confidentiels, à moins que la personne impliquée autorise de son propre gré leur publication. Si la personne est mineure, l'autorisation peut être donnée par le titulaire de l'autorité parentale. <p>Section II (Collecte, conservation et utilisation de renseignements nominatifs).</p> <ul style="list-style-type: none">• Dans l'article 63.1, il est précisé qu'un « organisme public doit prendre des mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support. »• Dans l'article 64, il est indiqué « nul ne peut, au nom d'un organisme public, recueillir un renseignement personnel si cela n'est pas nécessaire à l'exercice des attributions de cet

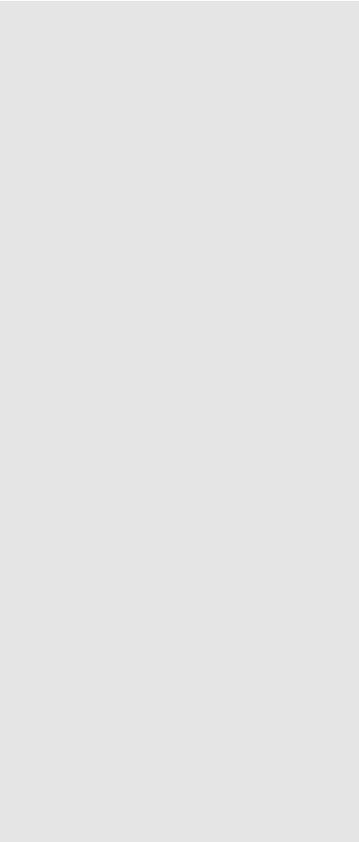
	<p>organisme ou à la mise en œuvre d'un programme dont il a la gestion. »</p>
<p><i>Code civil</i> du Québec (RLRQ c CCQ-1991)</p>	<p>Le Chapitre 3 concerne « le respect de la réputation et de la vie privée ».</p> <ul style="list-style-type: none"> • À l'article 35, la notion de consentement est exprimée formellement : « nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci y consente ou sans que la loi l'autorise. » • À l'article 36 il est également considéré une atteinte à la vie privée la « surveillance de la vie privée par quelque moyen que ce soit ».
<p>Charte des droits et libertés de la personne (RLRQ c C-12)</p>	<p>Dans le Chapitre 1 (Libertés et droits fondamentaux).</p> <ul style="list-style-type: none"> • L'article 1 stipule « tout être humain a droit à la vie, ainsi qu'à la sûreté, à l'intégralité et à la liberté de sa personne. Ensuite, l'article 4 soutient « toute personne a droit à la sauvegarde de sa dignité, de son honneur et de sa réputation ». • L'article 5 mentionne très brièvement « toute personne a droit au respect de sa vie privée ». • Enfin, l'article 44 souligne que « toute personne a droit à l'information, dans la mesure prévue par la loi. »
<p>Loi sur Bibliothèque et Archives nationales du Québec (RLRQ C B-1.2)</p>	<ul style="list-style-type: none"> • Dernièrement modifié en 2015. <p>Chapitre II (<i>Missions et pouvoirs</i>)</p> <ul style="list-style-type: none"> • L'article 14 énonce « Bibliothèque et Archives nationales a pour mission de rassembler, de conserver de manière permanente et de diffuser le patrimoine documentaire québécois publié et tout document qui s'y rattache et qui présente un intérêt culturel, de même que tout document relatif au Québec et publié à l'extérieur du Québec. Il a également pour mission d'offrir un accès démocratique au patrimoine documentaire constitué par ses collections, à la culture et au savoir et d'agir, à cet égard, comme catalyseur auprès des institutions documentaires

québécoises, contribuant ainsi à l'épanouissement des citoyens. »

- L'article 15.1 mentionne que « Bibliothèque et Archives nationales a également pour mission d'encadrer, de soutenir et de conseiller les organismes publics en matière de gestion de leurs documents, d'assurer la conservation d'archives publiques, d'en faciliter l'accès et d'en favoriser la diffusion. Il est aussi chargé de promouvoir la conservation et l'accessibilité des archives privées. »

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (PL-64)

- Présenter le 12 juin 2020.
- Plusieurs lois seraient modifiées par ce projet de loi s'il est accepté dans sa forme actuelle. C'est entre autres le cas de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels dans le secteur privé*.
- Le projet de loi introduit des règles à propos du « traitement des incidents affectant la confidentialité des renseignements personnels par les organismes publics et les entreprises ». De plus, « **il oblige ces organismes et ces entreprises à publier des règles encadrant la gouvernance à l'égard des renseignements personnels et, pour ceux qui recueillent ces renseignements par un moyen technologique, à publier et diffuser une politique de confidentialité** ». De plus, dans certaines circonstances, une exigence d'une « évaluation des facteurs relatifs à la vie privée » pourrait être demandée. C'est notamment le cas « **de tout projet de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels** ».
- Il a aussi pour intention de spécifier des exigences quant « **au consentement requis préalablement** à une collecte, une utilisation ou une communication de renseignements personnels. »



Dès lors, il prévoit « que les organismes publics et les entreprises doivent demander à la personne concernée son consentement distinctement de toute autre information communiquée à cette dernière. » De plus, il recommande « que le consentement nécessaire à certaines utilisations ou communications d'un **renseignement personnel sensible doit être manifesté de façon expresse.** »

- Des précisions sont énoncées sur « les obligations des organismes publics et des entreprises quant à la conservation des renseignements personnels, **en prévoyant notamment la possibilité d'anonymiser ces renseignements** ».
- Il prévoit également de « **retirer aux entreprises la possibilité de communiquer, sans le consentement des personnes concernées, des listes nominatives** et révisé les règles encadrant l'utilisation des renseignements personnels à des fins de prospection commerciale ou philanthropique ».

DOCUMENTS D'ORIENTATION DU SECTEUR DES BIBLIOTHÈQUES AU QUÉBEC ET AU CANADA

Association des bibliothèques publiques du Québec, *Lignes directrices pour les bibliothèques publiques du Québec*

- Publié en 2019

Dans le chapitre 3 (*Planification*)

- Le point 3.18 soutient que « la bibliothèque consulte régulièrement ses usagers et les non-usagers de la bibliothèque sur ses différents services au moyen de sondages, de groupes de discussion, d'entrevues formelles ou informelles, d'une boîte à idées, d'activités de cocréation, etc. Le résultat de ces consultations ainsi que l'analyse des plaintes et des commentaires formulés par le public alimentent la planification stratégique de la bibliothèque. »
- Le point 3.23 mentionne que « la récolte et l'analyse de données quantitatives et qualitatives sur les services de la bibliothèque font partie intégrante des activités de gestion de la bibliothèque ».

Dans le chapitre 6 (*Services*)

- Il est précisé dans l'introduction que « la bibliothèque met tout en œuvre pour favoriser l'autonomie de l'utilisateur. Elle étend son rayon d'action au-delà de ses frontières physiques, grâce à des actions hors les murs, mais également à l'aide de technologies qui lui permettent d'offrir ses services à distance. Elle s'emploie également à créer les conditions qui facilitent et rendent agréable et conviviale la relation entre le public et les divers services et activités qu'elle propose. »
- Le point 6.4 indique que « **la bibliothèque possède une politique qui assure la confidentialité des renseignements personnels** contenus dans ses divers registres et banques de données. » De plus, elle est soumise à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

- Le point 6.59 mentionne qu'elle a un **fichier des abonnés**. « En plus des renseignements personnels habituels, ce fichier peut contenir la **description de profils d'intérêt ou des données de géolocalisation**. Il peut également faire partie d'un fichier plus large constitué par l'organisme responsable (municipalité ou autres) qui intègre l'ensemble des services offerts à la population. **Le personnel ayant accès à ce fichier connaît et respecte les règles relatives à la confidentialité et à la protection des renseignements personnels** ».

Dans le chapitre 8 (Ressource documentaires et autres collections)

- Le point 8.1 énumère des concepts pour sa politique de développement des collections : liberté intellectuelle, lutte contre la censure, équilibre, flexibilité, indépendance professionnelle, intérêts de la communauté, voix des citoyens, concertation et complémentarité des collections.

Dans le chapitre 9 (Ressources technologiques)

- Le point 9.22 mentionne que « la bibliothèque analyse et sélectionne les systèmes et applications destinés au personnel et au public, en collaboration avec les services informatiques. » Plus particulièrement, à propos de la conservation des données. « Elle vérifie que **les données gérées par les logiciels, sont sécurisées, extractibles et exportables.** »
- À l'égard de la *sécurité et stabilité des systèmes*, le point 9.40 soutient qu'elle « prend toutes les mesures nécessaires pour assurer la fiabilité de ses systèmes informatiques. ». Ensuite, le point 9.41 stipule qu'elle « adopte des procédures éprouvées pour la sécurité, la sauvegarde, la validation et la restauration de ses données. » À l'égard des filtres, « les postes d'accès public à Internet ne sont soumis à aucun filtres susceptible de brimer le droit à l'information de l'utilisateur. »

<p>Code d'éthique de la Fédération canadienne des associations de bibliothèques</p>	<ul style="list-style-type: none"> • Approuvé le 27 août 2018. <p>Le point 3 (Vie privée, intimité, transparence).</p> <ul style="list-style-type: none"> • « Les bibliothécaires et les autres professionnel(le)s de l'information respectent la vie privée et la protection des données personnelles partagées, de fait, entre les usagers et les institutions. » • « Les relations entre les usagers et la bibliothèque sont confidentielles et les bibliothécaires et les autres professionnel(le)s de l'information prendront les mesures appropriées pour garantir que les données ne soient pas utilisées à d'autres fins que celle de l'usage pour lequel elles ont été recueillies. »
<p>Association des bibliothèques publiques du Québec (Table permanente de concertation des bibliothèques québécoises)</p>	<ul style="list-style-type: none"> • Publié en octobre 2016. • « Comme le proclame l'UNESCO, la raison d'être de la bibliothèque est d'assurer un accès libre et illimité à la connaissance, la pensée, la culture et l'information. » • « La bibliothèque est le lieu par excellence où l'accès aux ressources documentaires ou culturelles se fait librement et sans discrimination. » • « La bibliothèque outille ses usagers et rend accessible et diffuse le savoir afin que ceux-ci puissent développer des compétences en recherche et en évaluation de l'information. Ces compétences leur sont aussi utiles dans l'exercice de leurs droits démocratiques et peuvent les aider à jouer un rôle actif au sein de leur communauté. » • « La médiation numérique est au cœur des services de la bibliothèque, que ce soit par la formation aux outils technologiques ou par la mise à la disposition d'outils et de ressources documentaires numériques. Ainsi, elle contribue à réduire la fracture numérique et favorise l'acquisition de compétences technologiques. » • « La bibliothèque est un investissement collectif et social. En favorisant l'instruction, l'éducation, le perfectionnement et l'intégration sociale, elle contribue au développement des individus et de la

société, notamment en étant un vecteur de réduction des inégalités. »

Fédération canadienne
des associations
bibliothèques, *Énoncé
sur la diversité et
l'inclusion*

- Publié le 25 mai 2008.
- La Fédération « estime qu'une société pluraliste et diversifiée est au cœur de notre identité nationale. Les bibliothèques se doivent de contribuer à une culture qui apprécie la diversité et favorise l'inclusion sociale. »
- « Elles veillent à ce que les personnes puissent jouir des services sans que leur soient imposées par autrui des valeurs, des coutumes ou des croyances. »

BIBLIOGRAPHIE

Abraham, Rene, Schneider, Johannes et Jan Vom Brocke. (2019) « Data governance: A conceptual framework, structured review, and research agenda ». *International Journal of Information Management*, 49 : 424-438.

Affonso, Elaine Parra et Ricardo Cesar Gonçalves Sant'Ana. (2018). « Privacy awareness issues in user data collection by digital libraries ». *IFLA journal*, 44(3) : 170-182.

Amar, Muriel, Evans, Christophe et Agnès Vigué-Camus. (2016-2017). « Études et recherches récentes sur les usages numériques à la Bpi ». *Culture et Recherche, Les publics in situ en ligne*, Hiver (134) : 47-48.

Apprich, Clemens, Kyong Chun, Wendy Hui, Cramer, Florian et Hito Steyerl. (2018). *Pattern discrimination*. Lüneburg, Germany: Meson Press, 123 p.

Ashton, Daniel et Ronda Gowland-Pryde. (2019). « Arts audience segmentation : data, profiles, segments and biographies ». *Cultural Trends*, 28(2/3): 146-161.

Association des Bibliothécaires de France (ABF). (2018). *Charte du droit fondamental des citoyens à accéder à l'information et aux savoirs par les bibliothèques*. Bib'lib: Bibliothèque pour l'accès Libre à l'information et aux savoirs. En ligne. http://www.abf.asso.fr/fichiers/file/ABF/biblib/charte_biblib_abf.pdf. (Consulté le 22 juin 2021).

Association des Bibliothécaires de France (ABF). (2017). *Communiqué : L'ABF s'engage pour que les bibliothèques restent un espace de liberté pour s'informer*. En ligne. <http://www.abf.asso.fr/1/183/646/ABF/-communiquelabf-sengage-pour-que-les-bibliotheques-restent-un-espace-de-liberte-pour-sinformer>. (Consulté le 22 juin 2021).

Association des bibliothèques publiques du Québec (ABPQ). (2019). *Lignes directrices pour les bibliothèques publiques du Québec*. Publié par l'Association des bibliothèques publiques du Québec, BANQ et le Réseau BIBLIO du Québec, 144 p. En ligne. http://lignesdirectricesbiblioquebec.ca/pdf/lignes_directrices_biblio_2019.pdf. (Consulté le 22 juin 2021).

Autorité canadienne pour les enregistrements Internet (ACEI). (2020). *Attitudes des Canadiens sur les enjeux relatifs à l'Internet*. En ligne. <https://www.cira.ca/fr/resources/letat-de-linternet/rapport/attitudes-des-canadiens-sur-les-enjeux-relatifs-a-linternet>. (Consulté le 22 juin 2021).

Azzaria, Georges et Hélène Zimmermann. (2019). « Pratiques et représentations des internautes québécois en matière de consentement, de droit à la vie privée et de droit d'auteur ». *Lex-Electronica* 24, hors-série, 48 p.

Badouard, Romain, Musiani, Francesca, Méadel, Cécile et al. (2012). « Towards a typology of Internet governance socio-technical arrangements ». In *Normative Experience in Internet Politics*, sous la dir. de Françoise Massit-Folléa, Cécile Méadel et Laurence Monnoyer-Smith. Coll. « Sciences Sociales ». Paris : Presses des Mines, 99-124.

Badouard, Romain, Mabi, Clément et Guillaume Sire. (2016). « Inciter, contraindre, encadrer. Trois logiques de gouvernementalité numérique ». *French Journal for Media Research*, (6) : 2-17.

Baillargeon, Jean-Paul (sous la dir.). (1996). *Les publics du secteur culturel. Nouvelles approches*. Coll. « Culture et Société ». Laval : Presses universitaires de Laval, 192 p.

Barnes, Susan B. (2006). « A privacy paradox: social networking in the United States ». *First Monday*, 11(9). En ligne.
<https://firstmonday.org/ojs/index.php/fm/article/view/1394/1312>. (Consulté le 22 juin).

Barth, Susanne, de Jong, Meno D.T., Junger, Marianne, Hartel, Pieter H. et Janina C. Roppetl. (2019). « Putting the privacy paradox to the test: online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources ». *Telematics and informatics*, 41 : 55-69.

Black, Carolyn, Setterfield, Lucy et Rachel Warren. (2018). *Online data privacy from attitudes to action: an evidence review*. Edinburgh: Ipsos MORI Scotland for Carnegie UK Trust, 46 p.

Beauchemin, William-J., Maignien, Noémie et Nadia Duguay. (2020). *Portraits d'institutions culturelles montréalaises. Quels modes d'action pour l'accessibilité, l'inclusion et l'équité ?* Sainte-Foy : PUL, 410 p.

Beaudouin, Valérie, Garron, Isabelle et Nicolas Rollet. (2016). « “Je pars d'un sujet, je rebondis sur un autre” : pratiques et usages des publics de Gallica ». Rapport de recherche. Paris : Télécom ParisTech ; Bibliothèque nationale de France ; Labex Obvil, 29 p.

Beaudouin, Valérie et Jérôme Denis. (2016-2017). « Le renouvellement des dispositifs de connaissance des publics ». *Culture et Recherche, Les publics in situ en ligne*, Hiver (134) : 45-46.

Beck, Estelle. (2018). « Les données personnelles des usagers en bibliothèque : de beaux défis de gestion en perspective ». *Documentation et bibliothèques*, 64(1): 16-27.

Beer, David. (2016). *Metric power*. Londres : Palgrave Macmillan, 223 p.

Beer, David. (2015). « Productive measures: culture and measurement in the context of everyday neoliberalism ». *Big Data & Society*, Mai, 1-12.

Beer, David et Roger Burrows. (2013). « Popular culture, digital archives and the new social life of data ». *Theory, Culture and Society*, 30(4): 47–71.

Bellman, Steven, Johnson, Eric J., Kobrin, Stephen J. et Gerald L. Lohse. (2004). « International differences in information privacy concerns: a global survey of consumers ». *Information Society*, 20(5): 313-324.

Benghozi, Pierre-Jean et Françoise Benhamou. (2008). « Longue traîne : levier numérique de la diversité culturelle ? ». *Culture prospective*, 1(1) : 1-11.

Bennett, Colin J. et Christopher Parsons. (2013). « Privacy and surveillance: the multidisciplinary literature on the capture, use and disclosure of personal information in cyberspace ». In *The Oxford Handbook of Internet Studies*, sous la dir. de William H. Dutton. Oxford : Oxford University Press, 486-508.

Bergstrom, Annika. (2015). « Online privacy concerns: a broad approach to understanding the concerns of different groups for different uses ». *Computers in Human Behavior*, 53: 419-426.

Bertot, John Carlo, Estevez, Elsa et Tomasz Janowski. (2016). « Universal and contextualized public services: digital public service innovation framework ». *Government Information Quarterly*, (33) : 211-222.

Bloche, Patrick et Patrice Verchère. (2011). *Rapport d'information sur les droits de l'individu dans la révolution numérique*. Paris : Assemblée nationale (France). Document 3560, 384 p.

Boisselet, Romain. (2018). « (Auto)-censure et surveillance de masse, quels impacts pour les bibliothèques ? ». *Bulletin des Bibliothèques de France*, 15. En ligne. https://bbf.enssib.fr/tour-d-horizon/auto-censure-et-surveillance-de-masse-quels-impacts-pour-les-bibliotheques_68537. (Consulté le 22 juin 2021).

Bonet, Lluís et Emmanuel Négrier. (2018). « The participative turn in cultural policy: Paradigms, models, contexts ». *Poetics*, 66 : 64-73.

Bowers, Stacey L. (2006). « Privacy and Library Records ». *The Journal of Academic Librarianship*, 32(4): 2377-2383.

Bowers, Stacey L. (2008). « Self-Service Holds: A Violation of Library Patrons' Privacy ». *Libraries*, 47(4): 54-57.

boyd, danah et Kate Crawford. (2012). « Critical questions for Big Data: Provocations for a cultural, technological and scholarly phenomenon ». *Information, Communication & Society*, 15(5): 662–679.

Brites, Marie-José, Chimirri, Niklas Alexander, Amaral, Inês, Seddighi, Gilda, Torres da Silva, Marisa et Maria Francesca Murru. (2018). « Stakeholder discourses about critical literacies and audience participation ». In *The Future of Audiences: A foresight analysis of interfaces and engagement*, sous la dir. de Ranjana Das et Brita Ytre-Arne. Londres : Palgrave Macmillan, 179-195.

Brown, Wendy. (2015). *Undoing the demos: neoliberalism's stealth revolution*. New York: Zone Books, 296 p.

Bygrave, Lee A. et Jon Bing. (2009). *Internet Governance. Infrastructure and Institutions*. Oxford: Oxford University Press, 246 p.

Caillet, Bruno. (2016-2017). « Quelles réponses au procès d'élitisme fait aux structures culturelles ? ». *Culture et Recherche, Les publics in situ et en ligne*, Hiver (134) : 36-39.

Calimaq. (2018). « Archives et RGDP : le droit à la mémoire comme manifestation d'un droit social des données ». *S.I.Lex*. En ligne : <https://scinfolex.com/2018/04/13/du-droit-a-la-memoire-comme-manifestation-dun-droit-social-des-donnees>. (Consulté le 22 juin 2021).

Campbell, D Grant et Scott R Cowan. (2016). « The paradox of privacy: Revisiting a core library value in an age of big data and linked data ». *Library Trends*, 64(3) : 492-511.

Cardon, Dominique. (2015). *À quoi rêvent les algorithmes. Nos vies à l'heure des big data*. Paris : Seuil, 112 p.

Cardon, Dominique. (2019). *Culture numérique*. Coll. « Hors collection ». Paris : Presses de Sciences Po, 432 p.

Cardon, Dominique et Julien Levrel. (2009). « La vigilance participative. Une interprétation de la gouvernance de Wikipédia ». *Réseaux*, 2(154) : 51-89.

Casemajor, Nathalie, Bellavance, Guy et Guillaume Sirois avec la collaboration de Marika Laforest, Louise Sicuro, Nathalie Leduc, Louise Boucher, Martine El Ouardi, Romuald Jamet, Morad Jeldi et Annie Perron. (2018). *Pratiques culturelles numériques et plateformes participatives. Opportunités, défis et enjeux*. FRQSC Action concertée sur la culture et le numérique - Synthèse des connaissances. Montréal : INRS, 188 p.

Cavoukian, Ann. (2006). *Privacy by Design: The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices*. Toronto : Commissariat à l'information et à la vie privée de l'Ontario, 12 p.

Chen, Hsin-Liang, Doty, Philip, Mollman, Carol, Niu, Xi, Yu, Jen-chien et Tao Zhang. (2015). « Library Assessment and Data Analytics in the Big Data Era: Practices and Policies ». *Library and Learning Resources*, 52(1) : 1-4.

Chovet, Marion. (2019). « La protection de la vie privée des lecteurs par les bibliothécaires français ». Mémoire d'étude. Lyon : Université de Lyon (ENSSIB), 115 p.

Canadian Library Association. (2015). « CLA Statement on Bill C-51, the Anti-terrorism Act, 2015 ». *cla.ca*. En ligne : <http://cla.ca/wpcontent/uploads/CLA Stmt C51 anti terrorism 13mar2015 final ltrhd.pdf>. (Consulté le 22 juin 2021).

Cliche, Dominic. (2017). *La ville intelligente au service du bien commun : Lignes directrices pour allier l'éthique au numérique dans les municipalités au Québec*. Québec : Gouvernement du Québec, Commission de l'éthique en science et en technologie, 128 p.

Commission Nationale Informatique et Libertés (CNIL). (2017). *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*. Paris : CNIL, 80 p.

Commissariat à la protection de la vie privée du Canada (CPVPC). (2019). *Réforme des droits sur la vie privée : Pour faire respecter les droits et rétablir la confiance envers le gouvernement et l'économie numérique. Rapport annuel au Parlement 2018-2019 concernant la Loi sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels et les documents électroniques*. Ottawa : CPVPC, 1913-3375.

Couldry, Nick et Alison Powell. (2014). « Big Data from the Bottom Up ». *Big Data & Society*, 1(2) : 1-5.

Crawford, Kate, Miltner, Kate et Gray Mary. L. (2014). « Critiquing Big Data: Politics, ethics, epistemology ». *International Journal of Communication*, (8) : 1663–1672.

Das, Ranjana et Brita Ytre-Arne. (2018). *The Future of Audiences: A Foresight Analysis of Interfaces and Engagement*. Londres : Palgrave Macmillan, 309 p.

D'Alché-Buc, Florence, Beaudoin, Valérie, Bermès, Emmanuelle, Chevallier, Philippe, Le Moullec-Rieux, Aude, Nouvellet, Adrien, Prieur, Christophe et François Roueff. (2017).

Analysis of Gallica and Data BnF logs and Modelling of Behaviour Patterns: Presentation of the Main Results. Research Report. Paris: Bibliothèque nationale de France (BnF), Télécom ParisTech, 6 p.

Dalton, Russell. (2004). *Democratic Challenges, Democratic Choices: The Erosion in Political Support in Advanced Industrial Democracies*. Oxford: Oxford University Press. 242 p.

Derbas Thibodeau, François R. et Christian Poirier. (2019). « Bibliothèques publiques et virage citoyen : enjeux institutionnels et communicationnels ». *Communiquer*, (26) : 47-66.

Déziel, Pierre Luc, Benyekhlef, Karim et Ève Gaumont. (2020). *Repenser la protection des renseignements personnels à la lumière des défis soulevés par l'IA : Document de réponse aux questions posées par la Commission d'accès à l'information du Québec dans le cadre de la consultation sur l'intelligence artificielle*. Montréal : Laboratoire de Cyberjustice et Observatoire international sur les impacts sociétaux de l'IA et du numérique, 39 p.

Dilhac, Marc-Antoine, Abrassart, Christophe et Nathalie Voarino (sous la dir.). (2018). *Rapport de la Déclaration de Montréal pour un développement responsable de l'intelligence artificielle*. Montréal : Université de Montréal. En ligne. <https://papyrus.bib.umontreal.ca/xmlui/handle/1866/22498>. (Consulté le 22 juin 2021).

Direction générale de l'action contre le racisme du gouvernement de l'Ontario (DGACR). (2018). *Normes relatives aux données en vue de repérer et de surveiller le racisme systémique*. Toronto : DGACR, 100 p.

Donnat, Olivier. (2016-2017). « La question du public, d'un siècle à l'autre ». In *Culture et Recherche, Les publics in situ et en ligne*, Hiver (134): 6-8.

Dourish, Paul. (2016). « Algorithms and their others: Algorithmic culture in context ». *Big Data & Society*, 1-11.

Elmer, Greg. (2003). *Profiling Machines: Mapping the Personal Information Economy*. Cambridge, MA: MIT Press, 176 p.

Elmer, Greg, Ganaele, Langlois et Joanna Redden. (2015). *Compromised data: From Social Media to Big Data*. New York: Bloomsbury Academic, 296 p.

Esquenazi, Jean-Pierre. (2010). *Sociologie des publics*. Coll. « Repères ». Paris : La Découverte, 128 p.

- Fawcett, Paul, Flinders, Matthew, Hay, Colin et Matthew Wood (sous la dir.). (2017). *Anti-Politics, Depoliticization, and Governance*. Oxford : Oxford University Press, 352 p.
- Fédération canadienne des associations de bibliothèques. (2008). *Énoncé sur la diversité et l'inclusion*. Ottawa : FCAB. En ligne. <http://cfla-fcab.ca/fr/lignes-directrices-et-exposes-de-position/enonce-sur-la-diversite-et-linclusion/>. (Consulté le 22 juin 2021).
- Feng, Xiangjun et Weimei Pan. (2016). « Determinants of User Acceptance of Electronic Recordkeeping Systems: A User-Focused Empirical Study of System Characteristics ». *Canadian Journal of Information and Library Science*, 40(2) : 124-151.
- Fraser, Nancy. (1990). « Rethinking the public sphere: A contribution to the critique of actually existing democracy ». *Social Text*, (25/26): 56-80.
- Freeman, Lisa M. et Nick Blomley. (2019). « Enacting property: Making space for the public in the municipal library ». *Environment and Planning C: Politics and Space*, 37(2): 199-218.
- Gambs, Sébastien. (2020). « Respect de la vie privée et problématiques éthiques à l'ère des données massives ». Présentation. Colloque *Éthique, justice et connaissance* organisé par le Centre de recherche en éthique de Montréal. En ligne. https://www.ciqss.org/sites/default/files/documents/S%C3%A9bastien%20Gambs_%C3%A9thiques.pdf. (Consulté le 22 juin 2021).
- Gillespie, Tarleton. (2014). « The Relevance of Algorithms ». In *Media Technologies: Essays on Communication, Materiality and Society*, sous la dir. de Gillespie Tarleton, Pablo J. Boczkowski et Kristen A. Foot. Cambridge, MA : MIT Press, 167-193.
- Gitelman, Lisa. (2013). *Raw data is an oxymoron*. Cambridge, MA : MIT Press, 192 p.
- Godinho, Myron A, Ann Borda, Timothy Kariotis, Andreea Molnar, Patty Kostkova et Siaw-Teng Liaw (2021). « Knowledge co-creation in participatory policy and practice: Building community through data-driven direct democracy. » *Big Data & Society*, 8(1): 205395172111019430.
- Goldsmith, Jack et Tim Wu. (2006). *Who Controls the Net? Illusions of a Borderless World*. Oxford: Oxford University Press, 175 p.
- Hadley, Steven et Elenora Belfiore. (2018). « Cultural Democracy and Cultural Policy ». *Cultural Trends*, 27(3), 218-223.
- Hadley, Steven, Johanson, Kayta, Walmsley, Ben et Anne Torreggiani. (2019). « Reflections on Audience Data and Research ». *Cultural Trends*, 28(2/3) : 81-85.

- Hamel, Pierre et Bernard Jouve. (2006). *Un modèle québécois ? Gouvernance et participation dans la gestion publique*. Montréal : Les Presses de l'Université de Montréal, 142 p.
- Hanquinet, Laurie, O'Brien, Dave et Mark Taylor. (2019). « The coming crisis of cultural engagement? Measurement, methods, and the nuances of niche activities ». *Cultural Trends*, 28(2/3) : 198-219.
- Hoffman, Christian Pieter, Christoph Lutz et Giulia Ranzini. (2016). « Privacy cynicism: A new approach to the privacy paradox ». *Journal of Psychosocial Research on Cyberspace*, 10(4), article 7.
- Iliadis, Andrew et Federica Russo. (2016). « Critical data studies: An introduction ». *Big Data & Society*, 1-7.
- Irwin, Bill. (2012). « The Value of a Communitarian Approach to Public Library Board Governance: Rejecting Current Neoliberal Practice ». *Canadian Journal of Information and Library Science*, 36(1): 1-15.
- Jacquet, Amandine. (2017). *Bibliothèques troisième lieu*. Paris : Association des bibliothécaires de France (ABF), 200 p.
- Jahjah, Marc. (2017). *État de l'art théorique, méthodologique et critique sur les usages et les pratiques, état de l'art - Phase 1*. Paris : Bibliothèque nationale de France (BnF), Observatoire de la vie littéraire et Telecom ParisTech, 19 p.
- Jamali, Hamid R., Nicholas, David et Paul Huntington. (2005). « The use and users of scholarly e-journals: A review of log analysis studies ». *Aslib Proceedings, New Information Perspectives*, 57(6) : 554-571.
- Jauréguiberry, Francis et Serge Proulx. (2011). *Usages et enjeux des technologies de communication*. Coll. « Société-Poche ». Toulouse : Erès, 144 p.
- Johnson, Bobbie. (2010). « Privacy no longer a social norm, says Facebook founder ». *The Guardian*. En ligne.
<https://www.theguardian.com/technology/2010/jan/11/facebook-privacy>. (Consulté le 22 juin 2021).
- Jones, Kyle M.L., Briney, Kristin A., Goben, Abigail, Salo, Dorothea, Asher, Andrew et Michael R. Perry. (2020). « A comprehensive primer to library learning analytics practices, initiatives, and privacy issues ». *College & Research Libraries*, 81(3): 570-591.

Kennedy, Helen. (2015). « Is data culture? Data analytics and the cultural industries ». In *The Routledge Companion to the Cultural Industries*, sous la dir. de Kate Oakley et Justin O'Connor. Londres : Routledge, 398-407.

Kennedy, Helen et Giles Moss. (2015). « Known or knowing publics? Social media data mining and the question of public agency ». *Big Data and Society*, 1-11.

Kennedy, Helen, Steedman, Robin et Rhianne Jones. (2020a). « Approaching public perceptions of datafication through the lens of inequality: a case study in public service media ». *Information, Communication & Society*, 1-17.

Kennedy, Helen, Hartman, Todd, Steedman, Robin et Rhianne Jones. (2020b). « Public perceptions of good data management: Findings from a UK-based survey ». *Big Data & Society*, 1-16.

Kennedy, Helen., Oman, Susan., Taylor, Mark., Bates, Jo et Robin Steedman. (2020c). *Public understanding and perceptions of data practices: a review of existing research*. Living with data. Sheffield: University of Sheffield, 65 p.

Kennedy, Helen Oman, Susan, Taylor, Mark, Bates, Jo et Robin Steedman. (2020d). « Methods ». *Living with data*. Sheffield: University of Sheffield. En ligne. <https://livingwithdata.org/current-research/methods/>. (Consulté le 22 juin 2021).

Kitchin, Rob et Tracey P. Lauriault. (2014). « Towards critical data studies: charting and unpacking data assemblages and their work ». *The Programmable City Working Paper 2*, 19 p.

Kooiman, Jan. (2003). *Governing as governance*. Londres : Sage, 264 p.

Koikkalainen, Petri. (2011). « Social Inclusion ». In *The SAGE Handbook of Governance*, sous la dir. de Mark Bevir. Londres : Sage, 454-467.

Kukutai, Tahu et John Taylor (sous la dir.). (2016). « Data sovereignty for indigenous peoples: current practices and future needs ». In *Indigenous Data Sovereignty: Toward an Agenda*. Canberra: Australian National University Press, 317 p.

Laboratoire de Cyberjustice pour IVADO et Synapse C. (2019). *Guide de bonnes pratiques concernant la création de politiques de confidentialité dans le secteur de la culture*. Montréal : Laboratoire de Cyberjustice, 29 p.

Lahire, Bernard. (2009). « Entre sociologie de la consommation culturelle et sociologie de la réception culturelle ». *Idées économiques et sociales*, (1) : 6-11.

- Laprise, John et Francesca Musiani. (2015). « Internet Governance ». *International Encyclopedia of Digital Communication and Society*, sous la dir. de Peng Hwa Ang et Robin Mansell. New York: Wiley-Blackwell, 1-9.
- Larson, Ronald. (2019). « Library stakeholder attitudes and new technology ». *Library Management*, 40(1/2): 28-140.
- Lefebvre, Elsie et Jean-Sébastien Bélanger. (2020). *Donner par la donnée*. Atelier numérique, Synapse C. En ligne. <https://www.facebook.com/watch/?v=264806881290350>. (Consulté le 22 juin 2021).
- Le Figaro avec Reuters. (10 février 2017). « Le délit de consultation des sites djihadistes annulé (Conseil constitutionnel) ». *Le Figaro*. En ligne. <https://www.lefigaro.fr/flash-actu/2017/02/10/97001-20170210FILWWW00084-le-delit-consultation-des-sites-djihadistes-annule.php>. (Consulté le 22 juin 2021).
- Legoux, Renaud et Amélie Duceppe. (2020). *Incarner ses valeurs avec les données en temps de crise : le cas du théâtre Jean Duceppe*. Atelier numérique. Synapse C. En ligne. <https://www.facebook.com/watch/?v=608209286708469>. (Consulté le 22 juin 2021).
- Legoux, Renaud et Simon Lord. (2019). « La culture des données, un élément qui change la donne ». *Gestion*, 44(1) : 96-99.
- Maceli, Monica G. (2018). « Encouraging patron adoption of privacy-protection technologies: challenges for public libraries ». *IFLA Journal*, 44(3) : 195-202.
- Manach, Jean-Marc. (2020). *La vie privée, un problème de vieux cons ?* Limoges : Fyp, 224 p.
- Marks, Gary, Hooghe, Liesbet et Kermit Blank. (1996). « European integration from the 1980s: State-Centric v. Multi-level Governance ». *Journal of Common Market Studies*, 34(3): 341–377.
- Martel, Marie. (2018). « Modéliser la maison des communs : l'évaluation de l'impact des fab labs en bibliothèque ». *Documentation et bibliothèques*, 64(2) : 23-30.
- Martel, Marie. (2017). « Le design du "care" en bibliothèque : du tiers lieu au lieu d'inclusion sociale ». *I2D Information, données et documents*, 54 (1) : 52-54.
- Mathson, Stephanie et Jeffrey Hancks. (2007). « Privacy please? A comparison between self-checkout and book checkout desk circulation rates for LGBT and other books ». *Journal of access services*, 4(3-4) : 27-3.

Marwick, Alice, Fontaine, Claire et danah boyd. (2017). « “Nobody sees it, nobody gets mad” : social media, privacy, and personal responsibility among low-SES youth ». *Social Media + Society*, Avril, 1-14.

Marx, Lisa. (2019). « Participation as policy in local cultural governance ». *Cultural Trends*, 28(4): 294-304.

McDermott, Yvonne. (2017). « Conceptualising the right to data protection in an era of Big Data ». *Big Data & Society*, 1-7.

McLaverty, Peter. (2011). « Participation ». In *The Sage handbook of governance*, sous la dir. de Mark Bevir. Londres : Sage, 402-418.

McStay, Andrew. (2020). « Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy ». *Big Data & Society*, 3(2): 1–11.

Micheli, Marina, Marisa Ponti, Max Craglia et Anna Berti Suman (2020). « Emerging models of data governance in the age of datafication. » *Big Data & Society*, 7(2): 2053951720948087.

Milan, Stefania et Emiliano Treré. (2020). « The rise of the data poor: the COVID-19 pandemic seen from the margins ». *Social Media + Society*, 1-5.

Milan, Stefania et Lonneke van der Velden. (2016). « The Alternative Epistemologies of Data Activism ». *Digital Culture & Society*, 2(2), 1-11.

Moore, Paul. (2016). « Big Data and structural organisation in major arts bodies: an evolving ethnographic method ». *Cultural Trends*, 25(2): 104-115.

Musiani, Francesca et Valérie Schafer. (2018). « La gouvernance, un enjeu transversal d’Internet au numérique ». *Enjeux numériques*, (4) : 7-11.

Négrier, Emmanuel et Philippe Teillet. (2013). « Politiques culturelles territoriales : le niveau monte-t-il ». *L’Observatoire*, 2(43) : 29-45.

Observatoire de la culture et des communications du Québec. (2017). *État des lieux sur les métadonnées relatives aux contenus culturels*. Gouvernement du Québec : Institut de la statistique du Québec, 118 p.

Observatoire international sur les impacts sociétaux de l’IA et du numérique (OBVIA). (2021). *Mémoire présenté dans le cadre de la SQRI 2022*. En ligne. <https://observatoire-ia.ulaval.ca/sqri-2022/>. (Consulté le 22 juin 2021).

Offe, Clauss. (2009). « Governance: an “empty signifier”? ». *Constellations*, 16(4) : 550-562.

Office québécois de la langue française. (2019). « Mégadonnées ». En ligne. http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26507313. (Consulté le 22 juin 2021).

Office québécois de la langue française. (2019). « Métadonnées ». En ligne. http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8869869. (Consulté le 22 juin 2021).

Padovani, Claudia et Elena Pavan. (2011). « Actors and interactions in global communication governance: The Heuristic Potential of a Network Approach ». In *The Handbook of Global Media and Communication Policy*, sous la dir. de Robin Mansell et Marc Raboy, Malden : Wiley-Blackwell, 543-563.

Pangrazio, Luci et Neil Selwyn. (2019). « Personal data literacies: A critical literacies approach to enhancing understanding of personal digital data ». *New media & Society*, 21(2): 419-437.

Pasek, Anne, Bivens, Rena et Mél Hogan. (2019). « Data segregation and algorithmic amplification: A conversation with Wendy Hui Kyong Chun ». *Canadian Journal of Communication*, 44(3): 455-469.

Pasquier, Dominique. (2018). *L'Internet des familles modestes. Enquête dans la France rurale*. Coll. « Sciences sociales. » Paris : Presses des Mines, 222 p.

Pasquier, Dominique et Dominique Mehl. (2004). « Figures du public ». *Réseaux*, 4(126) : 9-232.

Pedersen, Darhl M. et Frances Shelia. (1990). « Regional differences in privacy preferences ». *Psychological Reports*, 66(3): 731-736.

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

Perrin, Andrew. (2018). *Americans are changing their relationship with Facebook*. Washington: Pew Research Center. En ligne. <http://www.pewresearch.org/facttank/2018/09/05/americans-are-changing-their-relationship-with-facebook/>. (Consulté le 22 juin 2021).

Phoenix SPI. (2019). *Rapport final : Sondage auprès des Canadiens sur la protection de la vie privée de 2018-2019*. Réalisé pour le Commissariat à la protection de la vie privée du Canada. En ligne. <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le->

[commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2019/por_2019_ca/](https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2019/por_2019_ca/). (Consulté le 22 juin 2021).

Phoenix SPI. (2016). *Rapport final : Sondage auprès des Canadiens sur la protection de la vie privée de 2016*. Réalisé pour le Commissariat à la protection de la vie privée du Canada. En ligne. https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2016/por_2016_12/. (Consulté le 22 juin 2021).

Peacock, Sylvia E. (2014). « How web tracking changes user agency in the age of Big Data: the used user ». *Big Data & Society*, 1-11.

Poirier, Christian. (2017). « La citoyenneté culturelle : considérations théoriques et empiriques ». In *Expériences critiques de la médiation culturelle*, sous la dir. de Nathalie Casemajor, Marcelle Dubé, Jean-Marie Lafortune et Ève Lamoureux. Coll. « Monde culturel ». Sainte-Foy : Presses de l'université Laval, 153-171.

Potoglou, Dimitris, Dunkerbley, Fay, Patil, Sunil et Neil Robinson. (2017). « Public preferences for internet surveillance, data retention and privacy enhancing services: evidence from a pan-European study ». *Computers in Human Behavior*, 75 : 811-825.

Preibusch, Soren. (2013). « Guide to measuring privacy concern: review of survey and observational instruments ». *International Journal of Human-Computer Studies*, 71: 1133-1143.

Proulx, Serge et Stéphane Couture. (2006). « Pratiques de coopération et éthique du partage à l'intersection de deux mondes sociaux : militants du logiciel libre et groupes communautaires au Québec ». In *Intelligence Collective* sous la dir. de J.M. Penalva. Paris : Presses de l'École des Mines, 137-152.

Radio-Canada. (2019). « La Loi antiterroriste fédérale contestée en cour ». *Ici.radio.canada.ca*. En ligne. <https://ici.radio-canada.ca/nouvelle/730577/contestation-tribunaux-loi-antiterroriste-association-libertes-civiles>. (Consulté le 22 juin 2021).

Redden, Joanna. (2015). « Big data as system of knowledge: investigating Canadian governance ». In *Compromised Data: From Social Media to Big Data*. Sous la dir. de Greg Elmer, Ganaele Langlois et Joanna Redden. Londres : Bloomsbury, 17-39.

Redden, Joanna. (2018). « The harm that data do ». *Scientific American*, 319(5): En ligne. <https://www.scientificamerican.com/article/the-harm-that-data-do/>. (Consulté le 22 juin 2021).

Richter, Solina, Bell, Jennifer, Jackson, Margot K., Lee, Leah D., Dashora, Pushpanjali et Soleil Surette. (2019). « Public library users: perspectives of socially vulnerable populations ». *Journal of Library Administration*, 59(4) : 431-441.

Roberts, Lynne D. (2016). « Student attitudes toward learning analytics in higher education: “The Fitbit Version of the learning world” ». *Frontiers in Psychology*, 7: 1-11.

Rogers, Richard. (2009). « Post-Demographic Machines ». In *Walled Garden*, sous la dir. de Annet Dekker et Annette Wolfsberger. Amsterdam: Virtueel Platform, 29-39.

Rollet, Nicolas, Beaudouin, Valérie et Isabelle Garron. (2017). « Vidéo-ethnographie des usages de Gallica : une exploration au plus près de l’activité ». *Document numérique*, 20(2/3) : 97-114.

Romuald, Ripon. (2001). « L’articulation entre enquêtes qualitatives et quantitatives : l’exemple des études menées à la Bibliothèque nationale de France ». In *Les publics des équipements culturels. Méthodes et résultats d’enquêtes*, sous la dir. de Olivier Donnat et Sylvie Octobre. Coll. « Les travaux du DEP ». Paris : Ministère de la culture et de la communication, 99-108.

Rosenau, James N. et Ernst-Otto Czempiel. (1992). *Governance without government: Order and change in the world*. Cambridge: Cambridge University Press, 311 p.

Rouvroy, Antoinette et Thomas Berns. (2013). « Gouvernamentalité algorithmique et perspectives d’émancipation ». *Réseaux*, (1): 163-196.

Saez, Guy. (2004). « Gouvernance culturelle territoriale : les acteurs ». In *Institutions et vie culturelles*. Sous la dir. de Guy Saez. Paris : La Documentation Française, 39-43.

Samarati, Pierangela. (2001). « Protecting respondents identities in microdata release ». *IEEE, Transactions on Knowledge and Data Engineering*, 13(6): 1010–1027.

Schmitter, Philippe C. (2001). « What is there to legitimise in the European Union? And how might this be accomplished? ». *The Jean Monnet Center for International and Regional Economic Law & Justice*, 6(2): 1-18.

Schumacher, Clara et Dirk Ifenthaler. (2018). « Features students really expect from learning analytics ». *Computers in Human Behavior*, 78: 397-407.

Servet, Mathilde. (2010). « Les bibliothèques troisième lieu : une nouvelle génération d’établissements culturels ». *Bulletin des bibliothèques de France (BBF)*, 55(4) : 57-66.

Seyfert, Robert et Jonathan Roberge. (2016). *Algorithmic cultures: essays on meaning, performance and new technologies*. Londres : Routledge, 192 p.

Shaffer, Christopher. (2014). « The Patriot Act a decade later: a literature review of librarian responses and strategies ». *Indiana Libraries*, 33(1): 22-25.

Sirois, Guillaume. (2018). « Entre confrontation et coopération : la représentation des intérêts des artistes et des travailleurs culturels de la francophonie canadienne ». *Minorités linguistiques et société*, (10) : 176-195.

Souchier, Emmanuël, Devallon, Jean, Desprès-Lonnet, Marie, Jeanneret, Yves et Joëlle Le Marec. (2003). *Lire, écrire, récrire : objets, signes et pratiques des médias informatisés*. Paris : Éditions de la Bibliothèque publique d'information, 350 p.

Stevens, Charles H. (1977). « Governance of library networks ». *Library Trends*, 26(2) : 219-240.

Striphas, Ted. (2015). « Algorithmic culture ». *European Journal of Cultural Studies*, 18(4/5): 395-412.

Sturges, Paul, Davies, James Eric, Dearnley, James et Ursula Iliffe. (2003). « User privacy in the digital library environment: an investigation of policies and preparedness ». *Library Management*, 24(1/2) : 44-50.

Tchéhouali, Destiny et Josée Plamondon. (Février 2019). *Données d'usage et usage des données à l'ère des plateformes : De la nécessité d'un encadrement réglementaire pour une meilleure affirmation de notre souveraineté numérique*. Montréal : ISOC Québec ; Coalition pour la Culture et les Médias, 30 p.

Thielman, Sam. (2016). « Librairies promise to destroy user data to avoid threat of government surveillance ». *The Guardian*. En ligne.
<https://www.theguardian.com/books/2016/nov/30/library-user-data-government-surveillance-donald-trump>. (Consulté le 22 juin 2021).

Travis, Tiffini A. et Christian Ramirez. (2020). « Big data and academic libraries: the quest for informed Decision-Making ». *Libraries and the Academy*, 20(1): 33-47.

Trottier, Daniel. (2018). « Privacy and Surveillance ». In *The Sage Handbook of Social Media*, sous la dir. de Jean Burgess, Alice Marwick et Thomas Poell. Londres : Sage, 463-480.

Tummont, Nikki et Dawn McKinnon. (2018). « Attitudes and practices of Canadian academic librarians regarding library and online privacy: A national study ». *Library and Information Science Research*, 40(2): 86-97.

Valentine, Jeremy. (2017). « Cultural governance and cultural policy: hegemonic myth and political logics ». In *The Routledge Handbook of Global Cultural Policy*, sous la dir. de Victoria Miller, Victoria Miller et Dave O'Brien. New York: Routledge, 148-164.

Van Dijck, José. (2014). « Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology ». *Surveillance & Society*, 12(2) : 197-208.

Vaillancourt, Christine et Jean-Robert Bisailon. (2020). « Lexique ». *LATICCE*. En ligne. <https://wiki.uqam.ca/display/CEIMLAT/Lexique>. (Consulté le 22 juin 2021).

Villani, Cédric. (Mars 2018). *Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne*. Paris : Mission parlementaire du gouvernement français, 233 p.

Ville de Montréal. (2012). *Politique de données ouvertes de la Ville de Montréal*. En ligne. <http://donnees.ville.montreal.qc.ca/portail/politique-de-donnees-ouvertes/>. (Consulté le 22 juin 2021).

Vitak, Jessica, Liao, Yuting, Kumar, Priya et Mega Subramaniam. (2018). « Librarians as Information Intermediaries: Navigating Tensions Between Being Helpful and Being Liable ». In *Transforming Digital Worlds*, sous la dir. de Gobinda Chowdhury, Julie Mcleod, Val Gillet et Peter Willet. New York: Springer, 693-702.

Widdersheim, Michael M. (2015). « Governance, legitimation, commons: A public sphere framework and research agenda for the public library sector ». *Libri*, 65(4): 237-245.

Wissinger, Christina L. (2017). « Privacy literacy: from theory to practice ». *Communications in Information Literacy*, 11(2): 378-389.

Wylie, Megan, Sculthorp, Miranda, Gagnon-Turcotte, Sarah et Chatwin, Merlin (2021). *Une voie prometteuse pour promouvoir la gouvernance des données dans le secteur des arts de la scène : analyser les chartes et les principes pour la gouvernance des données*. Montréal : Nord Ouvert et Association canadienne des organismes artistiques (CAPACOA).

Yao, Mike. Z., Rice, Ronald E. et Kier Wallis. (2007). « Predicting user concerns about online privacy ». *Journal of the American Society for Information Science and Technology*, 58(5): 710-722.

Ylipulli, Johanna et Aale Luusua. (2019). « Without libraries what have we? Public libraries as nodes for technological empowerment in the era of smart cities, AI and big data ». *Proceedings of the 9th International Conference on Communities & Technologies: Transforming Communities*, Vienne: ICPS Proceedings, 92-101.

Young, Alyson Leigh et Anabel Quan-Haase. (2013). « Privacy protection strategies on Facebook: The Internet privacy paradox revisited ». *Information, Communication and Society*, 16(4): 479-500.

Ytre-Arne, Brita et Ranjana Das. (2019). « An agenda in the interest of audiences: facing the challenges of intrusive media technologies ». *Television & New Media*, 20(2): 184-19



**Institut national
de la recherche
scientifique**