Synthèse de connaissances

Gouvernance des données

La fiducie d'utilité sociale, un outil à fort potentiel

Dépôt légal – Bibliothèque et Archives nationales du Québec.
ISBN 978-2-924879-46-7

tiess

À propos du TIESS

Le TIESS est un organisme de liaison et de transfert en innovation sociale (OLTIS) reconnu par le ministère de l'Économie et de l'Innovation (MEI). Le TIESS regroupe de nombreux acteurs de l'économie sociale et solidaire et du développement territorial, de même que des centres de recherche, des universités et des collèges. Il contribue au développement territorial par le transfert de connaissances : il outille les organismes d'économie sociale et solidaire afin qu'ils puissent faire face aux enjeux de société de façon innovante et transformer leurs pratiques. Cette publication fait partie de la collection de synthèses de connaissances qu'il met gratuitement à leur disposition.

Pour découvrir nos autres titres : **tiess.ca**

Contributions

Rédaction : Jessica Leblanc

Édition : Judith Oliver

Révision linguistique : Stéphane J. Bureau

Révision bibliographique : Le Collaboratoire

Graphisme : MamboMambo

Remerciements

Ce travail a été rendu possible grâce à l'implication soutenue et constante de nombreuses personnes. Des chercheures en droit ainsi que des experts en gouvernance et en mutualisation de données ont enrichi et stimulé la rédaction de ce document. Réunies en comité de suivi, ces personnes ont été essentielles à la réalisation de cette synthèse de connaissances. Le TIESS tient à remercier Annie Bérubé (TIESS) • Lauriane Gorce (Nord Ouvert) • Sarah Gagnon-Turcotte (Nord Ouvert) • Émilien Gruet (TIESS) • Anne-Sophie Hulin (Université d'Ottawa et ANITI Toulouse) • Geneviève Huot (TIESS) • Samuel Kohn (Nord Ouvert) • Jean-Noé Landry (Nord Ouvert) • Marie-Anne Marchand (TIESS) • Joël Nadeau (TIESS) • Marie Plamondon (Nord Ouvert) • Alexandra Popovici (Université de Sherbrooke) • Karine Saboui (Nord Ouvert) • Miranda Sculthorp (Nord Ouvert) • Léah Suissa-Rocheleau (TIESS).

La rédaction de cette synthèse de connaissances a été rendue possible grâce au soutien financier du ministère de l'Économie et de l'Innovation, de la Ville de Montréal et de Common Approach to Impact Measurement.

Québec

Montréal

COMMON APPROACH
TO IMPACT MEASUREMENT

Publication de Territoires innovants en économie sociale et solidaire, novembre 2021.

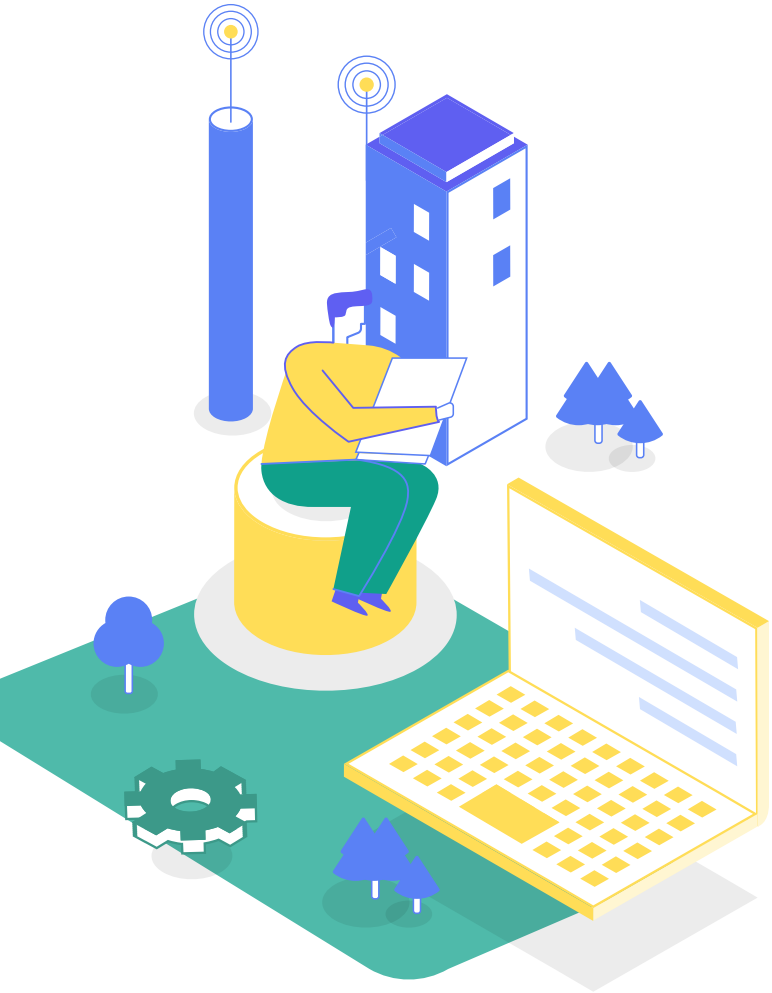
Pour citer : Leblanc, J. (2021). *Gouvernance des données : la fiducie d'utilité sociale, un outil à fort potentiel.* Territoires innovants en économie sociale et solidaire.

Table des matières

Introduction

Aujourd'hui, une grande partie de nos activités quotidiennes est numérisée sous forme de données. Nos achats, notre écoute de musique, notre consultation de contenus médiatiques, ce que l'on aime ou non, le temps que l'on passe à faire telle ou telle chose constituent autant d'informations qui sont collectées, stockées et analysées à des fins diverses.

De l'intelligence artificielle aux objets connectés, les avancées technologiques ont mis en lumière la valeur de ces données. Une fois structurés et interprétés, ces renseignements permettent d'accroître les connaissances des acteurs d'un secteur d'activité, qui pourront notamment optimiser l'allocation des ressources, développer de nouvelles capacités, personnaliser ou créer un service, améliorer l'expérience client, etc. (Stalla-Bourdillon et al., 2020, p. 4-2; HM Treasury, 2018, p. 4). Des données de qualité sont par ailleurs des outils essentiels pour affronter les défis qui nous préoccupent actuellement : parce qu'elles permettent de guider nos décisions, ces informations peuvent servir des fins autres que pécuniaires, qu'elles soient d'ordre politique, social ou économique.



Même si on ne détient pas de chiffres fiables et précis à ce sujet, il est certain que les données pèsent de plus en plus lourd sur l'économie (Duboc et Noël, 2021, p. 12). En quelques années à peine, nous avons généré et collecté plus de données que depuis le début de l'humanité (Nora et al., 2014). **L'économie repose aujourd'hui grandement sur le numérique et, dans un monde connecté, les données représentent une des principales ressources créatrices de richesses** (Klein et Huang, 2013). En ce sens, Statistique Canada (2019b) souligne que les dépenses en investissement et en stocks de capital sont en hausse constante depuis 2005 en ce qui concerne les données, les bases de données et la science des données. Compte tenu du contexte actuel, il est raisonnable de penser que ces développements continueront de s'accélérer dans les prochaines années.

Cette richesse est néanmoins concentrée entre les mains d'un petit nombre d'acteurs. Des compagnies comme Google et Amazon accaparent de très grandes quantités de données sur leurs consommateurs, renforçant et affinant toujours davantage leurs offres de services et de produits. Pour ces entreprises, qui ont été les premières à collecter des informations massivement, l'accès aux données représente un avantage significatif qui contribue à l'écrasement de la concurrence et à la concentration du marché du numérique (Delacroix et al., 2020, p. 4 ; Blankertz, 2020, p. 10). Or, l'accumulation de données exclusives (ou en silos) par une minorité d'entreprises constitue une menace à la vie privée et aux droits des citoyens. Ce phénomène constitue de surcroît un enjeu économique lié à l'accroissement des inégalités et à la fracture numérique entre individus, et entre collectivités et territoires (Klein et Huang, 2013, p. 87).

Nombreux sont ceux qui cherchent, souvent dans l'urgence, une solution à ces problèmes. La modernisation en cours des lois qui encadrent la collecte et l'accès aux renseignements personnels au Québec, en Ontario et au Canada ainsi que la récente adoption de la *Charte des données numériques* par la Ville de Montréal (2020) illustrent cette situation. Les mêmes efforts de réglementation sont déployés à l'international tant pour la protection des renseignements personnels que la gouvernance des données. Ces solutions sont néanmoins souvent fondées sur une approche qui vise la protection de l'individu, et non la prise en charge collective.

Les occasions créées par l'économie sociale

Dans un contexte où les règles sont en grande partie dictées par de grandes entreprises, l'économie sociale (ÉS) nous semble porteuse de solutions qui remettent en question cet ordre établi. Par ses pratiques collectives, l'ÉS est à même de proposer de nouvelles façons de faire afin de rediriger la richesse générée par ces données vers le bien commun.

À cet égard, le partage ou la mutualisation de données apparaissent comme des pratiques prometteuses. Des données mutualisées permettent de générer des connaissances variées et riches sur les pratiques des acteurs comme sur l'ensemble du mouvement de l'économie sociale. Cette mise en commun favorise également la formulation de solutions innovantes adaptées à la complexité des enjeux rencontrés aujourd'hui. L'ÉS peut également promouvoir l'idée selon laquelle les données représentent dans certains cas une ressource qu'il convient de gérer de manière collective.

Ces pratiques de partage et de mutualisation se heurtent toutefois à des obstacles de deux ordres.

Au niveau social, le fait de collecter des données sur l'ensemble de nos activités de manière constante, l'opacité de ces démarches et la faible protection de ces données - tant sur le plan technique que juridique - créent un contexte de méfiance à l'égard des organisations publiques ou privées[1] qui colligent, partagent et utilisent des données. Ce manque de confiance explique d'ailleurs que certaines initiatives ou innovations technologiques demeurent inexploitées[2].

Au niveau des organisations, la compétition et les préoccupations concernant la réputation, les intérêts propriétaires ou la vie privée des individus peuvent nourrir une certaine réticence à mutualiser des données (Stalla-Bourdillon et al., 2020, p. 4). Sans compter les méconnaissances techniques, le manque de compétences et la faible littératie numérique, qui peuvent parfois freiner ce type de pratique.

C'est dans ce contexte qu'émergent les « fiducies de données ». Il s'agit d'un moyen parmi d'autres mis de l'avant pour répondre au manque de protection des données personnelles et au déséquilibre des pouvoirs entre les individus, les gouvernements et les entreprises qui ont la mainmise sur ces données. Les fiducies de données permettraient, selon les cas, de faciliter le partage et l'échange de données entre organisations (Hardinges, 2020), de rééquilibrer le contrôle respectif que les entreprises, les collectivités et les individus peuvent exercer sur les données (Delacroix et Lawrence, 2019, p. 252 ; Mozilla Insights et al., 2020, p. 13) et d'améliorer ou de renforcer la protection de la vie privée et l'autonomie des individus à l'égard de leurs données (Element AI et Nesta, 2019, p. 31).

Le gouvernement canadien recommande actuellement la création de telles fiducies (Gouvernement du Canada, 2019). Cette idée circule également au sein du ministère de l'Économie et de l'Innovation du Québec (Fournier Gosselin et al., 2021).

1 Selon une enquête de Statistique Canada, 61 % des internautes ont supprimé l'historique de leur navigateur, 60 % ont bloqué des courriels (courrier indésirable et pourriels) et 42 % ont modifié les paramètres de confidentialité de leurs comptes ou applications pour limiter l'accès à leur profil ou à la quantité de renseignements personnels qui apparaissent sur leur profil. Statistique Canada (2019a).

2 Le cas de l'application COVI développée par le MILA en pleine pandémie et finalement abandonnée illustre parfaitement cet enjeu. Voir l'article de Delphine Jung (2020, 10 juin) « COVID-19 : l'application de traçage du Mila mise au placard par Ottawa », *Radio-Canada*.

Le potentiel de la fiducie d'utilité sociale

Dans le cadre du partage ou de la mutualisation de données, la gouvernance prend une importance particulière. En effet, les données, qu'elles concernent des individus ou des organisations, peuvent revêtir une dimension sensible qui requiert de construire une confiance solide entre les acteurs par des mécanismes de communication, de reddition de compte et d'imputabilité.

Cette synthèse de connaissances vise à cerner le potentiel de la fiducie d'utilité sociale[3] pour assurer une gouvernance de données digne de confiance qui tend vers le bien commun. Cet outil juridique, prévu au *Code civil du Québec*, vise à favoriser la réalisation d'un but d'intérêt général, notamment à caractère culturel, éducatif, philanthropique ou scientifique. Dans un premier temps, nous aborderons les différents types de données et leur cadre juridique, c'est-à-dire les règles qui régissent de manière générale le partage et la mutualisation de ces données. Dans un deuxième temps, il sera question des différentes approches collaboratives de la gouvernance de données et de l'application de la fiducie d'utilité sociale au monde des données.

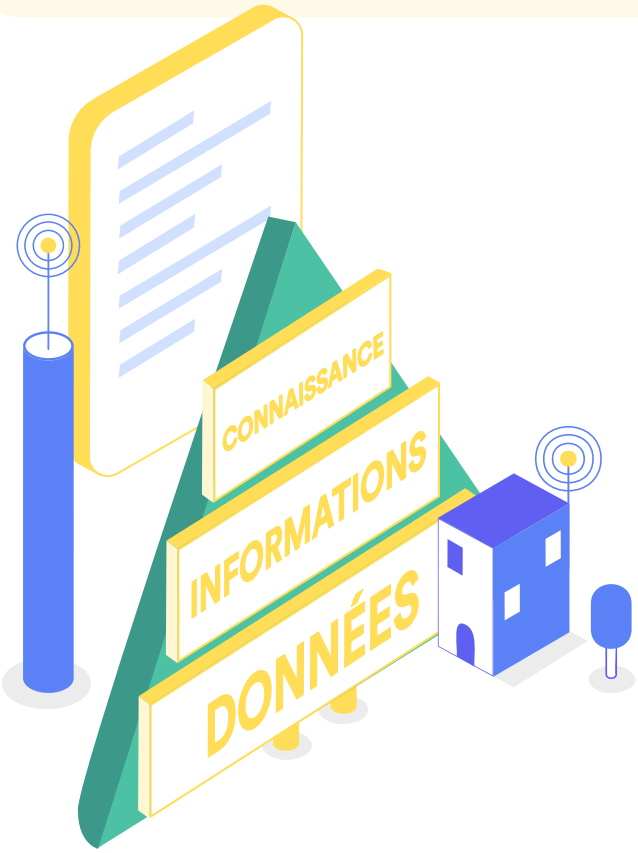
Enfin, il faut souligner que ce texte est publié dans un contexte de changement. Après la réception des mémoires à l'automne 2020, le projet de loi 64 a été à l'étude de la Commission des institutions de l'Assemblée nationale du Québec au cours de l'hiver et du printemps 2021. Au moment de la rédaction de cette synthèse de connaissances, le projet de loi 64 n'était toujours pas adopté et de nombreux articles doivent encore être modifiés. Il se pourrait donc que certaines informations ne soient plus exactes ou applicables après l'adoption de ce projet de loi.

3 Pour une présentation de cet outil juridique, nous référons les lecteurs et lectrices à la synthèse de connaissances et au guide que le TIESS lui a consacrés.

1. Que sont les données ?

Définition

Les données constituent la représentation de faits sous différentes formes : textes, chiffres, images, sons ou vidéos (Gagnon-Turcotte et al., 2021, p. 43). Les données sont numériques lorsque leur représentation à l'aide de chiffres et de symboles permet leur traitement par ordinateur (Courmont, 2016, p. 48). Ainsi, une donnée, comme un chant d'oiseau, devra être décomposée et recomposée en plusieurs autres données en utilisant un langage distinct afin d'être traitée par un système informatique.



La pyramide du savoir est souvent utilisée afin de décrire l'articulation entre les données, l'information et la connaissance (Rowley, 2007, p. 163 ; Ackoff, 1989). Les données sont ainsi comprises comme le matériau brut à partir duquel sont élaborées l'information et la connaissance par une mise en contexte et une interprétation (Courmont, 2016, p. 49).

Cette relation n'est pourtant pas aussi linéaire et directe qu'elle y paraît. En effet, **les données ne sont pas des clés immédiates de connaissances – elles ne procurent aucune information en elles-mêmes. La création de relations causales, la recherche de sens et la validation de l'information sont des activités qui requièrent l'intervention humaine** (Ollion et Boelaert, 2015, para. 3 ; Lugmayr et al., 2017, p. 205). De plus, les données ne sont pas neutres et préanalytiques. Elles ont nécessairement fait l'objet de choix quant à leur portée, leur précision et leur localisation, et reflètent les décisions prises par la personne ou l'organisation qui les collectent. Or, ces choix en matière de collecte de données sont modelés par des connaissances et par une certaine représentation du monde social qui déterminent les paramètres de la collecte et de l'analyse (Courmont, 2015, p. 43).

La numérisation massive des données a encouragé un mouvement qui vise leur accessibilité, notamment celles qui ont un intérêt pour le public (Courmont, 2016, p. 32).

Que sont les données ouvertes ?

La ***Charte internationale sur les données ouvertes*** (2015) en donne la définition suivante :

« Les données ouvertes sont des données numériques accessibles dont les caractéristiques techniques et juridiques permettent la libre utilisation, réutilisation et redistribution par quiconque, en tout temps, en tout lieu. »

La ***Charte des données numériques*** adoptée par la Ville de Montréal suggère plutôt cette définition (Laboratoire d'innovation urbaine, 2020) :

« Ressources informationnelles structurées numériques mises à la disposition du public sous une licence ouverte d'utilisation. »

La numérisation des données a également engendré leur accumulation dans une proportion jusqu'alors inégalée, ce qui a donné lieu à l'expression ***big data*** (ci-après « les données massives »). Il n'existe pas de définition consensuelle et stabilisée des données massives. On les qualifie néanmoins souvent par les trois V : volume, variété et vélocité (Da Sylva, 2017, p. 6-7 ; Zikopoulos et al., 2012, p. 5 ; Kitchin et McArdle, 2016, p. 1 ; Ollion et Boelaert, 2015, paragr. 4).

Les trois V des données massives[4]

1. Le **volume** correspond à la quantité de données.
2. La **vélocité** correspond à la vitesse de collecte des données. Ces données sont créées en temps réel, de façon permanente ou immédiate, contrairement, par exemple, à certaines données scientifiques qui requièrent beaucoup de temps réparti à travers plusieurs étapes.
3. La **variété** des données souligne l'éventail de sources et de types de données.

Catégorisation des données

Les données sont souvent classées selon leur mode de création. Les données sont généralement **représentatives**, c'est-à-dire qu'elles mesurent un phénomène comme l'âge, le nombre de voitures ou des opinions. Elles peuvent également être **inférées** d'une absence ou **dérivées** d'autres données (Scassa, 2018, p. 43 ; Kitchin, 2014, p. 1 ; Coutts et Gagnon-Turcotte, 2020, p. 12-13).

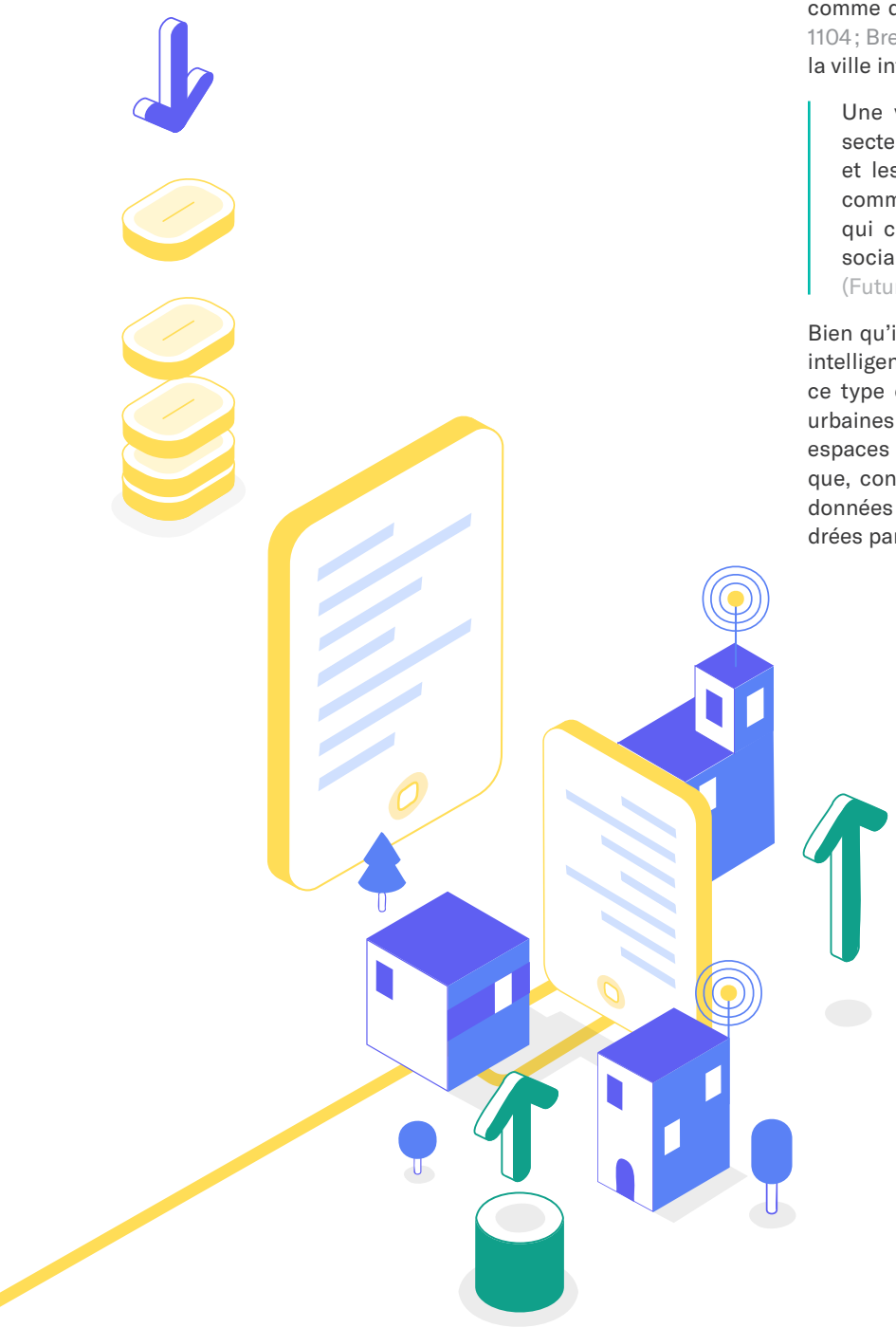
Dans le cadre d'une offre de services en ligne, on distingue généralement les **données d'usage** des **données descriptives**. Les données d'usage concernent la personne qui utilise le service (nom, contenus préférés, montant des transactions, recherches). Les données descriptives concernent l'objet du service. Dans le cas d'un service de visionnement de films en ligne, ce type de données correspond, par exemple, au titre du film, son équipe de production, son format (Tchéhouali et Plamondon, 2018, p. 7-8).

Afin de faciliter la compréhension, la gestion et l'analyse de ces données, on utilise des **métadonnées**, c'est-à-dire des données qui renseignent sur la nature de certaines autres données. Ce sont des renseignements qui sont « générés lorsqu'on utilise la technologie et qui permettent de situer dans leur contexte (qui, quoi, où, quand et comment) diverses activités » (Commissariat à la protection de la vie privée, 2014, p. 1). Dans le cas d'un appel téléphonique, en plus du contenu de l'échange entre les deux interlocuteurs, l'appel génère des métadonnées concernant sa durée, la localisation de chaque interlocuteur et le numéro de téléphone composé. Les métadonnées permettent également de faire des rapprochements entre d'autres données. Par exemple, la donnée « ville » permet de rassembler les données « Québec » et « Sherbrooke » (Tchéhouali et Plamondon, 2018, p. 9).

On distingue ensuite les **données publiques**. L'Organisation de coopération et de développement économiques (ci-après « OCDE ») définit les données publiques comme des données générées, créées, collectées, transformées, préservées, disséminées ou financées par ou au profit d'un gouvernement ou d'une institution publique (OCDE, 2020, p. 6). Les données publiques sont généralement **ouvertes**, c'est-à-dire accessibles au public sans restriction, à moins de conflits avec des considérations privées ou de sécurité publique.

Les décideurs, dont ceux du Québec, voient de nombreux avantages à rendre accessibles les données publiques, notamment le soutien de l'innovation sociale et numérique ainsi qu'une plus grande transparence des institutions (Secrétariat du Conseil du trésor du gouvernement du Québec, 2018 ; Secrétariat du Conseil du trésor, 2019).

4 Certains ajoutent un quatrième V pour la véracité (Lugmayr et al., 2017, p. 197-198).



Finalement, il est souvent fait mention des **données urbaines**, une notion fortement liée à celle de ville intelligente (traduction de *smart city)*. La notion de ville intelligente est née dans un contexte de marketing urbain et a été propulsée, notamment, par des compagnies qui définissaient les villes comme des marchés potentiels (Mann et al., 2020, p. 1103-1104 ; Breux et Diaz, 2017, p. 3). Cependant, on peut concevoir la ville intelligente dans un tout autre ordre d'idée :

> Une ville intelligente ouverte est un lieu où tous les secteurs et les résidents collaborent afin que les données et les technologies soient utilisées pour développer la communauté d'une manière juste, éthique et transparente qui concilie le développement économique, le progrès social et la responsabilité à l'égard de l'environnement. (Future Cities Canada)

Bien qu'il n'existe aucune définition consensuelle de la ville intelligente, on constate que les données sont au centre de ce type de projet (Breux et Diaz, 2017, p. 7). Les données urbaines représentent donc ces données collectées dans les espaces physiques de la ville (Sidewalk Labs, 2018). À noter que, contrairement aux données personnelles et certaines données publiques, les données urbaines ne sont pas encadrées par des lois particulières.

2. Le cadre juridique des données

Les règles qui s'appliquent aux données varient selon le type de données, d'où l'intérêt de bien les distinguer. Le cadre juridique pertinent peut être scindé en au moins deux régimes, soit les lois visant la protection de la vie privée et des renseignements personnels et les droits de propriété.

Qualification juridique des données

Afin de déterminer quelles lois s'appliquent aux données, il est d'abord nécessaire de les qualifier juridiquement. Cela signifie qu'il faut déterminer si les données entrent dans une ou l'autre des catégories définies par la loi.

Au Québec, deux lois sont particulièrement importantes en ce qui concerne les données :

- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après « *Loi sur l'accès* »), qui s'applique aux documents détenus par les organismes publics ;
- la *Loi sur la protection des renseignements personnels dans le secteur privé* (ci-après « Loi sur la protection »), qui s'applique aux personnes qui recueillent, détiennent, utilisent ou communiquent à des tiers des renseignements personnels à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du *Code civil du Québec*.

Ces deux lois sont actuellement soumises à un processus de modification. À l'été 2020, la ministre de la Justice de l'époque, Sonia Lebel, présentait le projet de loi 64, qui vise à moderniser les règles en matière de protection des renseignements personnels. Ce projet de loi, selon la ministre, est fondé sur deux principes : redonner aux citoyens le contrôle de leurs renseignements personnels et responsabiliser les organisations qui utilisent ces renseignements.

Ces deux lois définissent certaines catégories de données.

Renseignement personnel : un renseignement personnel est un renseignement qui concerne une personne physique et qui permet de l'identifier[5]. S'il est adopté, le projet de loi 64 précisera qu'un renseignement personnel doit permettre d'identifier directement ou indirectement une personne, ce qui élargit la portée de cette définition.

Renseignement personnel sensible : s'il est adopté, le projet de loi 64 prévoit la catégorie de renseignement personnel sensible. Un renseignement sera considéré comme sensible lorsque, « de par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée[6] ».

Le projet de loi 64 introduit également les catégories de renseignements personnels dépersonnalisés et anonymisés.

Renseignement personnel dépersonnalisé : un renseignement personnel est dépersonnalisé « lorsqu'il ne permet plus d'identifier directement la personne concernée[7] ».

Renseignement personnel anonymisé : un renseignement personnel est anonymisé « lorsqu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne[8] ». À noter que, dans le projet de loi 64, l'anonymisation est présentée comme une alternative à la destruction d'un renseignement une fois que la fin pour laquelle la donnée a été collectée est atteinte. Cette anonymisation doit être faite pour permettre une utilisation des renseignements personnels à des fins sérieuses et légitimes. L'anonymisation des renseignements personnels ne pourra donc pas être réalisée dans toutes les circonstances.

Les renseignements personnels jouissent de la protection de la *Loi sur l'accès* et de la *Loi sur la protection*. Toutefois, certains renseignements personnels sont considérés comme publics par la loi et sont exemptés de l'application de ces lois qui visent leur protection[9]. En effet, dans certains cas, il est nécessaire d'établir un équilibre entre le droit à la vie privée et l'accès à l'information (Benyekhlef et Déziel, 2018, p. 278). On peut donner en exemple des renseignements concernant une faillite, qui peuvent être d'intérêt public pour des investisseurs ou pour établir un dossier de crédit[10] (Guilmain et Gratton, 2019, p. 80). Un individu peut également consentir à ce que ses renseignements personnels collectés par des autorités publiques soient rendus publics[11].

5 Art. 2 de la *Loi sur la protection*.
6 Art. 102 du projet de loi 64 modifiant l'article 12 de la *Loi sur la protection*.
7 Art. 102 du projet de loi 64 modifiant l'article 12 de la *Loi sur la protection*.
8 Art. 111 du projet de loi 64 modifiant l'article 23 de la *Loi sur la protection*.
9 Art. 1, al. 5 de la *Loi sur la protection*.
10 Voir la décision de la *Commission d'accès à l'information, C.P. c. Équifax Canada inc.*, 2013 QCCAI 99.
11 Art. 53 de la *Loi sur l'accès*.

Les données qui n'entrent pas dans l'une ou l'autre des catégories mentionnées ci-dessus ne sont pas soumises à l'application de ces lois. Pour les fins de cette synthèse, elles seront nommées **renseignements non personnels**.

La qualification juridique des données peut être ardue dans certains cas. En effet, les catégories de renseignements personnels et de renseignements non personnels sont fluides, dynamiques et varient selon le contexte (Stalla-Bourdillon, 2021, p. 6). Dans la pratique, il est incertain que l'on puisse distinguer les renseignements non personnels des renseignements personnels dans une base de données puisque les organisations ne les classent pas nécessairement selon cette catégorisation (Graef et al., 2018, p. 3). L'ajout de l'adverbe « indirectement » à la définition des renseignements personnels dans le projet de loi 64 signifie que la catégorie de renseignements personnels pourra fluctuer selon le contexte de la collecte, mais également selon les recoupements, les combinaisons et les inférences qu'une base de données permettra d'établir.

Protection de la vie privée et renseignements personnels

Il est souvent évoqué, même par les politiciens[12], que nos renseignements personnels nous appartiennent. D'un point de vue des acteurs de la société civile, la propriété évoque en effet le contrôle (Bernelin, 2019, paragr. 1) et est perçu comme un moyen d'empêcher le pillage et le partage des renseignements personnels dans un but commercial (Anciaux et al., 2017, p. 22 ; Léger et Bentata, 2019, p. 13). Par ailleurs, il est également soutenu que la propriété de ses renseignements personnels pourrait forcer le partage de la valeur économique créée par ces données, permettant ainsi une juste rétribution des individus qui les génèrent.

Or, au Québec, la propriété des renseignements personnels n'existe pas.

En droit québécois, la protection des renseignements personnels ainsi que le contrôle de l'individu sur ses renseignements sont des composantes du droit à la vie privée[13].

12 Voir l'article de Fanny Lévesque dans *La Presse* (2020).

13 *Pascal Métal inc. c. Turcotte*, 2021 QCCS 1828, paragr. 73.

La **protection de la vie privée** est un droit reconnu par la *Charte des droits et libertés de la personne*[14] et le *Code civil du Québec*[15]. Il s'agit d'un **droit de la personnalité**, c'est-à-dire un droit qui met en jeu un intérêt d'ordre moral, non évaluable en argent. Une personne ne peut transmettre son droit à la vie privée, lequel est considéré comme incessible. On ne peut le céder ou y renoncer par contrat. Une personne ne peut par ailleurs en être privée par autrui ; le droit à la vie privée ne peut être saisi.

L'intensité du droit à la vie privée peut varier selon la qualification des renseignements personnels. Plus les informations sont de nature personnelle et intime, plus l'expectative de vie privée est élevée[16].

Si on ne peut céder ou renoncer complètement à notre droit à la vie privée, rien n'empêche de conclure des contrats quant à l'**exercice de ce droit**. C'est exactement ce qui survient lorsque nous utilisons des services numériques gratuits. En échange de nos renseignements personnels, la plateforme offre des produits ou des services, comme le courriel ou un réseau social. Il y a donc un contrat qui se forme - entre l'utilisateur et la plateforme - qui porte entre autres sur l'exercice de notre droit à la vie privée. Un auteur en décrit ainsi le processus :

> Durant la phase d'inscription, l'internaute doit créer et renseigner son profil sur le site. Une fois le profil renseigné, l'internaute « accepte les conditions d'utilisation du site » pour finaliser son inscription. Généralement, l'acceptation de ces conditions nécessite un simple clic de la part de l'internaute. Durant cette phase, les politiques de confidentialité du site sont soumises à l'internaute. Ce dernier formule ensuite son consentement au traitement, en acceptant les conditions d'utilisation, comprenant les politiques de confidentialité. Une fois inscrit, l'internaute entre dans la phase d'utilisation du site. Lors de la phase d'inscription, il bénéficie des services du site (partage, personnalisation de contenu, création d'un compte, etc.). C'est durant cette phase d'utilisation qu'il va divulguer ses données personnelles en interagissant avec d'autres internautes ou avec le site de réseautage. (Dauverchain, 2018, p. 24-25)

Les métadonnées et la vie privée

Les renseignements personnels ne sont pas les seules données qui soulèvent des enjeux relativement à la vie privée. Les métadonnées peuvent souvent révéler beaucoup d'informations sur un individu (Benyekhlef et Déziel, 2018, p. 190). Le Commissariat à la protection de la vie privée du Canada l'explique ainsi :

> [...] l'information sur le lieu où se trouve une personne obtenue à partir des tours de téléphonie mobile, le nom de l'émetteur ou du récepteur d'un message électronique, ou les achats par internet, par exemple, [traduction] « ne constituent peut-être pas le contenu de nos communications, mais ils peuvent donner une image très détaillée de notre vie » (Commissariat à la protection de la vie privée, 2014, p. 4).

Selon Benyekhlef et Déziel (2018, p. 191), il est essentiel que les métadonnées soient protégées au nom du droit à la vie privée.

La notion de consentement est au cœur des opérations de collecte et de communication des renseignements personnels. Le projet de loi 64, s'il est adopté, prévoit que tout consentement doit être manifeste, libre, éclairé et donné à des fins spécifiques. Il doit surtout être demandé pour chacune de ces fins, en termes simples et clairs[17]. En ce qui concerne les renseignements personnels sensibles, ce consentement doit être manifesté de façon expresse[18]. Selon une lecture *a contrario,* cela pourrait ouvrir la porte à un consentement implicite en matière de renseignements personnels non sensibles (Uzan-Naulin et Barbach, 2020).

14 Art. 5 de la *Charte des droits et libertés du Québec*.

15 Art. 3 et 35 du *Code civil du Québec*.

16 *Pascal Métal inc. c. Turcotte*, 2021 QCCS 1828, paragr. 74.

17 Art. 103 du projet de loi 64 modifiant l'article 14 de la *Loi sur la protection*.

18 Art. 102 du projet de loi 64 modifiant l'article 12 de la *Loi sur la protection*. Un consentement exprès est un « [c]onsentement exprimé par un comportement qui manifeste clairement la volonté de conclure un acte juridique». (Centre de recherche en droit privé et comparé du Québec, 2003)

Au Québec, une organisation qui collecte des renseignements personnels doit informer les personnes concernées des fins auxquelles ces renseignements sont recueillis[19]. Un renseignement personnel ne peut donc être utilisé qu'aux fins pour lesquelles il a été collecté, à moins du consentement de la personne concernée[20]. Lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, l'entreprise doit le détruire ou l'anonymiser. Cette anonymisation doit être réalisée à des fins légitimes et sérieuses[21].

Dans le cadre de la collecte, l'organisation qui recueille des renseignements personnels peut prévoir la communication de ces renseignements à des tiers. Le cas échéant, les personnes qui fournissent leurs renseignements doivent être informées du nom du tiers pour qui la collecte est faite ou le nom des tiers à qui il est nécessaire de communiquer les renseignements pour les fins déterminées[22].

Toute personne qui fournit ses renseignements selon cette procédure consent à leur utilisation et à leur communication, mais toujours aux fins déterminées dans le cadre de la collecte[23].

En ce qui concerne le partage des renseignements personnels, la *Loi sur la protection* exige le consentement manifeste, libre et éclairé des individus à la communication des renseignements personnels les concernant[24]. La loi n'autorise pas, actuellement, « de collectes, d'utilisations ou de communications de renseignements personnels sur la base d'un consentement implicite ou tacite » (Benyekhlef et Déziel, 2018, p. 326).

Le projet de loi 64 assouplit ce principe, mais essentiellement à des fins commerciales. Ainsi, une entreprise pourra communiquer des renseignements personnels à un tiers sans le consentement des personnes concernées lorsque la communication de ces renseignements est nécessaire pour conclure une transaction commerciale[25]. Pour l'application de cet article, transaction commerciale signifie :

> [...] l'aliénation ou [...] la location de tout ou partie d'une entreprise ou des actifs dont elle dispose, [la] modification de sa structure juridique par fusion ou autrement, [...] l'obtention d'un prêt ou de toute autre forme de financement par celle-ci ou d'une sûreté prise pour garantir une de ses obligations.

Une telle communication sans le consentement de la personne concernée sera également possible dans le cas où « cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise qu'elle confie à cette personne ou à cet organisme[26] ». Dans ce dernier cas, le tiers ne peut pas conserver les renseignements personnels après l'exécution du mandat ou du contrat.

19 Art. 99 du projet de loi 64 modifiant l'article 8 de la *Loi sur la protection*.

20 Art. 102 du projet de loi 64 modifiant l'article 12 de la *Loi sur la protection*. Il existe néanmoins cinq exceptions à cette règle, soit :

1° lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli ;

2° lorsque son utilisation est manifestement au bénéfice de la personne concernée ;

2.1° lorsque son utilisation est nécessaire à des fins de prévention et de détection de la fraude ou d'évaluation et d'amélioration des mesures de protection et de sécurité ;

2.2° lorsque son utilisation est nécessaire à des fins de fourniture ou de livraison d'un produit ou de prestation d'un service demandé par la personne concernée ;

3° lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé.

21 Art. 110 du projet de loi 64 modifiant l'article 23 de la *Loi sur la protection*

22 Art. 99 du projet de loi 64 modifiant l'article 8 de la *Loi sur la protection*.

23 Art. 99 du projet de loi 64 créant l'article 8.3 de la *Loi sur la protection*.

24 Art. 13 de la *Loi sur la protection*. Le projet de loi 64 reprend presque intégralement ce principe à l'art. 102 du projet de loi 64 modifiant l'art. 13 de la *Loi sur la protection*.

25 Art. 107 du projet de loi 64 créant l'article 18.4 de la *Loi sur la protection*.

26 Art. 107 du projet de loi 64 créant l'article 18.4 de la *Loi sur la protection*.

La propriété des renseignements personnels : une idée alléchante, mais controversée

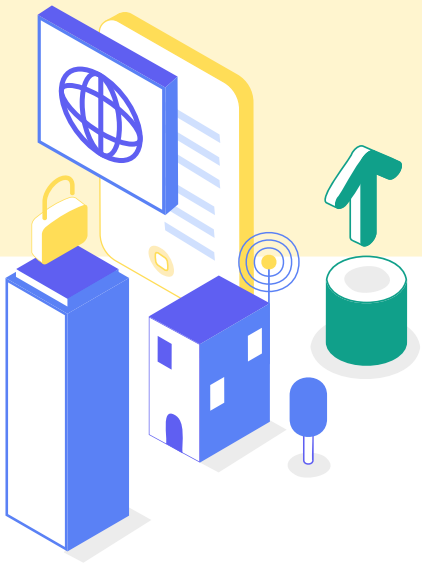
Bien que le droit québécois et le droit canadien[27] s'éloignent complètement de l'idée d'une propriété des renseignements personnels, le débat sur la reconnaissance d'un tel droit est très présent dans d'autres pays. Au Québec, cette question ne se pose pas puisque le droit à la vie privée est reconnu par la loi comme un droit de la personnalité.

Dans un pays où la question se pose, comme en France, on note néanmoins que la majorité des auteurs constatent que la propriété des données personnelles semble être une fausse bonne idée. Deux raisons sont souvent invoquées : 1) l'appropriabilité incertaine des données personnelles et 2) l'inopportunité économique d'une telle solution.

Peut-on s'approprier des renseignements personnels ?

Les données personnelles ont un caractère hybride (Augagneur, 2015, paragr. 47 ; Rochfeld, 2014b), ce qui entraîne une complexité concernant leur statut juridique et donc leur possibilité ou non d'être un objet de propriété. Les données personnelles représentent des actifs économiques pour ceux qui les valorisent, mais également un prolongement des êtres humains en ce qu'elles reflètent certains éléments qui leur sont propres (identité, vie privée, choix personnels) (Bernelin, 2019, paragr. 11 ; Mouron, 2018 ; Mattatia et Yaïche, 2015). Ce caractère hybride pose un obstacle important à la propriété.

Aussi, certaines données, notamment celles qui relèvent de la génétique d'une personne, sont partagées entre plusieurs ; dans cet exemple, les membres d'une même famille. Ces données ont donc une dimension collective qui s'harmonise difficilement avec la propriété, laquelle est d'abord individuelle (Pellegrini, 2018, p. 516).



Quelle serait l'efficacité d'une telle propriété ?

Plusieurs auteurs remettent en question le fait que la propriété des données personnelles accorderait un réel contrôle des individus sur l'usage qui en est fait. Cette propriété ne permettrait pas d'atteindre les objectifs souhaités et, dans les faits, pourrait accroître le pouvoir des entreprises au détriment des individus (Bernelin, 2019, paragr. 14 ; Debet, 2016 ; Anciaux et al., 2017, p. 30 ; Delacroix et al., 2020, p. 7).

D'abord, une propriété des données personnelles ferait en sorte qu'un individu perdrait complètement le contrôle de ces données une fois celles-ci vendues, ce qui réduirait à néant sa protection (Debet, 2016 ; Delmas-Marty, p. 54 ; Pellegrini, 2018, p. 516).

Plus globalement, l'idée d'un droit de propriété renvoie à l'individu seul la responsabilité de gérer et de protéger ses données, ce qui nie le rapport de force entre usagers et entreprises ainsi que le déséquilibre de moyens et de ressources entre usagers (Conseil national du numérique, 2014, p. 37). Ainsi, le rééquilibrage entre les internautes et les entreprises qui collectent des données par la reconnaissance d'un droit de propriété apparaît inatteignable, sauf pour les personnes qui disposent de richesses particulières (Conseil d'État, 2014, p. 265 ; Anciaux et al., 2017, p. 28 ; Pellegrini, 2018, p. 516).

[27] Dans le reste du Canada, où les droits civils sont régis par la *common law*, la professeure Scassa note que la propriété des données personnelles ne correspond pas à l'état du droit (2018, p. 14).

Droits de propriété sur les données

Droit de propriété du *Code civil du Québec*

Qu'en est-il des renseignements non personnels ? La situation en cette matière est complètement différente puisque ces données ne sont pas une composante du droit à la vie privée, mais des biens immatériels susceptibles d'être appropriés.

Dans les dernières années, le droit de propriété a étendu son emprise sur l'immatériel. Parmi les juristes, il existe encore des résistances à la reconnaissance d'un droit de propriété sur les choses immatérielles (des objets intangibles) comme les données, mais ces résistances s'effritent de plus en plus. Compte tenu de la dématérialisation du monde et des richesses, il est maintenant reconnu en droit que tous les biens incorporels peuvent être objets de propriété (Normand, 2004, p. 183). Il en est ainsi puisque le droit de propriété fait preuve de propension à « embrasser tout ce qui a une valeur économique, sans être limité par la corporéité des choses » (Gidrol-Mistral, 2016, p. 99). Les tribunaux ont en ce sens reconnu que la clientèle[28], le savoir-faire ou l'information sont des choses immatérielles appropriées ou susceptibles d'être appropriées[29].

En ce qui concerne les données, la juge Marie Deschamps, telle qu'elle était alors, s'est prononcée à leur égard. Le litige concernait des données portant sur des recherches de titres fonciers contenues dans des avis juridiques. La juge Deschamps qualifie ces données de biens immatériels à l'aide d'une analogie avec le savoir-faire (le *know-how*) :

> Le Tribunal croit que le raisonnement utilisé pour analyser les connaissances d'un technicien est applicable aux connaissances d'un avocat. Pour émettre l'avis au client, l'avocat utilise des informations fournies par son client et obtenues, pour la plupart, de la lecture des titres qu'il interprète à l'aide de son expertise juridique. Ces interprétations, colligées dans les avis aux clients, constituent une banque de données. Comme dans le cas des connaissances techniques, la banque de données peut être qualifiée de *know-how*, bien meuble incorporel susceptible d'appropriation[30].
>
> [Soulignement ajouté]

Cette expansion de la propriété à l'immatériel reflète un durcissement des droits exclusifs et individuels au Québec comme ailleurs dans le monde. Ce contexte de durcissement a largement motivé le développement des logiciels libres et des communs numériques [voir section sur les communs de données].

Propriété intellectuelle

Les données numériques peuvent également être appréhendées sous l'angle des droits de propriété intellectuelle, mais uniquement dans des cas très précis.

Les droits de la propriété intellectuelle (brevets, marques, dessins industriels, droits d'auteur) sont régis par des lois canadiennes. Dans le cas des données numériques, la *Loi sur le droit d'auteur*[31] est d'un intérêt particulier.

Tous les droits intellectuels reposent sur la prémisse que les idées et les faits ne sont pas appropriables. Ces éléments sont ce qu'on appelle des *res communis*, des choses communes, lesquelles peuvent être définies ainsi : « Chose non susceptible d'appropriation et dont l'utilisation est commune à tous » (Centre Paul-André Crépeau, 2012).

Le droit d'auteur porte donc sur l'expression particulière d'une idée et non sur l'idée elle-même. Encore là, toute expression d'une idée n'est pas protégée par le droit d'auteur ; cette expression doit être « originale, particulière et individualisée[32]. »

L'originalité est la porte d'entrée du droit d'auteur[33]. Ce critère d'originalité n'est pas défini dans la *Loi sur le droit d'auteur*, mais la Cour suprême du Canada en a ainsi dessiné les contours : une œuvre originale est le produit de l'exercice du talent et du jugement d'un auteur[34]. Une œuvre originale consacre le statut d'auteur, lequel jouit d'un droit exclusif et opposable à tous du seul fait de sa création[35]. L'auteur d'une œuvre originale jouit automatiquement du droit d'auteur sans qu'il soit nécessaire d'enregistrer son œuvre (Scassa, 2018, p. 4).

28 *Mirarchi c. Lussier*, 2007 QCCA 248.
29 *Gaudreau c. 9090-2438*, 2007 QCCA 1254.
30 *Hindle c. Cornish*, [1991] R.J.Q. 1723, J.E. 91-1118 (C.A.)
31 *Loi sur le droit d'auteur,* L.R.C. (1985), c. C-42.
32 *Pelchat c. Zone 3 inc.*, 2013 QCCS 78, paragr. 41.
33 *Robertson c. Thomson Corp.*, 2006 CSC 43, paragr. 35.
34 À noter que la version anglaise utilise le terme *skill* et non talent, lequel nous semble plus large.
35 Art. 3 de la *Loi sur le droit d'auteur*.

La *Loi sur le droit d'auteur* protège, entre autres choses, la compilation[36], laquelle est définie ainsi : « les œuvres résultant du choix ou de l'arrangement de tout ou partie d'œuvres littéraires, dramatiques, musicales ou artistiques ou de données[37]. » À titre d'exemple, un journal peut être considéré comme une compilation de textes et donc être protégé par le droit d'auteur.

> [O]n retrouve beaucoup d'éléments originaux dans un journal : le contenu rédactionnel, le choix et la disposition des articles, l'arrangement des annonces publicitaires et des images, ainsi que la police et le style employés. Toutefois, la véritable originalité d'un journal réside dans son contenu rédactionnel, car c'est le choix des textes, et les textes eux-mêmes, qui touchent le cœur et l'esprit des lecteurs[38].

Dans un cas comme celui-ci, le droit d'auteur du journal ne s'étend pas jusqu'au contenu des articles, celui-ci relevant du droit d'auteur des journalistes.

Ainsi, dans certains cas, la *Loi sur le droit d'auteur* pourrait protéger une compilation de données sous réserve que celle-ci respecte le critère d'originalité à travers le choix et l'arrangement des éléments qui la composent. Cette affirmation peut être illustrée par un cas véridique, soit un litige devant les tribunaux concernant un site internet qui avait reproduit des informations et des données copiées du *Guide de l'auto*. Ces données concernaient la consommation d'essence, la vitesse maximale et l'accélération sur une distance déterminée. La Cour d'appel du Québec a conclu que la compilation de données peut être protégée par le droit d'auteur dans ces deux situations[39] :

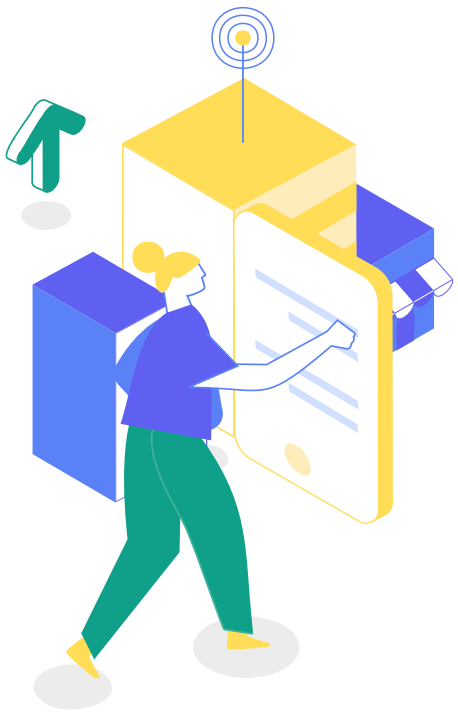
1

Lorsque la compilation est rehaussée par une présentation visuelle particulière qui attire l'attention du lecteur. Elle est, dans ce cas, « incontestablement le fruit d'un exercice par l'auteur de son savoir-faire et de son jugement[40] ».

2

Lorsque les mêmes données étalons sont systématiquement fournies (et qu'elles n'existent pas dans le domaine public sous cette forme) afin de générer une comparaison entre des modèles[41].

Qu'en est-il des données prises isolément, sans qu'elles soient organisées en compilation ? Pour rappel, le droit d'auteur ne protège pas les faits, qui sont du domaine public. Selon la professeure de droit Teresa Scassa, il est néanmoins possible que les données puissent être protégées par le droit d'auteur. Cette position tient à la distinction entre les faits et les données, une distinction qui n'est pas toujours facile à établir. Elle note que certaines personnes voient les faits comme les fondements des données, alors que d'autres considèrent les faits comme la réalité objective. Selon cette dernière conception, les faits existeraient indépendamment de ceux qui les enregistrent (Scassa, 2018, p. 3). La professeure Scassa conclut que cette distinction ouvre la porte à la reconnaissance par les tribunaux d'un droit d'auteur sur des données, en particulier dans le cas des données dérivées et inférées. Il existe néanmoins des obstacles importants à cette reconnaissance (2018, p. 10).



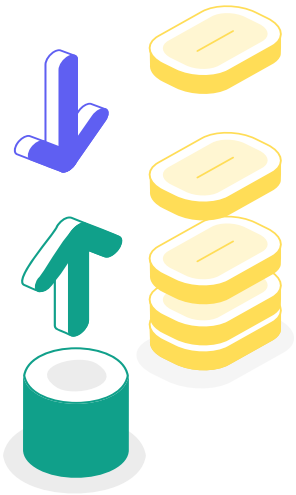
36 *CCH Canadienne Ltée c. Barreau du Haut-Canada*, 2004 CSC 13, paragr. 8.
37 Art. 2 de la *Loi sur le droit d'auteur.*
38 *Robertson c. Thomson Corp.*, 2006 CSC 43, paragr. 39.
39 Cela n'exclut pas qu'il puisse exister d'autres situations dans lesquelles une compilation de données est protégée par le droit d'auteur.
40 *Gahel c. Corporation Xprima.com,* 2008 QCCA 1264, paragr. 45.
41 *Gahel c. Corporation Xprima.com*, 2008 QCCA 1264, paragr. 54.

Limites du cadre juridique actuel

L'approche fondée sur le consentement individuel qui prévaut encore aujourd'hui a été largement critiquée de part et d'autre.

Individuellement, les utilisateurs de services numériques ont peu de contrôle sur leurs données, lesquelles sont généralement transmises à des entreprises par des transactions ou des activités en ligne réalisées par tout un chacun. La cession de nos droits sur ces données se fait quant à elle par la signature de formulaires de consentement complexes et souvent opaques (Blankertz, 2020, p. 8-9). Il est aujourd'hui improbable qu'une personne seule soit en mesure de lire et de comprendre toutes les clauses contenues dans ces contrats compte tenu du nombre de transactions ou de collectes de données effectuées en une seule journée, pour chaque individu (Loi et al., 2020, p. 13 ; Blankertz, 2020, p. 8-9).

Pour les entreprises qui collectent des données, chaque renseignement considéré individuellement ne vaut à peu près rien ; c'est souvent la masse de renseignements qui acquiert une valeur, pourvu que ces données soient d'une qualité et d'une intégrité suffisantes et qu'elles soient interprétées avec nuance. Ces données deviennent ainsi des ressources qu'il faut réglementer comme des ressources collectives et « non comme une addition de renseignements portant sur des individus » (Trudel, 2018). Le cadre juridique nous maintient dans une logique individuelle alors que des actions collectives sont nécessaires afin de se réapproprier les espaces numériques qui sont de plus en plus privatisés.



Le droit à la vie privée en lui-même comporte une **dimension collective**. D'abord, en consentant à la collecte de renseignements personnels, une personne peut du même coup dévoiler des informations sur des tiers, notamment les membres de son entourage (Ligue des droits et libertés, 2020, p. 19). Ensuite, les entreprises et les organisations qui collectent suffisamment de données sur les utilisateurs d'un service ou d'un produit peuvent constituer des groupes algorithmiques. En analysant des données primaires et en composant des groupes en fonction de certaines caractéristiques (genre, âge), des organisations et des entreprises sont en mesure d'inférer, avec un certain niveau de certitude, les probabilités qu'une personne adopte un comportement ou une habitude de vie ou soit en train de vivre une situation particulière (Déziel, 2018, p. 835-839). Ces organisations ou entreprises peuvent alors cibler leurs publicités afin d'influencer les habitudes de consommation. Ces regroupements sont souvent élaborés à partir de renseignements personnels dépersonnalisés ou anonymisés, de sorte que les individus ignorent généralement leur appartenance à un groupe algorithmique (Du Perron, 2020, p. 39 40).

Target et la prédiction des grossesses

Il y a quelques années, un magasin de la chaîne Target a fait les manchettes pour avoir envoyé des coupons rabais pour des articles de bébé à une jeune femme. En voyant ces coupons, le père de la jeune femme est devenu furieux et a invectivé un responsable du magasin au motif que la compagnie incitait sa fille à devenir enceinte.

Or, Target avait simplement prédit, par la formation de groupes algorithmiques et en analysant les achats de ces groupes, la grossesse de la jeune femme, qui ne l'avait pas révélée à son père. Grâce à des renseignements personnels collectés et achetés de tiers, Target avait établi une liste de 25 produits consommés par les femmes enceintes. Selon les achats effectués par une cliente, Target lui attribuait une cote de probabilité. À partir d'un certain seuil, Target inférait avec un degré de précision assez élevé que la cliente était enceinte.

Si certains acteurs soulèvent qu'une approche individuelle est insuffisante en matière de réglementation et d'encadrement des grandes compagnies technologiques, ce sont souvent les enjeux de surveillance ou de profilage qui retiennent, avec raison, leur attention (Barreau du Québec, s.d.; Union des consommateurs, 2019).

Mais il y a plus. Les règles fondées sur le consentement et la protection de l'individu ne permettent pas de freiner ou de contrôler les dynamiques d'accaparement et de la concentration des données dans les mains de quelques acteurs (Ho et Chuang, 2019, p. 204).

Le contexte québécois actuel se distingue quant à son approche très prudente en matière de collecte et de communication des renseignements personnels. La communication de renseignements personnels à un tiers requiert le consentement des individus concernés [voir section sur la protection de la vie privée et les renseignements personnels]. Cette approche ne doit pas nécessairement être décriée ou abandonnée, mais elle complique inévitablement tout projet de mutualisation ou de partage de données entre organisations. Le projet de loi 64 assouplit cette approche, mais les assouplissements proposés à la règle du consentement en matière de communication de données à un tiers visent principalement les transactions commerciales ainsi que les contrats de services et d'entreprises élaborés dans un but précis et pour un temps limité. Ces assouplissements pourraient principalement bénéficier au privé et à l'économie traditionnelle et miner la capacité des entreprises collectives à mutualiser des ressources.

Le cadre juridique de la collecte et de la communication des données, et plus largement du numérique, est appelé à changer, ce qui représente une occasion à saisir. Le mouvement de l'économie sociale pourrait gagner à se positionner à l'égard de ces changements et à construire un discours concernant les conditions nécessaires pour bâtir un écosystème numérique alternatif. En observant les développements législatifs qui se préparent ailleurs, il est possible de cerner certains enjeux qui pourraient se poser au Québec et au Canada et dont l'économie sociale aurait intérêt à s'emparer.

On peut par exemple souligner que la proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données[42], soumis le 25 novembre 2020, prévoit un traitement différencié pour les entités qui agissent dans un but non lucratif et dans l'intérêt général. Le règlement distingue donc les règles qui devraient être appliquées selon la finalité poursuivie par les organisations qui collectent des données, soit dans un but privé ou d'intérêt général. Une telle distinction entre entités à but lucratif et non lucratif pourrait s'avérer pertinente en contexte québécois.

À titre de second exemple, la France se penche actuellement sur la possibilité de créer un **droit à l'interopérabilité** (Conseil national du numérique de France, 2020; Duponchelle, 2015; De Hert et al., 2018). L'interopérabilité correspond à une notion d'abord technique et informatique qu'on peut définir ainsi :

> Dans une première approche, [l'interopérabilité désigne] la « capacité de matériels, de logiciels ou de protocoles différents à fonctionner ensemble et à partager des informations ». Plus précisément, il est proposé de définir l'interopérabilité comme la capacité d'éléments matériels ou immatériels à échanger des données et à utiliser mutuellement les données échangées, par le recours à des standards ouverts de communication. L'interopérabilité constitue donc la condition sine qua non d'un fonctionnement coordonné et efficace des technologies et outils numériques, par une compréhension mutuelle des informations échangées et une aptitude à réutiliser lesdites informations. (Duponchelle, 2015, p. 18)

En somme, l'interopérabilité permet à différents systèmes, plateformes et applications de communiquer de l'information entre eux et de réutiliser les données transférées.

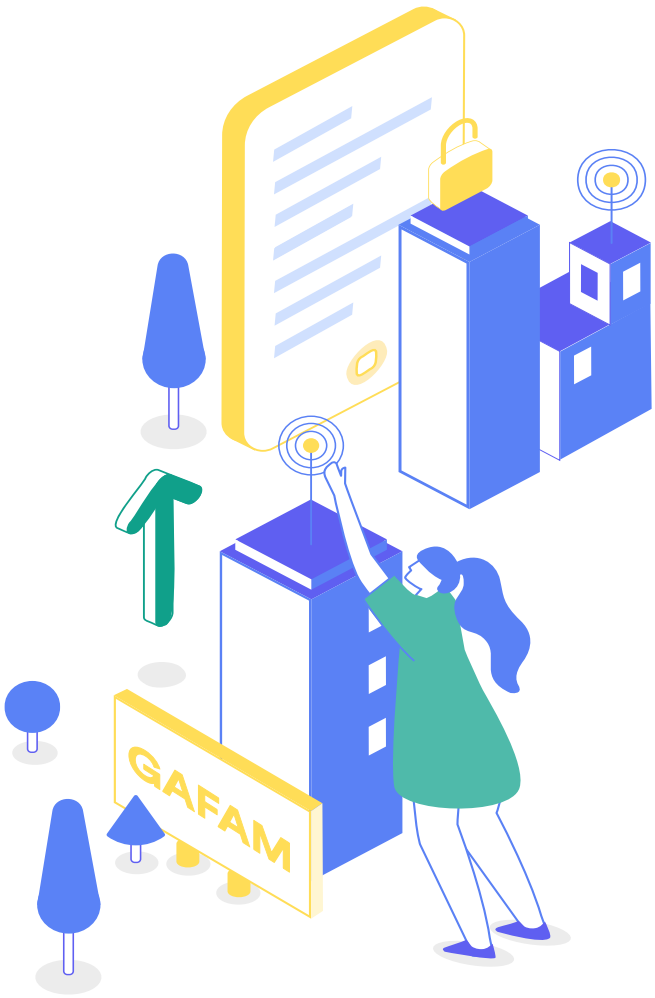
Selon le Conseil national du numérique de France, l'interopérabilité permettrait de lutter contre les effets de réseaux en animant la concurrence entre plateformes, de renforcer la liberté de choix des consommateurs de passer d'une plateforme à une autre et de renforcer la maîtrise des utilisateurs sur leurs données (2020, p. 7).

[42] Proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données, 25 novembre 2020, COM (2020) 767 final, 2020/0340 (COD).

Au Canada, l'interopérabilité fait l'objet de timides discussions. En mai 2019, le gouvernement canadien a annoncé l'adoption de la *Charte canadienne du numérique* qui énonce dix principes. L'un de ces principes est « Transparence, portabilité[43] et interopérabilité » (Gouvernement du Canada, 2019). Ce document, qui n'a aucun poids en droit puisqu'il s'agit uniquement d'un énoncé de principes, ne définit pas l'interopérabilité et il est difficile de comprendre quelles mesures le gouvernement envisage d'adopter en cette matière. Aussi, en octobre 2020, la Ville de Montréal a intégré l'interopérabilité et la portabilité des données dans sa *Charte des données numériques* afin de favoriser « l'échange, l'utilisation et l'*agnosticisme technique* » (2020, p. 12).

De leur côté, les géants du numérique comme Facebook et Microsoft produisent de la documentation et adoptent des discours concernant la portabilité et l'interopérabilité (Egan, 2019 ; Walker, 2020), cependant l'application de ces techniques n'a pas pour objectif de créer un réseau plus ouvert, mais plutôt de constamment renouveler l'intérêt des consommateurs pour leurs propres produits.

Sans présumer de la compatibilité de ces idées avec le droit québécois et de leur adéquation aux besoins des acteurs de l'économie sociale, ces deux exemples visent simplement à montrer qu'il est possible d'adapter le cadre législatif applicable aux données à des aspirations d'intérêt général. L'économie sociale, en se questionnant sur ses besoins et ses ambitions, pourrait ainsi entrevoir un cadre législatif propre à ce secteur ou du moins proposer des règles différenciées, tout en adoptant les mêmes standards de protection.



[43] En droit, la portabilité signifie qu'une personne peut demander à une entité qui a collecté ses données de lui communiquer un renseignement personnel et de lui en fournir une copie. Ce droit permet également aux individus de demander le transfert de ces renseignements à une autre personne ou organisation « autorisée par la loi à recueillir un tel renseignement » (article 112 du projet de loi n° 64 modifiant l'article 27 de la *Loi sur la protection*). À la demande du requérant, le renseignement informatisé doit être communiqué dans un « format technologique structuré et couramment utilisé ».

3. Les approches collaboratives de la gouvernance des données

La gouvernance des données peut être comprise à différents niveaux. **Dans une conception très large, la gouvernance des données « détermine qui prend les décisions, comment elles sont prises et comment les décideurs sont tenus responsables en ce qui a trait à la collecte, l'utilisation, le partage ou le contrôle des données d'une organisation ou d'un groupe »** (Gagnon-Turcotte et al., 2021, p. 33).

Dans une conception plus précise, on peut décomposer les différents éléments qui contribuent à la mise en place de cette gouvernance (Abraham et al., 2019). Ces éléments sont[44] :

1

Des **conditions préexistantes**, qui peuvent être internes (modes de fonctionnement et priorités des organisations) ou externes (législation en vigueur, normes et standards d'un milieu ou d'une région) et qui influencent le périmètre de la gouvernance des données.

2

Un **périmètre de la gouvernance** des données formé de trois sous-éléments :

a. Le niveau organisationnel de gouvernance. Qui participe à cette gouvernance ?

b. Les caractéristiques des données. Quelles sont les données concernées ?

c. Les champs d'application de la gouvernance. Quels sont les objectifs de la gouvernance ? On peut citer en exemple la qualité, la sécurité, l'architecture et le cycle de vie des données.

3

Ce périmètre détermine les **mécanismes structurels** (organes décisionnels, rôles et responsabilités, etc.), procéduraux (politiques, normes, gestion des problèmes, etc.) et relationnels (communication, formation, coordination, prise de décisions, etc.) de la gouvernance.

4

L'ensemble des conditions et des choix effectués auront des **conséquences mesurables**, que ce soit à l'égard de l'efficacité opérationnelle d'un groupe ou de la confiance entre les acteurs.

Tour d'horizon des approches collaboratives de la gouvernance de données

Dans plusieurs pays, différents acteurs réfléchissent au partage et à la mutualisation de données afin de poursuivre des objectifs communs. Différentes approches collaboratives de la gouvernance de données ont ainsi émergé, lesquelles sont intimement liées au contexte juridique de chacun de ces pays.

La plupart de ces approches impliquent une entité qui se superpose aux individus afin de prendre des décisions concernant l'accès à leurs renseignements personnels et, dans certains cas, de les protéger contre un mésusage. Cette entité peut être gouvernée de manière démocratique ou non. C'est à travers cette entité que les données peuvent être gérées comme une ressource collective et non comme une ressource individuelle.

Les partenariats de données

L'expression partenariat de données réfère à « [t]oute initiative où au moins deux organisations s'unissent autour d'un objectif commun, lequel requiert le partage et la valorisation de données » (Gagnon-Turcotte et al., 2021, p. 17). Les partenariats de données représentent donc une approche collaborative particulière de la gouvernance de données.

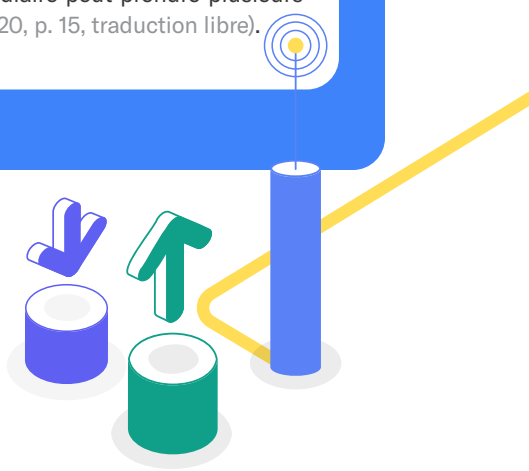
Dans la plupart des cas, cette entité est fondée sur la notion de *stewardship*. Cette notion réfère très largement au principe d'une gouvernance responsable des données qui implique un contrôle et un usage de ces données pour le bien commun ainsi qu'une surveillance de cet usage. Au Québec, la fiducie d'utilité sociale incarne bien cette notion de *stewardship*, comme il sera montré dans la prochaine section.

[44] Pour une présentation approfondie de ce cadre conceptuel, voir Gagnon-Turcotte et al., 2021, p. 33-50.

Le tableau suivant présente **les approches collaboratives de gouvernance de données les plus souvent citées** dans la littérature scientifique et la littérature grise.

Communs de données	Les communs de données impliquent des **données partagées à titre de ressource commune** et dont la gestion est assurée par une communauté d'utilisateurs (Hagan et al., 2019). Les communs de données sont un type de communs numériques.
Data trust **(hors Québec)**[45]	Il existe plusieurs définitions du *data trust*. Voici les deux plus fréquentes : « Structure légale qui permet de mettre en œuvre une **gestion raisonnée** (*stewardship*) et **fiduciaire** de données au bénéfice d'un groupe d'organisations ou d'individus » (Hardinges, 2020, traduction libre). « Mécanisme par lequel des individus **mutualisent des droits** sur les données conférées par la loi dans un ***trust***. Le fiduciaire exerce les droits en question en lieu et place des bénéficiaires de la fiducie » (Ada Lovelace Institute, 2021, p. 34, traduction libre).
Coopérative de données	Une coopérative de données consiste essentiellement à utiliser le véhicule juridique bien connu de la coopérative pour permettre à des individus et à des organisations de mutualiser des données au bénéfice du collectif. La coopérative regroupe des personnes qui s'associent afin d'exploiter une entreprise conformément aux règles d'action coopérative, incluant le **contrôle collectif et démocratique.**
Collectif de données	Cette expression englobe toutes les formes de collaboration qui regroupent des partenaires de différents secteurs (entreprises, institutions de recherche, institutions publiques) qui partagent des données afin de résoudre des problématiques sociales (Verhulst et Sangokoya, 2015 ; Bass et Old, 2020, p. 11, traduction libre). La caractéristique centrale de ce partenariat est la **diversité des partenaires** qui collaborent pour résoudre une problématique sociale donnée.
Fiduciaire de données ou intermédiaire de confiance	Un fiduciaire de données est un **intermédiaire** entre les individus et les organisations qui collectent des données. Cet intermédiaire peut prendre plusieurs **formes expérimentales** (Mozilla Insights et al., 2020, p. 15, traduction libre).

De ces approches collaboratives, trois ont été davantage expérimentées et sont donc plus abouties et documentées : les **communs de données**, le ***data trust*** et la **coopérative de données**. Celles-ci ont été élaborées et testées dans d'autres pays. La dernière section de cette synthèse examinera donc comment traduire l'une de ces approches, la **fiducie de données**, en contexte québécois.



[45] Nous utilisons le terme *data trust* afin de bien faire la distinction entre cette notion élaborée dans des pays de *common law* et la fiducie qui existe au Québec.

Les communs de données

Les communs réfèrent à des ressources qui ne sont régies ni par la propriété privée ni par une autorité publique. Les communs désignent également à la fois la communauté qui se crée autour de ces ressources et les règles qu'elle adopte concernant leur accès, leur gestion et le partage des fruits ou des bénéfices tirés de ces ressources (Coriat, 2015, p. 13).

Que sont les communs ?

La notion de communs - ou *commons* - est issue des travaux de l'économiste Elinor Ostrom et peut être définie ainsi :

> des ensembles de ressources en accès partagé et collectivement gouvernées au moyen d'une structure de gouvernance assurant une distribution des droits et des obligations entre les participants au commun (*commoners*) et visant à l'exploitation ordonnée de la ressource, permettant sa reproduction dans le long terme. (Cornu et al., 2017, p. 267-268)

Les communs sont souvent très différents les uns des autres, en plus de présenter une multiplicité d'acteurs, de modes de gouvernance et de régimes juridiques (Coriat, 2015, p. 14 ; Parance et de Saint-Victor, 2014, p. 30). Les ressources naturelles, par exemple, se retrouvent en état de rareté et de rivalité alors que l'information est abondante et non rivale. Ces distinctions font en sorte que les communs ne poursuivent pas tous les mêmes objectifs.

L'ensemble des communs vise néanmoins à répondre à une **finalité de partage et de jouissance commune** (Rochfeld, 2014a, p. 103) de « ressources tant naturelles qu'intellectuelles et d'espaces tant physiques que numériques » (Clément-Fontaine, 2014, p. 261). Les communs ont également pour caractéristique d'être fondés sur ce qui a été appelé un **faisceau de droits**, lequel décompose la propriété en différents droits pouvant être distribués à travers les personnes qui participent au commun (Schlager et Ostrom, 1992 ; Orsi, 2015, p. 53-57).

Les communs numériques occupent une place particulière dans cet éventail. Les communs numériques sont « l'ensemble des éléments disponibles au public sous une forme numérique, soit qu'ils ne relèvent d'aucun monopole *ab initio*, soit qu'ils soient mis volontairement en partage » (Cornu et al., 2017, p. 278). Un commun numérique peut porter sur un logiciel libre ou des données, par exemple.

Les communs numériques sont par ailleurs directement liés au regain d'intérêt pour les communs observé depuis quelques années. En effet, l'un des traits saillants des trois dernières décennies est le durcissement et la diversification des droits privés exclusifs sur les savoirs et l'immatériel, notamment par le truchement de la propriété intellectuelle (Coriat, 2015, p. 8-9 ; Orsi, 2015, p. 51 ; Rochfeld, 2014a, p. 105).

À l'encontre de ce durcissement, le **mouvement des logiciels libres** a permis de subvertir la propriété en montrant que cette dernière pouvait aussi bien servir à exclure les autres qu'à les inclure (Xifaras, 2010). En effet, la licence *copyleft* est fondée sur l'idée que l'auteur a le droit de partager sa création et de bannir l'exclusivité que lui procure le droit d'auteur, faisant ainsi éclater les fondements de la propriété intellectuelle (Clément-Fontaine, 2012, p. 65). Cela correspond, selon Xifaras (2010, p. 57-58), à une manière de renverser la propriété contre elle-même.

Le logiciel libre pourrait d'ailleurs illustrer la décomposition de la propriété en faisceau de droits dont il était question plus haut. L'économiste Fabienne Orsi l'explique ainsi :

> À y regarder de près, on pourrait arguer [...] que ce sont ces mêmes principes de distribution, cette même organisation de la propriété que l'on retrouve au fondement des licences des logiciels libres. Ici, le support juridique est celui du droit d'auteur lequel, plutôt que d'être utilisé dans une logique exclusiviste et propriétaire, s'ouvre, par le biais du contrat, à l'ensemble d'une communauté, et se décline en plusieurs droits et devoirs de l'usager-contributeur.
>
> [...]
>
> Dans la philosophie des logiciels libres, le droit d'auteur est mobilisé pour protéger juridiquement les libertés accordées à chacun des utilisateurs : liberté d'exécuter, de copier, de distribuer, d'étudier, de modifier et d'améliorer ces logiciels. Ainsi, ouverture et inclusion sont organisées et protégées par la propriété selon des modalités bien précises de distribution des droits qui composent le faisceau. Il se pourrait donc bien qu'un nouveau mouvement soit né, porteur d'une conception renouvelée de la propriété comme faisceau de droits. (Orsi, 2015, p. 61)

Le réseau internet a lui-même profondément marqué la théorie des communs (Hess et Ostrom, 2007 ; Le Crosnier, 2018, paragr. 3). En effet, le réseau internet est « par définition un outil décentralisé auquel techniquement chacun peut se connecter afin de permettre l'échange. L'idée de partage qui est substantielle à la notion de "commun" est également immanente au fonctionnement et aux finalités du réseau des réseaux » (Clément-Fontaine, 2014, p. 261). Toutefois, affirmer que le réseau internet s'est construit comme un commun n'implique pas qu'il soit aujourd'hui gouverné comme tel. La question de la jouissance commune de ce réseau de même que la question de sa neutralité doivent demeurer au cœur des débats actuels sur sa gouvernance (2014, p. 268).

En ce qui concerne l'application de l'idée de communs aux données, il est ardu de dégager une définition précise tant l'expression de « communs de données » réfère à un ensemble d'initiatives qui ne permettent pas de dégager des lignes directrices (Ada Lovelace Institute, 2021, p. 54 ; Bass et Old, 2020, p. 11). En fait, l'expression de communs de données est souvent utilisée de manière interchangeable pour désigner des coopératives ou des fiducies de données ou d'autres partenariats de données (Gagnon-Turcotte et al., 2021, p. 20).

De manière générale, on peut définir un commun de données comme des **données partagées à titre de ressource commune** et dont la gestion est assurée par une **communauté d'utilisateurs** (Hagan et al., 2019).

On trouve néanmoins un effort de théorisation de ces communs dans le domaine de la recherche scientifique (Bass et Old, 2020, p. 15). Un commun de données peut ainsi être entendu comme une infrastructure en ligne qui ordonne les données et leur stockage grâce à des outils couramment utilisés pour analyser et partager des données de manière à créer une ressource ouverte au sein d'une communauté de recherche (Grossman et al., 2016, p. 11). L'organisation des données en commun permet aux acteurs de la recherche de s'assurer du développement de cette ressource tout en garantissant certains standards de sécurité (Bass et Old, 2020, p. 15).

On peut aussi considérer Wikidata comme un commun de données (Mozilla Insights et al., 2020, p. 11). Wikidata est un répertoire centralisé pour les données des autres projets Wikimedia, dont Wikipédia ou Wikisource. Les données de Wikidata sont publiées sous une licence Creative Common, plus particulièrement la licence CC0 1.0 Universel (CC0 1.0) Transfert dans le Domaine Public. Cette licence permet la libre réutilisation des données, lesquelles peuvent être copiées, modifiées, distribuées et analysées, même dans un but commercial.

Le *data trust* (hors Québec)

L'expression *data trust* a fait couler beaucoup d'encre et plusieurs conceptions de cette approche de la gouvernance de données ont émergées de ce bouillonnement. Deux de ces conceptions sont ici présentées[46].

Dans une première conception, un *data trust* peut être défini comme un mécanisme permettant à des individus de **mettre en commun les droits individuels sur les données** créés par des lois. Grâce à cet outil, les fiduciaires prennent des décisions quant aux données en lieu et place des individus concernés.

Dans les pays anglo-saxons, le *trust* peut être défini comme une relation dans laquelle une ou plusieurs personnes (les fiduciaires) sont propriétaires de biens au bénéfice d'autrui (les bénéficiaires) (Vanderlinden et al., 2017 ; Pavlich, 2019, p. 5). La désignation de bénéficiaires est essentielle à la création d'un *trust* puisque le fiduciaire doit agir dans leur intérêt supérieur. Le fiduciaire doit démontrer une loyauté envers les bénéficiaires et faire preuve de diligence dans ses actions et de prudence dans sa prise de décision.

En ce sens, Sylvie Delacroix et Neil Lawrence proposent de créer des *data trusts* dans lesquels les individus seraient à la fois les créateurs de la fiducie et les bénéficiaires des données (2018). Le *data trust* constituerait ainsi un intermédiaire entre les individus qui verseraient leurs droits sur les données dans le *trust* et les utilisateurs de ces données. Les fiduciaires auraient la mission de prendre des décisions en lieu et place des individus concernés quant à l'accès et au partage des données. Ces auteurs imaginent un écosystème dans lequel des *data trusts* privés et publics émergeraient afin que les individus puissent choisir une gouvernance de données qui leur convient (Delacroix et al., 2020, p. 9). Les clauses de ce *trust* pourraient prévoir une structure de gouvernance dans laquelle les fiduciaires auraient l'obligation de consulter les constituants et les bénéficiaires. Dans un tel *trust*, les bénéficiaires sont essentiels puisque ce sont les seuls qui peuvent mettre en œuvre les obligations du fiduciaire.

La compatibilité du *trust* avec le monde des données, en premier lieu leur propriété, a été remise en question par l'Open Data Institute (ci-après « ODI »). Pour contourner cette difficulté, cette organisation suggère de créer des *data trusts* qui reprennent les idées sous-jacentes du *trust* – notamment la présence d'un fiduciaire et ses obligations de loyauté, de prudence et de diligence – sans pour autant qu'il s'agisse d'un *trust* au sens juridique du terme. Un *data trust* peut donc être compris, selon cette deuxième acception, comme une structure légale permettant de mettre en œuvre une **gestion des données raisonnée** (*stewardship*) et de **nature fiduciaire**, au bénéfice d'un groupe d'organisations ou d'individus (Hardinges, 2020).

[46] Pour une présentation plus complète des différentes conceptions de l'expression *data trust*, voir la synthèse de connaissance rédigée en anglais à ce sujet.

L'idée centrale de cette conception du *data trust* est qu'il est nécessaire de déléguer à un tiers indépendant – une entité publique ou privée – les décisions concernant les données collectées, notamment les décisions concernant l'accès à ces données et les objectifs poursuivis. Ainsi, l'entité ou l'organisation qui collecte des données déléguerait à un tiers la tâche de veiller à la bonne administration de ces données, en lui permettant de prendre des décisions concernant leur accès et leur usage (Hardinges et al., 2019). Ce tiers indépendant s'engagerait à assurer des obligations inspirées de celles du fiduciaire dans le cas du *trust* au sens légal. Il s'agirait donc d'obligations stipulées dans l'intérêt de bénéficiaires, qui pourraient être des personnes qui ont accès aux données ou qui bénéficient de l'information créée avec ces données (Hardinges, 2018).

Malgré l'engouement récent dont il fait l'objet, il existe peu d'exemples de ce type de *data trust* (Mozilla et al., 2020).

Les coopératives de données

Au Québec, une coopérative est « une personne morale regroupant des personnes ou sociétés qui ont des besoins économiques, sociaux ou culturels communs et qui, en vue de les satisfaire, s'associent pour exploiter une entreprise conformément aux règles d'action coopérative[47] ». Les membres de la coopérative s'associent afin d'exploiter collectivement et démocratiquement une entreprise.

Cette forme d'entité peut être utilisée pour mettre sur pied un projet collectif de mise en commun et de partage de données. Une coopérative de données consiste ainsi à **mettre en commun des données et à décider collectivement de leur utilisation**, tout en permettant aux individus de retirer leur consentement quant à un usage non souhaité. Il s'agit d'un moyen pour des communautés de collecter, de mettre en commun et de partager des données dans un but commun et pour des individus d'exercer un contrôle quant à l'utilisation de ces données à travers un processus démocratique et collectif (Ada Lovelace Institute, 2021, p. 49 ; Hardjono et Pentland, 2019 ; Bass et Old, 2020, p. 11 ; Gagnon-Turcotte et al., 2021, p. 21). La coopérative de données serait également un moyen de réduire les déséquilibres présents au sein de l'économie mondiale des données en créant de larges regroupements d'individus (Pentland et Hardjono, 2020, p. 3).

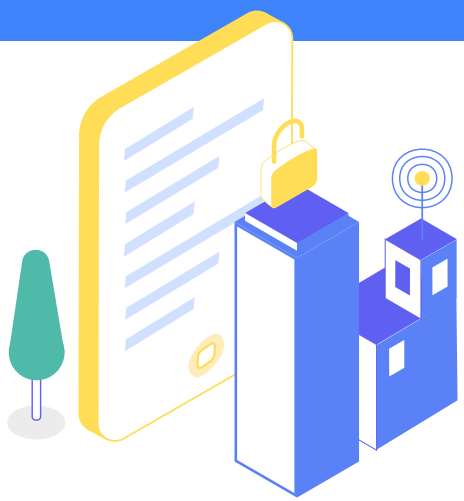
La littérature consultée ainsi que les quelques exemples de coopératives de données existantes montrent que cette forme juridique est particulièrement mobilisée en matière de renseignements personnels, mais dans une perspective de **valorisation** plutôt que de **protection** (Ada Lovelace Institute, 2021, p. 60-61). La coopérative de données prend ses distances avec l'idée d'une gestion individuelle de sa vie privée, laquelle est fondée sur la notion de consentement. En effet, pour les tenants de ce type d'organisation, les individus ont besoin d'une communauté pour évaluer les coûts et les bénéfices associés à la collecte, à l'usage et au partage de leurs informations, compte tenu du degré de complexité de ces opérations. La coopérative de données **n'exclut pas complètement la notion de consentement**, mais revoit certains de ses aspects pour les rediriger vers une **gouvernance collective** (Loi et al., 2020, p. 9).

Le coopérativisme de plateforme

Le coopérativisme de plateforme concerne la gouvernance collective et démocratique des leviers de pouvoir d'internet, soit ses plateformes et ses protocoles (Scholz et Schneider, 2016, p. 12 ; Hanna et al., 2020, p. 15).

Les plateformes coopératives sont des entreprises qui utilisent des sites internet, des applications mobiles ou des protocoles pour vendre des biens ou des services. Elles reposent sur une prise de décision collective par les personnes qui y travaillent ou utilisent leurs services (Platform Cooperativism Consortium, s.d.).

L'idée à la base du coopérativisme de plateforme est la suivante : si les plateformes étaient contrôlées par leurs usagers organisés en coopératives, la plupart des enjeux concernant la gouvernance, le traitement des employés et l'utilisation des données seraient résolus (Cousin et Martelloni, 2017, p. 28).



47 Art. 3 de la *Loi sur les coopératives*.

Les caractéristiques des coopératives de données

Les coopératives de données présentent au moins **trois caractéristiques** (Loi et al., 2020, p. 8 ; Hardjono et Pentland, 2019, p. 3 ; Hafen, 2019, p. 145).

1

Une **plateforme de gestion** ou un répertoire de données personnelles permettant aux individus de collecter, d'agréger et de contrôler une copie de leurs renseignements issus de différentes sources (dossier de santé, génome, données de commerce, etc.), leur permettant de choisir quelles données partager et avec quelle entité.

2

Un **processus démocratique** permettant aux membres de prendre des décisions collectives, notamment quant aux politiques et aux lignes directrices en matière d'éthique afin d'encadrer les transactions et les services rendus à travers le répertoire de données personnelles.

3

La coopérative doit promouvoir une **utilisation des données au bénéfice de ses membres**.

La mise en place d'une coopérative de données n'est cependant pas sans défis. Un premier obstacle concerne le changement d'échelle. La vitalité et la survie d'une telle entreprise reposent sur la faculté d'**agréger une quantité suffisante de données** et donc de mobiliser un grand nombre de personnes (Ada Lovelace Institute, 2021, p. 62). Si la coopérative de données parvient à rassembler suffisamment de membres, des questions liées à la gouvernance d'une coopérative regroupant un grand nombre de membres se poseront.

Trois exemples de coopératives de données

1

MIDATA

MIDATA est une coopérative suisse fondée en 2015. Les individus peuvent devenir membres de la coopérative, y verser leurs données personnelles, comme des données de santé, et prendre part aux décisions qui affectent l'organisation. Les personnes qui versent leurs données décident de l'utilisation que peut en faire MIDATA. Chaque personne peut notamment choisir les projets de recherche auxquels elle souhaite participer. Une charte prévoit le droit de retrait des données enregistrées. Contrairement à d'autres entreprises (TaData et Datawallet, par exemple), MIDATA ne rétribue pas les individus pour l'enregistrement de leurs données.

2

DRIVER'S SEAT

Cette coopérative incorporée aux États-Unis en 2019 a pour objectif de contribuer à la syndicalisation ou à la collectivisation de l'économie de la demande[48] (*gig economy*) dans le domaine du transport. L'application développée par Driver's Seat permet aux conducteurs de collecter les données générées par les trajets et de les partager avec la coopérative. Celle-ci agrège les données, les analyse et les communique aux membres. Ces analyses permettent aux membres d'optimiser leurs revenus en leur indiquant, par exemple, les périodes de pointe et les meilleures plateformes à utiliser selon la ville où ils travaillent. La coopérative vend également ces données aux autorités publiques afin de les soutenir dans la prise de décisions relativement à la planification du transport (Ada Lovelace Institute, 2021, p. 57).

3

SALUS COOP

Salus Coop est une autre coopérative de données vouée à la recherche en santé créée à Barcelone en 2017. Elle vise à légitimer le droit des citoyens à contrôler leurs propres données tout en facilitant leur partage dans le but d'accélérer la recherche et l'innovation en santé. Les membres de cette coopérative ont créé une licence qui s'applique aux données de recherche en santé. Cette licence impose aux utilisateurs des données d'en faire un usage exclusivement lié à la recherche biomédicale ou à la recherche en santé. Cet usage doit être non commercial, complètement anonyme et les résultats doivent être accessibles gratuitement. Les membres peuvent annuler ou modifier les conditions d'accès à leurs données à tout moment.

[48] L'économie de la demande réfère à une « [é]conomie caractérisée par une prédominance de travailleurs indépendants et de sous-traitants rémunérés à la tâche ou pour des contrats de courte durée » (OQLF, 2018).

4. Une solution propre au Québec : la fiducie d'utilité sociale de données

Auprès du grand public, la fiducie est surtout connue pour la gestion d'actifs financiers. On connaît depuis peu son potentiel pour la mise en œuvre de projets collectifs en ce qui a trait au patrimoine bâti (protection d'immeubles à forte valeur identitaire) ou naturel (protection d'écosystèmes ou de terres dont le potentiel agroécologique ou environnemental doit être préservé). Du point de vue des acteurs de l'économie sociale, la fiducie représente un moyen d'affecter des immeubles ou un terrain au bien commun afin d'en faire **une ressource commune, soustraite aux aléas et aux conséquences délétères du commerce marchand** (Marchand, 2019, p. 4).

En raison de son potentiel social en matière de gestion collective de ressources, la fiducie est également une solution avancée pour renouveler les approches collaboratives de la gouvernance de données.

Définition

Une fiducie d'utilité sociale de données est un moyen par lequel différentes organisations peuvent mettre en place une gouvernance de données responsable et digne de confiance dans un but commun et d'intérêt général.

Une fiducie (d'utilité sociale ou privée) pourrait également être mise en œuvre par une seule organisation afin d'aménager une gouvernance de données à l'interne. Il s'agirait dans ce cas d'un outil juridique privilégié par cette organisation pour encadrer sa gouvernance de données.

Les fiducies de données sont susceptibles d'avoir une panoplie d'applications, notamment dans des domaines où les données sont très sensibles, comme en santé. Nous nous concentrerons ici sur les organisations d'économie sociale qui souhaitent partager et mutualiser des données afin d'en tirer de nouvelles connaissances pour le bien commun.

Dans les faits, il n'existe à l'heure actuelle aucun projet de partage et de mutualisation de données qui emprunte le véhicule juridique de la fiducie d'utilité sociale. De nombreuses questions demeurent donc sans réponse, ce qui met en lumière la nécessité de l'expérimentation.

La fiducie en droit civil québécois[49]

La fiducie est une manière de détenir des biens pour autrui ou pour une fin particulière. Elle est constituée d'un patrimoine d'affectation, c'est-à-dire un ensemble de biens et d'obligations affectés à un but.

L'affectation réfère à un but ou une finalité. Un bien affecté possède une finalité particulière et devra être utilisé selon cette finalité et pas autrement : un terrain dont l'affectation est la conservation écologique, par exemple, ne pourra être utilisé à une fin commerciale tant et aussi longtemps que dure cette affectation.

La fiducie est fondée sur l'affectation de biens à un but particulier et non sur la propriété. En raison de leur affectation, **ces biens n'ont plus de propriétaire. Cela ne signifie pas que personne n'exerce un contrôle sur les biens en fiducie**. L'affectation des biens établit un nouveau rapport des personnes aux biens entièrement fondé sur la finalité ou le but attribué au bien. Cette affectation établit un autre régime juridique fondé sur les pouvoirs du ou des fiduciaires.

La fiducie est créée pour atteindre un objectif et les biens de la fiducie ne peuvent servir que cette finalité.

La constitution d'une fiducie d'utilité sociale

Selon le *Code civil du Québec*, « La fiducie résulte d'un acte par lequel une personne, le constituant, transfère de son patrimoine à un autre patrimoine qu'il constitue, des biens qu'il affecte à une fin particulière et qu'un fiduciaire s'oblige [...] à détenir et à administrer[50]. »

Les trois éléments essentiels pour donner vie à une fiducie d'utilité sociale

1. L'**affectation des biens** à une fin permise par la loi (détermination de la finalité ou du but).
2. La **transmission de biens** (fonciers, financiers, numériques, etc.) par le constituant à un patrimoine autonome.
3. L'**acceptation de la charge par le fiduciaire** et sa détention des biens.

[49] Nous avons délibérément évité de présenter en détail la fiducie d'utilité sociale puisque le TIESS a déjà produit une synthèse de connaissances sur cette question, en plus d'un guide.

[50] Art. 1260 du *Code civil du Québec*.

Dans le cadre d'une fiducie d'utilité sociale de données, il est important de comprendre que la transmission initiale ne concerne pas l'ensemble des données qui seront d'intérêt et dont les fiduciaires auront la charge d'administrer. Pour respecter le deuxième critère - « transmission de biens par le constituant à un patrimoine fiduciaire », - il suffit qu'un bien soit transmis au patrimoine fiduciaire ; ce bien peut être, par exemple, une somme d'argent ou la plateforme dédiée au traitement des données. Les données pourront venir augmenter la fiducie par la suite, au fil de leur collecte.

Le *Code civil du Québec* prévoit trois types de fiducies.

a. La **fiducie personnelle** est constituée dans le but de procurer un avantage à une personne déterminée[51]. Un exemple classique est un testament qui crée une fiducie pour qu'une personne puisse bénéficier des actifs de la personne défunte. Le bénéfice est direct ; dans cet exemple, les bénéficiaires reçoivent une somme d'argent ou d'autres biens selon les modalités prévues au testament.

b. La **fiducie d'utilité privée** est celle qui vise soit l'érection, l'entretien ou la conservation d'un bien corporel, soit l'utilisation d'un bien affecté à un usage particulier. Cette fiducie doit être à l'avantage indirect d'une personne ou à sa mémoire, ou bien à l'avantage d'un autre but de nature privée[52]. La portée de cette fiducie est très large. Les fiducies d'utilité privée peuvent être à vocation commerciale ou non commerciale. Elles peuvent aussi être perpétuelles.

c. Enfin, la **fiducie d'utilité sociale** est celle qui est constituée dans un but d'intérêt général, par exemple à caractère culturel, éducatif, philanthropique, religieux ou scientifique. Elle ne peut avoir pour objet essentiel de réaliser un bénéfice ou d'exploiter une entreprise[53].

La fiducie d'utilité sociale est en quelque sorte le prolongement de la fiducie d'utilité privée. Ce qui la distingue réellement, c'est l'affectation du patrimoine à un intérêt général et non privé (Beaulne, 2015, p. 107). Prenons l'exemple d'un fonds créé pour financer des études postsecondaires. Si le but stipulé est de fournir un soutien financier à une personne en particulier, comme l'enfant du constituant, il s'agit d'une fiducie d'utilité privée puisque le but est privé. Si le but stipulé est de fournir un soutien financier à des étudiants choisis annuellement afin d'encourager la persévérance scolaire, il s'agit d'une fiducie d'utilité sociale puisque le but stipulé est d'intérêt général.

Ainsi, dans le cas des données numériques, tant la fiducie d'utilité privée que la fiducie d'utilité sociale pourraient être des options envisageables. Tout dépend de la nature du but poursuivi par le ou les constituants.

51 Art. 1267 du *Code civil du Québec*.
52 Art. 1268 du *Code civil du Québec*.
53 Art. 1270 du *Code civil du Québec*.

Le potentiel de la fiducie d'utilité sociale pour la mise en œuvre d'une gouvernance de données responsable

La fiducie d'utilité sociale, envisagée comme un **outil de partage, de mutualisation ou même de gouvernance de données interne à une organisation**, ne représentera pas toujours la solution la plus appropriée ou celle qui répondra le mieux aux besoins et aux objectifs d'un projet.

Dans le processus de détermination du véhicule juridique privilégié, il est nécessaire de peser les avantages et les inconvénients de chaque véhicule. En ce qui concerne la fiducie d'utilité sociale, les éléments suivants pourront être pris en considération.

Un contrôle sur les données hors de la propriété

Les données ont une nature particulière qui les situe en inadéquation avec l'idée de propriété. Les données peuvent être **exclusives**, c'est-à-dire que leur propriétaire peut s'en réserver l'usage exclusif. Une organisation qui collecte des données peut décider qu'elle sera la seule à pouvoir les consulter et les analyser. Une fois partagées, les données deviennent néanmoins **non rivales**, c'est-à-dire qu'elles peuvent être facilement reproduites et que leur utilisation par une personne n'empêche pas leur utilisation par une autre (Cornu et al., 2017, p. 275-276). Or, l'une des caractéristiques centrales de la propriété individuelle est le fait que le propriétaire est le seul à pouvoir jouir des attributs d'un objet (Normand, 2020, p. 113). Par ailleurs, les données gagnent souvent en valeur par leur partage, et non par le fait de les garder pour soi, comportement généralement associé à la propriété. La nature non rivale des données se concilie donc difficilement avec le régime de propriété individuelle (Pellegrini, 2018, p. 515).

Certaines données, soit les renseignements personnels, ont également un cadre juridique qui leur est propre en raison des enjeux liés à la protection de la vie privée des individus. Ce cadre juridique exclut complètement l'idée de propriété et place le **consentement au cœur des opérations de collecte et de communication des données.**

La propriété fait cependant immanquablement référence au **contrôle**, ce qui, en matière de données, et plus particulièrement en matière de renseignements personnels, revêt une grande importance.

La fiducie offre ainsi une alternative à la propriété. Elle concilie d'une part le besoin de partager et de mutualiser des données et d'autre part le besoin de contrôler l'utilisation et l'accès à ces données selon une finalité déterminée. Ce contrôle est notamment assuré par le fait que la fiducie ne peut disparaître ou être détruite par la volonté des acteurs impliqués (constituants et fiduciaires). La fin de la fiducie doit être constatée, dans la plupart des cas, par un tribunal. Le contrôle découle également de l'affectation - du but déterminé par les constituants - qui encadre les décisions et les actions des fiduciaires. Enfin, des mécanismes de surveillance doivent être mis en place afin que les fiduciaires rendent compte de leur administration.

Une responsabilité claire

Tel que mentionné en introduction, le manque de confiance et d'imputabilité est un problème qu'il est nécessaire d'aborder de front en matière de gouvernance de données. Or, un aspect important de la fiducie est qu'elle rend les fiduciaires responsables de son administration.

En effet, la finalité de la fiducie **limite les actions et les décisions** que peuvent prendre les fiduciaires. Ces derniers doivent agir et décider en respectant cette finalité. S'ils agissent autrement et prennent des décisions qui vont à l'encontre de la finalité de la fiducie, ils deviennent personnellement responsables de leurs actions.

Par ailleurs, le *Code civil du Québec* prévoit un **mécanisme de surveillance et de contrôle** de l'administration de la fiducie[54]. Dans le cadre de ce mécanisme, il est prévu que les constituants, les bénéficiaires (s'ils existent) ou « un autre intéressé » puissent saisir le tribunal (Popovici, 2018, p. 230) dans le but de contraindre le fiduciaire à exécuter ses obligations, à faire un acte nécessaire à la fiducie, à l'empêcher de commettre un acte dommageable ou allant à l'encontre de l'affectation, ou de le destituer de ses fonctions.

Une solution au problème du consentement en ligne ?

Il est possible que des organisations d'économie sociale souhaitent collecter des données qui sont de la nature d'un renseignement personnel au sens de la *Loi sur la protection*. Une telle collecte devra respecter les obligations concernant le consentement. Or, un des éléments clés pour s'assurer d'un consentement libre et éclairé est l'obligation d'informer les individus sur les finalités ou les raisons de cette collecte de données[55].

C'est ici que la fiducie québécoise devient intéressante. Tout comme les règles entourant l'obtention du consentement en ligne, une fiducie de données placerait les **finalités de la collecte au cœur de son existence et de son fonctionnement.**

En effet, la finalité de la fiducie doit être déterminée dans l'acte de constitution par la ou les personnes qui la créent (les constituants). La fiducie ne peut permettre que l'on utilise les données dans un but autre que celui spécifié ; le ou les fiduciaires sont responsables que l'utilisation des données respecte la finalité déterminée en amont. Cette finalité ne peut être modifiée aisément puisque l'autorisation du tribunal est nécessaire.

La fiducie offre ainsi un cadre adéquat pour mettre en œuvre un **métaconsentement**. Dans le cadre d'un partage de renseignements personnels, le ou les fiduciaires pourraient être exemptés de demander de nouveau le consentement individuel des individus, dans la mesure où certaines conditions sont respectées.

Anne-Sophie Hulin explique ainsi cette idée :

> [...] la fiducie permettrait de mettre en œuvre un *méta-consentement* : en consentant à ce que les données soient mises en fiducies, les personnes *délèguent* leur consentement au fiduciaire à qui il appartient, par la suite, d'apprécier dans quelle mesure l'usage et le partage des données demeurent conformes aux dispositions fiduciaires. Ainsi, indirectement, les personnes retrouvent une maîtrise du traitement des données, et ce par l'intermédiaire du fiduciaire. (Hulin, 2020)

Le ou les fiduciaires pourraient ainsi donner accès aux données qu'ils contrôlent et les partager en s'assurant que cette exploitation respecte la finalité de la fiducie.

Cette idée de métaconsentement doit néanmoins être explorée davantage afin de vérifier sa conformité avec la future version de la *Loi sur la protection*. Cette question ne pourra être résolue qu'au terme de la révision de cette loi.

54 Art. 1287-1292 du *Code civil du Québec*.

55 Art. 99 du projet de loi 64 modifiant l'article 8 de la *Loi sur la protection* ; art. 13 du *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*.

Une flexibilité

À peu près tout, dans une fiducie, est soumis à la volonté et au choix des personnes qui la créent, c'est-à-dire les constituants. Les règles qui régissent la fiducie dans le *Code civil du Québec* sont peu nombreuses et laissent une grande place à la volonté des personnes impliquées.

Le *Code civil du Québec* ne limite pas les finalités qui peuvent être poursuivies par une fiducie. Ces finalités peuvent être commerciales, non commerciales, philanthropiques ou d'intérêt général.

Le *Code civil du Québec* laisse également aux constituants le soin de déterminer la durée de vie de la fiducie. La fiducie d'utilité privée et la fiducie d'utilité sociale peuvent être perpétuelles[56].

La possibilité de faire converger divers intérêts vers un but commun

La fiducie, et plus particulièrement la fiducie d'utilité sociale ou privée, pourrait permettre de faire converger les différents intérêts représentés par les individus dont les données sont collectées, les organisations qui en font la collecte et celles qui les utilisent.

Par ailleurs, la fiducie d'utilité sociale doit être constituée dans un but d'intérêt général et n'a pas pour objectif essentiel la réalisation de bénéfices ou l'exploitation d'une entreprise. Elle offre ainsi un cadre juridique intéressant pour équilibrer ces différents intérêts autour d'un objectif commun.

Une fiducie d'utilité sociale avec une affectation hors du commun

Un bon exemple de la versatilité de la fiducie est la Fiducie de recherche sur la forêt des Cantons-de-l'Est, vouée à la production de connaissances scientifiques.

La mission de cette fiducie est de « favoriser le développement et le transfert des connaissances scientifiques en aménagement forestier et en agroforesterie dans l'optique de proposer des solutions concrètes en matière de développement durable des ressources forestières et du territoire en zone habitée. »

Les constituants ont ainsi créé une fiducie dont la finalité unique répond parfaitement à leur aspiration.

[56] Art. 1273 du *Code civil du Québec*.

L'objet d'une fiducie d'utilité sociale de données

La polyvalence de la fiducie permet d'entrevoir plusieurs types de fiducies de données. Compte tenu de la nature particulière des données – exclusives mais non rivales – et de la qualification des renseignements personnels selon la *Loi sur la protection*, une fiducie de données portera vraisemblablement sur des droits et non sur les données elles-mêmes. Ces droits varieront selon le type de données (renseignements personnels, renseignements personnels sensibles ou renseignements non personnels).

Renseignements non personnels

Dans un premier cas de figure, un fiduciaire pourrait administrer des **droits relatifs à des renseignements non personnels**, comme des données descriptives. Les organisations ayant collecté ces données pourraient ainsi verser dans la fiducie les droits d'utiliser ces données à des fins d'analyse ou des droits de partage de ces données à des tiers selon les finalités et les paramètres déterminés dans l'acte de fiducie. Cet acte pourrait par exemple prévoir que ces données ne pourraient en aucun cas être partagées avec des entreprises tierces qui les utiliseraient à des fins publicitaires.

Renseignements personnels

Dans un deuxième cas de figure, une fiducie de données aurait pour objet des **droits sur des renseignements personnels** tels que définis par la loi. La *Loi sur la protection* reconnaît certains droits aux individus (notamment un droit au partage et un droit d'accès). Dans le cadre d'une fiducie de données, les individus délégueraient au fiduciaire le consentement requis pour exercer l'un ou l'autre de ces droits sous réserve du respect de certaines conditions, notamment la finalité de la fiducie. Dans le cas d'une fiducie de données de santé, par exemple, l'acte de fiducie pourrait prévoir que l'accès aux données ne serait accordé qu'à des chercheurs en santé affiliés à des universités pour les fins de leurs activités de recherche.

On peut ainsi pressentir une multitude de cas d'espèce de fiducies de données selon la nature et la diversité des données qui composent la fiducie. Cette diversité est par ailleurs la raison pour laquelle il est essentiel de tester cette innovation dans plusieurs contextes différents.

Les acteurs d'une fiducie d'utilité sociale de données

Plusieurs acteurs contribuent à la création, à l'administration ou à l'augmentation de la fiducie de données.

Le **constituant** représente la personne (un individu ou une personne morale) qui crée la fiducie par un transfert de bien. Le constituant donne littéralement vie à la fiducie. Le constituant joue en effet un rôle fondamental dans la création de la fiducie : il en détermine l'affectation. Cette finalité, une fois déterminée et consignée dans l'acte de fiducie, ne peut être modifiée autrement que par une décision du tribunal. Le constituant peut également surveiller la gestion des biens en fiducie en s'adressant au fiduciaire[57].

En ce qui concerne les fiducies de données, il est probable que les constituants seront généralement les organisations qui collectent les données ou celles qui pilotent la mutualisation des données. Il n'est pas nécessaire que tous les droits sur les données soient versés dans la fiducie au moment de sa création. Les organisations constituantes pourraient simplement transférer les sommes d'argent nécessaires à la création de la plateforme dédiée à traiter les données. La fiducie serait ainsi créée et des données pourraient y être versées par la suite.

Le **fiduciaire** est la personne désignée, généralement par le constituant, pour détenir et pour administrer la fiducie au bénéfice d'un ou de plusieurs tiers ou, dans le cas d'une fiducie d'utilité privée ou sociale, pour réaliser le but de la fiducie. Le fiduciaire n'est pas propriétaire des biens ; il les administre selon les règles de l'administration du bien d'autrui[58]. Le fiduciaire est donc central au fonctionnement de la fiducie : sans fiduciaire, la fiducie ne peut remplir son rôle puisque ni le constituant ni le bénéficiaire n'ont de droits sur les biens en fiducie. Le fiduciaire doit être une personne désintéressée, elle ne doit pas tirer profit de la fiducie. Dans le cadre d'une fiducie de données, la nomination de plusieurs fiduciaires sera probablement nécessaire, compte tenu des nombreuses connaissances requises pour administrer le patrimoine fiduciaire (sécurité de la solution technique privilégiée, stockage, architecture et analyse des données, aspects légaux, etc.).

Les **bénéficiaires** sont les personnes destinées à profiter des biens ou de l'existence de la fiducie. Il ne s'agit pas d'un rôle essentiel à la mise en place d'une fiducie ; le fait que la fiducie ait une finalité précise est plus important.

57 Art. 1287 du *Code civil du Québec*.
58 Art. 1278 du *Code civil du Québec*.

Outre les rôles centraux de constituants et de fiduciaires, une fiducie de données pourrait également réserver un rôle à la **communauté** formée autour du projet de partage ou de mutualisation de données. En effet, une fois la fiducie créée, des individus ou d'autres organisations pourront verser dans la fiducie des droits sur des données au fur et à mesure de leur collecte. Cette possibilité d'augmentation de la fiducie est prévue par l'article 1293 du *Code civil du Québec* qui traite de l'augmentation du patrimoine fiduciaire par contrat. Les droits transférés se confondront avec tous les autres droits détenus par la fiducie.

Les relations entre ces organisations, les individus concernés et la fiducie devront être opérationnalisées dans chaque cas d'espèce et inscrites soit dans l'acte de fiducie, soit dans un règlement de régie interne. Il est en effet possible de mettre en place certains aspects d'une gouvernance démocratique dans le cadre d'une fiducie[59], notamment des règles qui assurent la transparence et la reddition de compte, la représentation de différentes parties prenantes ainsi que la constitution de comités pouvant émettre des recommandations aux fiduciaires.

Les acteurs de la fiducie de données

- Déterminent l'affectation de la fiducie d'utilité sociale
- Surveillent l'administration de la fiducie

Constituants

Fiduciaires

- Administrent la fiducie
- Doivent respecter l'affectation de la fiducie
- Ne deviennent jamais propriétaires des biens

- Peuvent augmenter le patrimoine de la fiducie

Organisations qui collectent des données

Individus

- Peuvent augmenter le patrimoine de la fiducie

[59] Voir à ce sujet la synthèse de connaissances de Marie-Anne Marchand (2019) sur la fiducie d'utilité sociale, p. 22 et s.

Les enjeux

Les enjeux entourant la mise sur pied d'une fiducie de données relèvent d'au moins trois niveaux.

1

Fiducie de données

- Constituants
- Affectation de la fiducie et usage des données
- Financement
- Fiduciaires – compétences nécessaires
- Fiduciaires – pouvoirs et prises de décisions
- Fiduciaires – imputabilité, reddition de compte et assurances
- Durée

2

Interactions entre les acteurs

- Accès aux données et partage
- Littératie numérique et juridique
- Rôle de la communauté (organisations et individus)
- Gouvernance démocratique

3

Écosystème des données

- Relations de la fiducie de données avec d'autres fiducies
- Collecte de données et augmentation de la fiducie
- Interopérabilité
- Cadre juridique des données
- Stockage et architecture des données
- Analyse, publication et présentation des données

- Dans un premier temps, le **fonctionnement** de la fiducie de données devra être envisagé. L'**affectation** devra être soigneusement déterminée par les constituants afin de délimiter les paramètres de l'usage et du partage des données. Cette affectation devra être réfléchie en tenant compte de l'obligation de déterminer et de communiquer les finalités de la collecte de renseignements personnels. **Ces finalités doivent être suffisamment précises pour permettre un consentement libre et éclairé**. En ce qui concerne le fonctionnement de la fiducie, il sera également nécessaire de réfléchir au rôle des fiduciaires, aux qualités requises pour occuper cette charge et aux mécanismes de reddition de compte et de prise de décisions.
- Dans un deuxième temps, la fiducie de données sera au centre d'un certain nombre d'acteurs qui interagiront entre eux, à travers la fiducie ou autrement. Lorsque l'objectif d'une fiducie de données sera de **regrouper différents acteurs** autour d'un projet commun de partage ou de mutualisation de données, leurs relations devront être attentivement examinées. Les **questions d'accès et de partage** des données, notamment, devront être discutées en amont.
- Dans un troisième temps, la fiducie de données s'insérera dans un **écosystème plus large de données**, lequel déterminera des **contraintes techniques, économiques et légales**. Éventuellement, si plusieurs fiducies de données coexistent dans des domaines ou des champs d'application similaires, l'enjeu de la relation avec d'autres fiducies se posera également.

Cette énumération d'enjeux est prospective et n'a aucune prétention à l'exhaustivité. Elle devra être validée par l'expérimentation et par une coconstruction de connaissances. Il est possible que certains enjeux ne se posent que dans certains cas.

Les défis

La première question, fondamentale, est celle de l'opportunité du recours à la fiducie de données. Quelles sont les **utilisations les plus prometteuses** pour les fiducies de données en économie sociale ? À quels besoins concrets répondent-elles ? À cet égard, il est possible de formuler quelques hypothèses fondées sur cette synthèse de connaissances.

1

Une fiducie de données pourrait permettre une mise en commun des données d'un secteur particulier afin d'**améliorer et d'augmenter les connaissances** sur ce secteur. Elle permettrait dans ce cas d'établir un **cadre d'accès aux données mutualisées** en déterminant dans quels buts et pour quels usages cet accès serait accordé.

2

Ces connaissances pourraient être réservées aux acteurs impliqués dans la mise en place de la fiducie ou être partagées à l'externe ; la fiducie agirait alors comme **intermédiaire de partage**.

3

Une fiducie de données pourrait permettre de **créer un espace neutre de partage et de mise en commun de données**. Dans un contexte où des organisations pourraient se montrer méfiantes à l'idée de partager des données sensibles sur leur fonctionnement ou leurs activités, la fiducie de données pourrait représenter une entité dont le seul objectif consisterait à gérer l'accès aux données afin que toutes les organisations en profitent de manière égale.

4

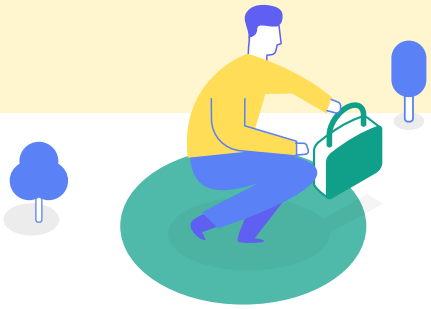
Une fiducie de données pourrait également **superviser et surveiller l'usage** des données fait par les acteurs impliqués.

5

Dans le cas où des renseignements personnels sont collectés, la fiducie de données pourrait **appuyer la mise en œuvre des obligations** auxquelles toutes les entreprises d'économie sociale qui collectent de telles données seront soumises lorsque le projet de loi 64 sera adopté. La fiducie permettrait ainsi de **mutualiser les coûts** associés à ces nouvelles obligations.

6

Dans certains cas où des renseignements personnels seront collectés, une fiducie de données pourra également être mise en place afin d'**assurer la protection** de ces renseignements. Elle serait alors un **outil de gouvernance interne** d'une organisation.



Ces usages impliquent de déléguer certaines décisions ou un certain contrôle aux fiduciaires de la fiducie de données. Un second défi consiste donc à **faire accepter cette délégation** de contrôle ou de prise de décision aux fiduciaires concernant des données sensibles (qu'il s'agisse de renseignements personnels ou non).

On doit également considérer que la fiducie représente un **instrument juridique complexe**. Dans le cadre de la création d'une fiducie de données, de nombreux efforts devront être consentis en matière d'éducation, de formation et de littératie numérique et juridique.

Finalement, l'objectif n'est pas de reproduire un écosystème fondé sur l'exploitation inéquitable des données, et ce, au détriment de certains acteurs. Il faudra donc aborder la question de la **viabilité financière** d'une fiducie de données et de la monétisation des données dans un cadre de redistribution économique et sociale.

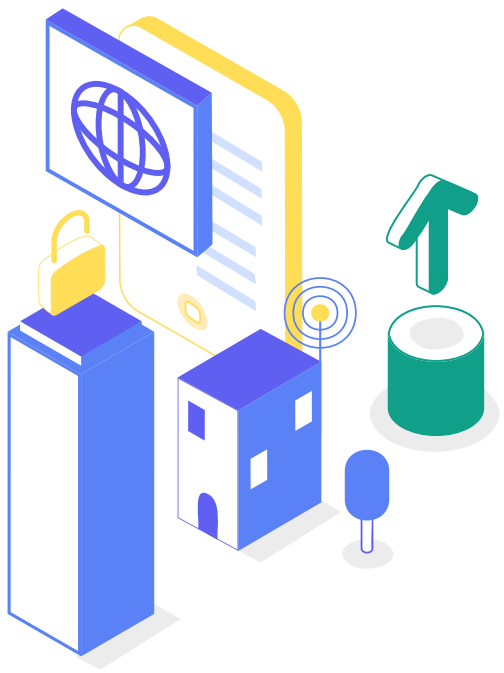
Conclusion

La fiducie de données constitue un outil de gouvernance de données parmi d'autres. Elle ne conviendra pas à toutes les situations et une analyse des besoins et des objectifs sera toujours une étape essentielle à tout projet de partage ou de mutualisation de données.

Toutefois, la fiducie de données se démarque des autres approches collaboratives de gouvernance de données pour trois raisons : elle fournit un encadrement juridique qui est à la fois établi et polyvalent ; elle place un but au centre de sa création et de son fonctionnement ; enfin, elle fait en sorte que des responsables sont clairement identifiés.

Bien que la fiducie de données ne convienne pas à toutes les situations, le secteur de l'économie sociale pourrait offrir un terrain fertile à l'expérimentation et au développement de cet outil juridique. En effet, ce secteur possède une longue tradition de pratiques collectives auxquelles se prête bien la fiducie d'utilité sociale puisqu'elle permet à des acteurs de se regrouper autour d'un but commun.

À l'heure actuelle, la fiducie de données soulève encore de nombreuses questions qui ne pourront être résolues qu'à travers l'expérimentation et la mise en pratique. Néanmoins, et bien que ces réflexions demeurent prospectives, l'outil revêt un potentiel certain.



Lexique général

Données

Les données constituent la représentation de faits sous différentes formes : textes, chiffres, images, sons ou vidéos (Gagnon-Turcotte et al., 2021, p. 43).

Renseignement personnel

Un renseignement personnel est un renseignement qui concerne une personne physique (un être humain) et qui permet de l'identifier. S'il est adopté, le projet de loi 64 précisera qu'un renseignement personnel doit permettre d'identifier directement ou indirectement une personne.

Renseignement personnel sensible

Un renseignement personnel sera considéré comme sensible lorsque, « de par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée[60] ». Les données de santé devraient, dans la plupart des cas, être des renseignements personnels sensibles.

Renseignement non personnel

Un renseignement non personnel est une donnée qui ne correspond pas à la définition d'un renseignement personnel. Des données descriptives, comme celles d'une œuvre littéraire (titre, éditeur, année de parution), sont des renseignements non personnels.

Gouvernance de données

La gouvernance de données « détermine qui prend les décisions, comment elles sont prises et comment les décideurs sont tenus responsables en ce qui a trait à la collecte, l'utilisation, le partage ou le contrôle des données d'une organisation ou d'un groupe » (Gagnon Turcotte et al., 2021, p. 33).

Partenariat de données

Un partenariat de données est une « initiative où au moins deux organisations s'unissent autour d'un objectif commun, lequel requiert le partage et la valorisation de données » (Gagnon-Turcotte et al., 2021, p. 17).

Mutualisation de données

« La mutualisation de données est le processus permettant la mise en commun de plusieurs sources de données. Les étapes de la mutualisation sont la collecte des données depuis les différentes bases existantes, l'identification des variables partagées, la création d'une clé commune, puis la combinaison sur la base de cette clé.

La mutualisation peut être interne à un organisme et lui permet d'intégrer ensemble ses différentes bases de données » (Lexique de Culture/NumériQC).

Valorisation des données

« Processus de collecte, de traitement et d'analyse de données, permettant l'utilisation optimale de celles-ci dans la poursuite d'un objectif donné » (OQLF, 2019).

[60] Art. 102 du projet de loi 64, modifiant l'article 12 de la *Loi sur la protection*.

Lexique de la fiducie

Fiducie

La fiducie est une manière de détenir des biens dans un intérêt qui n'est pas le sien. Elle constitue un patrimoine d'affectation, soit un patrimoine autonome auquel une finalité est attachée. La fiducie résulte d'un acte par lequel un constituant transfère des biens de son patrimoine à un autre patrimoine affecté à une finalité particulière et dont l'administration est assumée par un fiduciaire.

L'un de ses principaux avantages est qu'elle permet de donner un but précis (par le mécanisme de l'affectation) aux pouvoirs du ou des fiduciaires tout en modulant la responsabilité des acteurs en jeu.

Fiducie d'utilité sociale

La fiducie d'utilité sociale est une fiducie qui vise à favoriser un but d'intérêt général à caractère culturel, éducatif, philanthropique, religieux ou scientifique.

Patrimoine d'affectation

Ensemble autonome – c'est-à-dire distinct d'une personne – de droits et d'obligations assignés à la réalisation d'un but particulier (Centre Paul-André Crépeau, 2012).

Affectation

Finalité particulière attribuée à un bien (Centre Paul-André Crépeau, 2012).

Constituant(s)

Personne(s) qui crée(nt) la fiducie par un transfert de biens dans un patrimoine d'affectation. Le constituant joue un rôle crucial en ce qu'il détermine l'affectation de la fiducie. Il surveille également l'administration effectuée par le fiduciaire.

Fiduciaire(s)

Personne(s) ayant le pouvoir de gérer et d'administrer la fiducie. Un fiduciaire doit être une personne désintéressée. Les fiduciaires sont généralement des personnes physiques. Plusieurs fiduciaires peuvent être nommés pour administrer une fiducie.

Bibliographie

1. Lois et projets de lois

Code civil du Québec, RLRQ c. CCQ-1991.

Charte des droits et libertés de la personne, RLRQ c. C-12.

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c. A-2.1.

Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ c. P-39.1.

Loi sur les coopératives, RLRQ c. C-67.2.

Loi sur le droit d'auteur, L.R.C. (1985), c. C-42.

Projet de loi 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, 1re session, 42e Législature, Québec, 2020.

Proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données, 25 novembre 2020, COM(2020) 767 final, 2020/0340 (COD).

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

2. Décisions judiciaires

Frame c. Smith, [1987] 2 R.C.S. 99.

Hodgkinson c. Simms, [1994] 3 R.C.S. 377.

CCH Canadienne Ltée c. Barreau du Haut-Canada, 2004 CSC 13.

Robertson c. Thomson Corp., 2006 CSC 43.

Alberta c. Elder Advocates of Alberta Society, 2011 CSC 24.

Hindle c. Cornish, [1991] R.J.Q. 1723, J.E. 91-1118 (C.A.)

Provigo Distribution inc. c. Supermarché ARG inc., [1998] R.J.Q. 47, J.E. 98-39 (C.A.).

Bridgestone Firestone c. Trudeau, REJB 1999-14156 (C.A.).

Laoun c. Malo, [2003] R.J.Q. 381 (C.A.)

Mirarchi c. Lussier, 2007 QCCA 248.

Gaudreau c. 9090-2438, 2007 QCCA 1254.

Gahel c. Corporation Xprima.com, 2008 QCCA 1264.

Financière Banque Nationale Inc. c. Dussault, 2009 QCCA 1594.

Pascal Métal inc. c. Turcotte, 2021 QCCS 1828.

Pelchat c. Zone 3 inc., 2013 QCCS 78.

C.P. c. Équifax Canada inc., 2013 QCCAI 99.

3. Monographies

Beaulne, J. (2015). *Droit des fiducies* (3e éd.). Wilson & Lafleur.

Benyekhlef, K. et Déziel, P.-L. (2018). *Le droit à la vie privée en droit québécois et canadien*. Yvon Blais.

Cornu, M., Orsi, F. et Rochfeld, J. (2017). *Le dictionnaire des biens communs*. Presses universitaires de France.

Hess, C. et Ostrom E. (2007). *Understanding Knowledge as a Commons, From Theory to Practice.* The MIT Press.

Kitchin, R. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructure & Their Consequences.* Sage.

Normand, S. (2020). *Introduction au droit des biens* (3e éd.). Wilson & Lafleur.

Pavlich, D. (2019). *Trusts in Common-Law Canada* (3rd ed.). Lexis Nexis.

Scholz, T. et Schneider, N. (2016). *Ours to Hack and to Own: The Rise of Platform Cooperativism, A New Vision for the Future of Work and a Fairer Internet.* OR Books.

Waters, D.W.M., Gillen, M.R., et Smith, L.D. (2012). *Waters' Law of Trusts in Canada* (4th ed.). Carswell.

Zikopoulos, P.C., Eaton, C., de Roos, D., Deutsch, T. et Lapis, G. (2012). *Understanding Big Data.* McGraw Hill.

Bibliographie

4. Articles de périodiques et chapitres de livre

Abraham, R., Schneider, J. et vom Brocke, J. (2019). Data Governance: A Conceptual Framework, Structured, Review, and Research Agenda. *International Journal of Information Management,* 49, 424-438.

Ackoff, R.L. (1989). From Data to Wisdom. *Journal of Applied Systems Analysis*, 16, 3-9.

Anciaux, A. et Farchy, J. (2015). Données personnelles et droits de propriété : quatre chantiers et un enterrement. *Revue internationale de droit économique*, 29(3), 307-331.

Anciaux, A., Farchy, J. et Méadel, C. (2017). L'instauration de droits de propriété sur les données personnelles: une légitimité économique contestable. *Revue d'économie industrielle*, 158(2), 9-41.

Augagneur, L.-M. (2015). Vers de nouveaux paradigmes du droit dans l'économie numérique. *Revue trimestrielle de droit commercial et de droit économique*, 3, 455-473.

Balkin, J.M. (2016). Information Fiduciaries and the First Amendment. *UC Davis Law Review, 49*(4), 1183-1234.

Bernelin, M. (2019). La patrimonialisation des données personnelles: entre représentation(s) et réalité(s) juridique(s). *La Semaine Juridique, 46*, 2034-2041.

Cantin Cumyn, M. et Cumyn, M. (2006). La notion de biens. Dans S. Normand (dir.), *Mélanges offerts au professeur François Frenette* (p. 127-150). Les presses de l'Université Laval.

Chen, M., Ebert, D., Hagen, H., Laramee, R.S., van Liere, R., Ma, K.-L., Ribarsky, W., Scheuermann, G. et Silver, D. (2009). Data, Information, and Knowledge in Visualization. *IEEE Computer Graphics and Applications*, 29(1), 12-19.

Clément-Fontaine, M. (2012). Un renouveau des biens communs : des biens matériels aux biens immatériels. Dans M. Cornu, H.-J. Lucas, *Les modèles propriétaires - hommage au professeur Henri-Jacques Lucas* (p. 51-67). LGDJ.

Clément-Fontaine, M. (2014). Internet et la résurgence des « communs ». Dans B. Parance et J. de Saint-Victor (dir.), *Repenser les biens communs* (p. 261-274). CNRS.

Clément-Fontaine, M., Dulong de Rosnay, M., Jullien, N. et Zimmermann, J.-B., (2021). Communs numériques : une nouvelle forme d'action collective ? *Terminal, 130*. http://journals.openedition.org/terminal/7509

Courmont, A. (2015). Open data et recomposition du gouvernement urbain : de la donnée comme instrument à la donnée comme enjeu politique. *Informations sociales, 191*(5), 40-50.

Coriat, B. (2015). Introduction. Propriété, exclusivité et communs : le temps des dépassement. Dans B. Coriat (dir.), *Le retour des communs* (p. 7-20). Les liens qui libèrent.

Da Sylva, L. (2017). Les données et leurs impacts théoriques et pratiques sur les professionnels de l'information. *Documentation et bibliothèques, 63*(4), 5-34.

Debet, A. (2016). La protection des données personnelles, point de vue du droit privé. *Revue du Droit Public, 1*, 17-34.

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L. et Sanchez, I. (2018). The Right to Data Portability in the GDPR: Towards User-centric Interoperability of Digital Services. *Computer Law & Security Review, 34*(2), 193-203.

Delacroix, S. et Lawrence, N. (2019). Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance. *International Data Privacy Law, 9*(4), 236-252.

Delacroix, S. et Montgomery, J. (2020). From Research Data Ethics Principles to Practice: Data Trusts as a Governance Tool. http://dx.doi.org/10.2139/ssrn.3736090

Delacroix, S., Pineau, J. et Montgomery, J. (2020). Democratising the Digital Revolution: The Role of Data Governance. Dans B. Braunschweig et M. Ghallab (éds.), *Reflections on AI for Humanity* (p. 40-52). Springer.

Déziel, P.-L. (2018). Les limites du droit à la vie privée à l'ère de l'intelligence artificielle : groupes algorithmiques, contrôle individuel et cycle de traitement de l'information. *Les cahiers de propriété intellectuelle, 30*(1), 829-846.

Du Perron, S. (2020). La vie privée des groupes : nouveau cadre théorique pour une protection contre le profilage algorithmique. *Lex Electronica, 25*(2), 36-47.

Durand Folco, J. (2019). La « ville intelligente », au service de qui ? *Relations, 804*, 29-30.

Edwards, L. (2004). Reconstructing Consumer Privacy Protection On-line: A Modest Proposal. *International Review of Law, Computers & Technology, 18*(3), 313-344.

Bibliographie

Gidrol-Mistral, G. (2016). L'affectation à un but durable, vers une nouvelle forme d'appropriation des biens communs ? Réflexions autour de l'article 1030 du Code civil du Québec. *Revue générale de droit, 46*(1), 95-140.

Gidrol-Mistral, G. (2016). Les biens immatériels en quête d'identité. *Revue de droit de Sherbrooke, 46*, 67-137.

Grossman, R. L., Heath, A., Murphy, M., Patterson, M., et Wells, W. (2016). A Case for Data Commons: Toward Data Science as a Service. *Computing in Science & Engineering, 18(5), 10-20*. https://doi.org/10.1109/MCSE.2016.92

Guilmain, A. et Gratton, E. (2019). La protection des renseignements personnels dans le secteur privé au Québec : rétrospectives et perspectives. Dans Service de la qualité de la profession, Barreau du Québec. *Développements récents en droit à la vie privée, vol. 465* (p. 69-134). Yvon Blais.

Hafen E. (2019). Personal Data Cooperatives - A New Data Governance Framework for Data Donations and Precision Health. Dans J. Krutzinna et L. Floridi (éds.). *The Ethics of Medical Data Donation* (p. 141-149). Springer.

Ho, C.-H. et Chuang, T.-R. (2019). Governance of Communal Data Sharing. Dans A. Daly, S. K. Devitt et M. Mann (dir.), *Good Data* (p. 202-213). Institute of Network Cultures.

Kitchin, R. et McArdle, G. (2016). What Makes Big Data, Big Data? Exploring the Ontological Characteristics of 26 Data Sets. *Big Data & Society*, 3(1), 1-10.

Klein, J.-L. et Huang, P. (2013). La lutte contre l'exclusion numérique et la revitalisation des collectivités locales. *Nouvelles pratiques sociales, 26*(1), 84-101.

Lau, J., Penner, J. et Wong, B. (2020). The Basics of Private and Public Data Trusts. *Singapore Journal of Legal Studies*, 1, 90-114.

Le Crosnier, H. (2018). Communs numériques et communs de la connaissance. *tic&société, 12*(1), 1-12.

Loi, M., Dehaye, P.-O. et Hafen, E. (2020) : Towards Rawlsian 'Property-Owning Democracy' through Personal Data Platform Cooperatives. *Critical Review of International Social and Political Philosophy*. https://doi.org/10.1080/13698230.2020.1782046

Lugmayr, A., Stockleben, B., Scheib, C. et Mailaparampil, M.A. (2017), Cognitive Big Data: Survey and Review on Big Data Research and Its Implications. What Is Really "New" in Big Data? *Journal of Knowledge Management, 21*(1), 197-212.

Mann, M., Mitchell, P., Foth, M. et Anastasiu, I. (2020). #BlockSidewalk to Barcelona: Technological Sovereignty and the Social Licence to Operate Smart Cities. *Journal of the Association for Information Science and Technology, 71*(9), 1103-1115.

Mattatia, F et Yaïche, M. (2015). Être propriétaire de ses données personnelles (1re partie) : peut-on recourir aux régimes traditionnels de propriété ? *Revue Lamy droit de l'immatériel, 114*, 60-63.

Micheli, M., Ponti, M., Craglia, M. et Berti Suman, A. (2020). Emerging Models of Data Governance in the Age of Datafication. *Big Data & Society, 7*(2), 1-15.

McFarlane, B. et Stevens, R. (2010). *The Nature of Equitable Property. The Journal of Equity, 4*(3), 1-28.

Mouron, P. (2018). Pour ou contre la patrimonialité des données personnelles. *Revue européenne des médias et du numérique, 46-47*, 90-96.

Normand, S., (2004). Les nouveaux biens. *Revue du notariat, 106*(2), 177-204.

Ollion, E. et Boelaert, J. (2015). Au-delà des big data. *Sociologie, 3*(6). http://journals.openedition.org/sociologie/2613

Orsi, F. (2015). Revisiter la propriété pour construire les communs. Dans B. Coriat (dir.), *Le retour des communs. La crise de l'idéologie propriétaire* (p. 51-67). Les liens qui libèrent.

Paprica, A., Sutherland, E., Smith, A., Brudno, M., Cartagen, R. G., Crichlow, M., Courtney, B. K, Loken, C., McGrail, K. M. Ryan, A., Schull, M. J., Thorogood, A., Virtanen, C. et Yang, K. (2020). Essential Requirements for Establishing and Operating Data Trusts: Practical Guidance Co-developed by Representatives from Fifteen Canadian Organizations and Initiatives. *International Journal of Population Data Science, 5*(1), 1-10. https://ijpds.org/article/view/1353/3110

Parance, B. et de Saint-Victor, J. (2014). Commons, biens communs, communs : une révolution juridique est nécessaire. Dans B. Parance et J. de Saint-Victor (dir.), *Repenser les biens communs* (p. 9-32). CNRS.

Pellegrini, F. (2018). La portabilité des données et des services. *Revue française d'administration publique, 167*(3), 513-523.

Pentland, A., et Hardjono, T. (2020). 2. Data Cooperatives. *Building the New Economy*. https://doi.org/10.21428/ba67f642.0499afe0

Bibliographie

Popovici, A. (2018). Droits de regard : la fiducie dans le Code civil du Québec. In B. Lefebvre et C. Morin (éds). *Mélanges en l'honneur du professeur Jacques Beaulne* (p. 225-234). Wilson & Lafleur.

Rochfeld, J. (2014a). Quel modèle pour construire des « communs ». Dans B. Parance et J. de Saint-Victor (dir.), *Repenser les biens communs* (p. 103-128). CNRS.

Rochfeld, J. (2014b). Une nouvelle source en droit des contrats : la loi Informatique et libertés. *Revue des contrats, 1*, 119-122.

Rowley, J. (2007). The Wisdom Hierarchy: Representations of the DIKW Hierarchy. *Journal of Information and Communication Science, 33*(2), 163-180.

Schlager, E. et Ostrom, E. (1992). Property-Rights Regimes and Natural Resources: A Conceptual Analysis. *Land Economics, 68(3)*, 249-262.

Stoddart, J. (2020). Preface. Dans A. Guilmain et É. Gratton (dir.), *The Protection of Personal Information in the Private Sector in Québec* (p. IX-XIV). Yvon Blais.

Saint-Aubin, T. (2014). Les nouveaux enjeux juridiques des données (big data, web sémantique et linked data) : Les droits de l'opérateur de données sur son patrimoine numérique informationnel. *Revue Lamy droit de l'immatériel, 102*. https://hal-paris1.archives-ouvertes.fr/hal-01523989

Stalla-Bourdillon, S., Carmichael L. et Wintour, A. (2021). Fostering Trustworthy Data Sharing: Establishing Data Foundations in Practice. *Data & Policy, 3*, https://doi.org/10.1017/dap.2020.24

Stalla-Bourdillon, S., Thuermer, G., Walker, J., Carmichael, L. et Simperl, E. (2020). Data Protection by Design: Building the Foundations of Trustworthy Data Sharing. *Data & Policy, 2*(4), 1-10.

The First Nations Information Governance Centre (2019). First Nations Data Sovereignty in Canada. *Statistical Journal of the IAOS, 35*(1), 47-69.

van Erp, S. (2020). Management as Ownership of Data. Dans S. Lohsse, R. Schulze et D. Staudenmayer (éds.), *Data as Counter-performance – Contract Law 2.0. Munster Colloquia on EU Law and the Digital Economy* (p. 77-93). Nomos Verlagsgesellschaft.

Xifaras, M. (2010). Le copyleft et la théorie de la propriété. *Multitudes, 41*(2), 50-64.

5. Dictionnaires

Centre de recherche en droit privé et comparé du Québec. (2003). *Dictionnaire de droit privé et lexiques bilingues — Obligations.* Yvon Blais.

Centre Paul-André Crépeau de droit privé et comparé. (2012). *Dictionnaire de droit privé et lexiques bilingues — Biens.* Yvon Blais.

Office québécois de la langue française. (2018). Économie à la demande. Dans *Le grand dictionnaire terminologique*. http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26544629

Office québécois de la langue française. (2018). Valorisation de données. Dans *Vocabulaire du traitement de données*. https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/vocabulaire-traitement-donnees.aspx

Vanderlinden, J., Snow, G. et Poirier, D. (2017). *La common law de A à Z* (2e éd.). Yvon Blais.

6. Thèses et mémoires

Courmont, A. (2016). *Politiques des données urbaines : ce que l'open data fait au gouvernement urbain* [thèse de doctorat, Institute of Political Studies, Sciences Po Paris]. HAL. http://www.urbanisme-puca.gouv.fr/IMG/pdf/courmont_antoine_these.pdf

Dauverchain, M. (2018). *Le consentement dans le contexte du traitement de données personnelles sur les sites de réseautage social* [mémoire de maîtrise, Université Laval]. Corpus. https://corpus.ulaval.ca/jspui/bitstream/20.500.11794/29484/1/34026.pdf

Duponchelle, M. (2015). *Le droit à l'interopérabilité. Étude de droit de la consommation* [thèse de doctorat, École de droit de la Sorbonne]. HAL. https://tel.archives-ouvertes.fr/tel-01618804/document

Popovici, A. (2012). *Le patrimoine d'affectation. Nature, culture, rupture* [mémoire de maîtrise, Université Laval]. Corpus. http://hdl.handle.net/20.500.11794/23743

Bibliographie

7. Rapports

Ada Lovelace Institute et UK AI Council (2021, mars). *Exploring Legal Mechanisms for Data Stewardship, Working Group, Final Report*. https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/

Barreau du Québec (s.d.). *Réflexion sur une réforme de l'accès à l'information et de la protection des données personnelles.* Groupe de travail sur la protection des données personnelles. https://www.barreau.qc.ca/media/1667/rapport-reflexion-acces-information-protection-donnees.pdf

Bass, T. et Old, R. (2020). *Decode. Common Knowledge: Citizen-led Data Governance for Better Cities. DECODE and Nesta.* https://media.nesta.org.uk/documents/DECODE_Common_Knowledge_Citizen_led_data_governance_for_better_cities_Jan_2020.pdf

Blankertz, A. (2020). *Designing Data Trusts. Why We Need to Test Consumer Data Trusts Now*. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/designing_data_trusts_e.pdf

BPE Solicitors, Pinsent Masons et Reed, C. (2019). *Data Trusts: Legal and Governance Considerations*. Open Data Institute. http://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf

Breux, S., et Diaz, J. (2017). *La ville intelligente. Origine, définitions, forces et limites d'une expression polysémique.* INRS, Centre urbanisation, culture, société. http://espace.inrs.ca/id/eprint/4917/1/Rapport-LaVilleIntelligente.pdf

Commissariat à la vie privée. (2014). *Métadonnées et vie privée. Un aperçu technique et juridique*, Ottawa. 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/2014/md_201410/

Conseil d'État. (2014). *Le numérique et les droits fondamentaux, Paris, La Documentation française.* Les rapports du Conseil d'État. https://www.conseil-etat.fr/ressources/etudes-publications/rapports-etudes/etudes-annuelles/etude-annuelle-2014-le-numerique-et-les-droits-fondamentaux

Conseil national du numérique. (2014). *Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouvert et soutenable, Rapport remis au ministre de l'Économie, du Redressement productif et du numérique et à la secrétaire d'État chargée du numérique.* https://cnnumerique.fr/files/2017-09/CNNum_Rapport_Neutralite_des_plateformes.pdf

Conseil national du numérique. (2020). *Concurrence et régulation des plateformes. Étude de cas sur l'interopérabilité des réseaux sociaux.* https://cnnumerique.fr/files/uploads/2020/2020.07.06.ra_cnnum_concurrence_web.pdf

Cousin, L. et Martelloni, L. (2017). *A Cooperative Vision for the Collaborative Economy: Shaping a People-Centered and Democratic Collaborative Economy.* Cooperatives Europe. https://coopseurope.coop/node/712

Coutts, S. et Gagnon-Turcotte, S. (2020). *Data Governance and Digital Infrastructure, Analysis and Key Considerations for the City of Toronto, Final Report*. Open North. https://www.toronto.ca/wp-content/uploads/2020/08/95fb-2020-07-10-Open-North-Data-Governance-Report-Main-report-WEB.pdf

Delmas-Marty, M. (2020). Repenser le droit du numérique. *CNIL Cahiers IP Innovation & Prospective no 1, Vie privée à l'horizon*, 54. https://www.cnil.fr/sites/default/files/typo/document/CNIL-CAHIERS_IPn1.pdf

Duboc S. et Noël, D.J. (2021). *Économie et gouvernance de la donnée*. Conseil économique, social et environnemental. https://www.lecese.fr/sites/default/files/pdf/Avis/2021/2021_06_eco_gouv_donnee.pdf

Element AI et Nesta. (2019). *Data Trusts: A New Tool for Data Governance*. Element AI. hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf

Fournier Gosselin, V., Grondin, C., Joyce, A., Dumas, A., Mheir, F. et Rousseau, M. (2021). *Chantiers sur l'avenir du commerce de détail au Québec*. https://drive.google.com/file/d/1yrVYPYFWTzxK3mdBa1dHBk4I07AC-4xl/view

Gagnon-Turcotte, S., Sculthorp, M. et Coutts, S. (2021). *Les partenariats de données numériques : mettre les bases d'une gouvernance de données collaborative dans l'intérêt du public.* Nord Ouvert. https://opennorth.ca/fr/publications/1e9rhhxmmlkhdngj1a7gsz_fr

Graef, I., Gellert, R., et Husovec, M. (2018). *Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-personal Data Is Counterproductive to Data Innovation.* Tilburg University, TILEC Discussion Paper No. 2018-029. https://www.readcube.com/articles/10.2139%2Fssrn.3256189

Bibliographie

Hall, W. et Pesenti, J. (2017). *Growing the Artificial Intelligence Industry in the UK*. Government of the United Kingdom. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf

Hanna, T. et Lawrence M. (2020). *A Common Platform: Reimagining Data and Platforms*. Common Wealth et Democracy collaborative. https://democracycollaborative.org/common-platform?mc_cid=fd7223e9ea&mc_

Hardinges, J., Wells, P., Blandford, A., Tennison, J. et Scott, A. (2019). *Data Trusts: Lessons from Three Pilots. Open Data Institute*. https://theodi.org/article/odi-data-trusts-report/

Hardjono, T. et Pentland, A. (2019). *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management.* Cornell University. https://arxiv.org/abs/1905.08819

HM Treasury. (2018). *The Economic Value of Data: A Discussion Paper*. https://www.gov.uk/government/publications/the-economic-value-of-data-discussion-paper

Hoffmann, J. et Gonzalez Otero, B. (2020). *Demystifying the Role of Data Interoperability in the Access and Sharing Debate*. Max Planck for Innovation and Competition Research Paper No. 20-16, 20-21.

Léger, L. et Bentata, P. (2019). *Aux data, citoyens! Pour une patrimonialité des données personnelles*. Génération Libre. https://www.generationlibre.eu/aux-data-citoyens/

Marchand, M.-A. (2019). *Les fiducies d'utilité sociale : synthèse de connaissances. Territoires innovants en économie sociale et solidaire*. TIESS.

Mozilla Insights, Brandusescu, A. et van Geus, J. (2020). *Shifting Power through Data Governance. Mozilla Insights*. https://foundation.mozilla.org/en/initiatives/data-futures/data-for-empowerment/#10-data-governance-approaches-explored

OCDE. (2015). *Data-Driven Innovation: Big Data for Growth and Well-Being*. OECD Publishing.

OCDE. (2020). *Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information*. OECD/LEGAL/0362. https://legalinstruments.oecd.org/public/doc/122/122.en.pdf

O'Hara, K. (2019). *Data Trusts, Ethics, Architecture and Governance for Trustworthy Data Stewardship*. WSI White Paper # 1. https://cdn.southampton.ac.uk/assets/imported/transforms/content-block/UsefulDownloads_Download/0326D18DCC9E4BD08816BB5F994FCA76/White%20Papers%20No1.pdf

Scassa, T. (2018). *Data Ownership*. CIGI Papers No. 187. https://www.cigionline.org/sites/default/files/documents/Paper%20no.187_2.pdf

Secrétariat du Conseil du trésor. (2018). *Plan d'action pour l'accessibilité et le partage des données ouvertes des ministères et des organismes publics*. Gouvernement du Québec. www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/gouvernement_ouvert/plan_action_gouvernement_ouvert.pdf

Secrétariat du Conseil du trésor. (2019). *Stratégie de transformation numérique gouvernementale 2019-2023*. Gouvernement du Québec. www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/Strategie_TNG.pdf

Shearmur, R., Charron, M., et Pajevic, F. (2017). *La* 'région rurale intelligente' *à l'aune de la* 'ville intelligente' : *définition, critique et enjeux*, Document de travail préparé pour le Centre de recherche de développement territorial. http://crdt.ca/images/Documents/projets-resultats-enquete/2017_Shearmur_la_region_intelligente.pdf

Statistique Canada (2019a). *Enquête canadienne sur l'utilisation de l'Internet*. https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-fra.pdf

Statistique Canada (2019b). *La valeur des données au Canada : estimations expérimentales.* https://www150.statcan.gc.ca/n1/pub/13-605-x/2019001/article/00009-fra.htm

Tchéhouali, D. et Plamondon, J. (2018). *Données d'usage et usage des données à l'ère des plateformes : De la nécessité d'un encadrement règlementaire pour une meilleure affirmation de notre souveraineté numérique*. ISOC Québec, Coalition pour la culture et les médias (CCM).

Union des consommateurs. (2019). *Une charte des droits des internautes. Pour une perspective canadienne*. https://uniondesconsommateurs.ca/wp-content/uploads/2020/09/811429-rapport_Charte-droits-internautes_final.rev_.pdf

Bibliographie

8. Articles de journaux

Cadwalladr, C. et Graham-Harrison, E. (2018, 10 mars). Revealed: 50 million Facebook Profiles Garvested for Cambridge Analytica in Major Data Breach. *The Guardian*. www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Jung, D. (2020, 10 juin). COVID-19 : l'application de traçage du Mila mise au placard par Ottawa. *Radio-Canada*. https://www.lapresse.ca/covid-19/2020-06-10/application-de-tracage-covi-les-gens-de-mila-rendent-les-armes

Lévesque, F. (2020, 12 juin). Données personnelles : des amendes pouvant aller jusqu'à 25 millions. *La Presse*. https://www.lapresse.ca/actualites/politique/2020-06-12/donnees-personnelles-des-amendes-pouvant-aller-jusqu-a-25-millions.

Nora, D., Pénicaud, N. et Soula, C. (2014, 17 avril). Révolution big data, gros business. *Nouvel Observateur*, 66-70.

Trudel, P. (2018, 13 mars). La valeur de nos données personnelles. *Le Devoir*. https://www.ledevoir.com/opinion/chroniques/522496/la-valeur-de-nos-donnees-personnelles.

9. Articles en ligne

Du Perron, S. (2020). Projet de loi 64 : une réforme à l'européenne du droit à la protection des renseignements personnels. *Laboratoire de cyberjustice*. https://www.cyberjustice.ca/2020/06/17/projet-de-loi-64-une-reforme-a-leuropeenne-du-droit-a-la-protection-des-renseignements-personnels/

Hagan, M., Dempsey, J. et Jiménez, J.G. (2019). A *Data Commons for Law*. Medium. https://medium.com/legal-design-and-innovation/a-data-commons-for-law-60e4c4ad9340

Hardinges, J. (2018). *Defining a Data Trust*. ODI. https://theodi.org/article/defining-a-data-trust/

Hardinges, J. (2020). *Data Trusts in 2020*. ODI. https://theodi.org/article/data-trusts-in-2020

Hulin, A.-S. (2020). *Introduction à la fiducie québécoise de données*. Laboratoire de cyberjustice. https://www.cyberjustice.ca/2020/11/26/introduction-a-la-fiducie-quebecoise-de-donnees/

Lawrence, N. (2016). *Data Trusts.* Inverse Probability. https://inverseprobability.com/2016/05/29/data-trusts

McFarlane, B. (2019). *Data Trust and Defining Property. Property law*. https://www.law.ox.ac.uk/research-and-subject-groups/property-law/blog/2019/10/data-trusts-and-defining-property

Uzan-Naulin, J. et Barbach, A. (2020). PL 64 – *C comme consentement – Une simplification complexe ?* Fasken. https://www.fasken.com/fr/knowledge/projet-de-loi-64/2020/06/29-pl64-c-comme-consentement

Valverde, M. (2019a). *Google's "Urban Data" Plan: Evading Regulation While Promoting the Appearance of Transparency*. Centre for Free Expression. https://cfe.ryerson.ca/blog/2019/05/google%E2%80%99s-%E2%80%9Curban-data%E2%80%9D-plan-evading-regulation-while-promoting-appearance-transparency

Valverde, M. (2019b). *What Is a Data Trust and Why Are We Even Talking About It? Sidewalk Labs' Magic Tricks*. Centre for Free Expression. https://cfe.ryerson.ca/blog/2019/01/what-data-trust-and-why-are-we-even-talking-about-it-sidewalk-labs%E2%80%99-magic-tricks

Verhulst, S. G. et Sangokoya, D. (2015). *Data Collaboratives : Exchanging Data to Improve People's Lives*. Medium. https://medium.com/@sverhulst/data-collaboratives-exchanging-da-ta-to-improve-people-s-lives-d0fcfc1bdd9a

Walker, K. (2020). *In Support of Interoperability*. Google. The Keyword, https://blog.google/outreach-initiatives/public-policy/support-interoperability/

Wylie, B. et McDonald, S. (2018). *What Is a Data Trust?* Centre for International Governance Research. https://www.cigionline.org/articles/what-data-trust

Bibliographie

10. Autres

Culture/NumériQC. (s.d.). *Lexique de Culture*. https://culturenumeriqc.qcnum.com/lexique/

Culture pour tous. (s.d.). *Les métadonnées*. https://www.culturepourtous.ca/professionnels-de-la-culture/mutualisation/les-metadonnees/

Egan, E. (2019). *Portabilité et protection des données et de la vie privée*. Facebook. https://about.fb.com/fr/news/2019/09/comment-tracer-la-voie-a-suivre-en-matiere-de-confidentialite-et-de-portabilite-des-donnees/

First Nations Information Governance Centre. (2021). *Les principes de PCAP des Premières Nations*. https://fnigc.ca/fr/les-principes-de-pcap-des-premieres-nations/

Future Cities Canada. (s.d.). https://futurecitiescanada.ca/fr/portail-old/

Gouvernement du Canada. (2019). *Renforcer la protection de la vie privée dans l'ère numérique*. https://www.ic.gc.ca/eic/site/062.nsf/fra/h_00107.html

International Open Data Charter. (2015, September). *Principles*. https://opendatacharter.net/principles/

Laboratoire d'innovation urbaine de Montréal. (2020). *Charte des données numériques*. Ville de Montréal. https://laburbain.montreal.ca/sites/default/files/charte_donnees_numeriques_1_0.pdf?fbclid=IwAR2PWKyS98hrB0nJ58-xKTn_Ll6ztuBvdN0WISCMobdhBCzErGAaudnQ0xo

Ligue des droits et libertés. (2020). *Mémoire présenté dans le cadre des Consultations particulières et auditions publiques au sujet du projet de Loi 64 : Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*. https://liguedesdroits.ca/wp-content/fichiers/2020/09/memoire_projet_loi_64_renseignement_personnel_20200923.pdf

MIDATA. (s.d.). *Coopérative*. https://www.midata.coop/fr/cooperative/

Platform Cooperativism Consortium. (s.d.). *What is a Platform Co-op*. https://platform.coop/

Sidewalk Labs (2018). *Digital Governance Proposals for DSAP Consultation*. https://waterfrontoronto.ca/nbe/wcm/connect/waterfront/41979265-8044-442a-9351-e28ef6c76d70/18.10.15_SWT_Draft+Proposals+Regarding+Data+Use+and+Governance.pdf?MOD=AJPERES

Limite de responsabilité

Le TIESS, ses employés et son conseil d'administration ne peuvent être tenus responsables d'un dommage présenté comme résultant de l'utilisation de cette synthèse dans le cadre d'une participation ou du démarrage d'un projet de fiducie d'utilité sociale de données, dans la collecte ou le partage de renseignements personnels ou dans l'application d'une politique de confidentialité des renseignements détenus par une organisation.

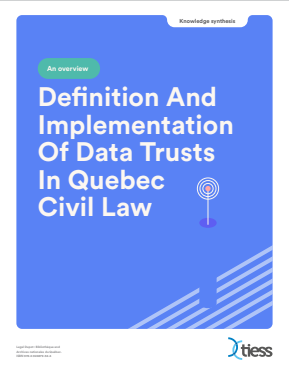
Les informations contenues dans ce guide sont fournies par le TIESS à titre indicatif seulement et ne visent pas à conseiller le public quant à ses droits et obligations légales. Elles reposent notamment sur des lois et des règlements qui peuvent être différents au moment de la consultation, voire inapplicables ou non conformes à la situation du lecteur. Ainsi, rien dans ce texte ne peut être interprété comme une opinion professionnelle ou une réponse à une situation particulière.

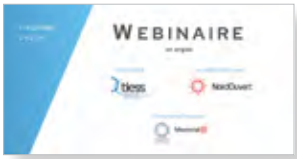
Ces informations ne peuvent remplacer la consultation d'un professionnel, avocat ou notaire. Une telle consultation est recommandée à toute personne ou organisme qui souhaite s'engager dans un processus visant la constitution d'une fiducie d'utilité sociale de données.

Cette synthèse vous a-t-elle été utile ? Avez-vous des suggestions pour l'améliorer ? Nous sommes à votre écoute : **info@tiess.ca**

Poursuivez votre lecture

Sur le même sujet





Webinaire Data Governance and Data Trust

Introduction à la fiducie québécoise de données (article)

Nos publications récentes

Et toutes les autres publications disponibles sur tiess.ca/publications

Québec Montréal

COMMON APPROACH
TO IMPACT MEASUREMENT