

LA GOUVERNANCE DES DONNÉES  
DANS LE DOMAINE DE LA SANTÉ

# POUR UNE FIDUCIE DE DONNÉES AU QUÉBEC ?

Kassandra McAdams-Roy, Philippe Després,  
Pierre-Luc Déziel

Janvier 2021



OBSERVATOIRE INTERNATIONAL  
SUR LES IMPACTS SOCIÉTAUX  
DE L'IA ET DU NUMÉRIQUE

Ce rapport a été réalisé avec le soutien financier de l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA) et des Fonds de recherche du Québec.

**Pour citer ce rapport :**

McAdams-Roy, K., Després, P., Déziel, P-L. (2021). La gouvernance des données dans le domaine de la santé : Pour une fiducie de données au Québec ? Observatoire international sur les impacts sociétaux de l'IA et du numérique, Québec, 55p. [doi.org/10.5281/zenodo.7617888](https://doi.org/10.5281/zenodo.7617888)



Cette œuvre est mise à disposition selon les termes de la [Licence Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/).



**Observatoire international sur les impacts sociétaux de l'intelligence artificielle et du numérique**

Pavillon Charles-De Koninck, local 2489  
1030, avenue des Sciences-Humaines  
Université Laval  
Québec (Québec) G1V 0A6

observatoireia@ulaval.ca  
observatoire-ia.ulaval.ca

DOI : 10.5281/zenodo.7617888  
ISBN : IS978-2-925138-22-8

## SOMMAIRE EXÉCUTIF

### Promesses technologiques et protection des intérêts personnels à l'ère des données massives : Comment trouver un juste milieu ?

Les nouvelles technologies numériques ont connu d'importants avancements au cours des dernières années. Étant à l'aube de l'ère de l'intelligence artificielle, ces dernières ont créé une soif inédite pour les données de toutes sortes.

Bien que ces technologies soient prometteuses de nombreuses améliorations à nos vies quotidiennes ainsi qu'à plusieurs domaines telle la médecine, le droit, et la pharmacologie, elles engendrent aussi de nombreuses préoccupations. Pour un, la concentration de pouvoir en les plus grands détenteurs de données crée un déséquilibre de pouvoir important avec les individus et le degré de contrôle qu'ils détiennent sur leurs données personnelles, et soulève aussi plusieurs questions en matière de droit de la concurrence et d'antitrust. Les pratiques de ces entreprises qui tendent à manipuler leurs utilisateurs à leur profit soulèvent également des questions d'ordre éthique. Il y a aussi lieu de se méfier d'un pouvoir de surveillance étatique qui deviendrait trop large.

Pris ensemble, ce contexte ainsi que les nombreux scandales impliquant des atteintes à la protection des données personnelles ont donné lieu à une importante érosion de la confiance du public au courant des dernières années.

Ainsi, il y a actuellement un effort en cours pour trouver des solutions qui sauront mieux encadrer ces nouvelles technologies et protéger les intérêts individuelles et collectifs, sans toutefois nuire à l'essor de leur plein potentiel.

La fiducie de données fut identifiée comme une telle solution. Prônée pour sa versatilité et sa flexibilité, elle est présentée comme un outil qui permettrait de trouver un juste milieu entre innovation et protection des intérêts individuels dans le cadre d'une stratégie de gouvernance responsable des données. Plusieurs sont ainsi à étudier son applicabilité dans différents secteurs et différentes juridictions et elle est l'objet de la présente étude.

Cette étude s'intéresse spécifiquement à savoir si une fiducie de données pourrait être établie au Québec pour la gestion des données dans le domaine de la santé.

Étant donné que ce domaine représente des enjeux et intérêts particuliers au niveau de la gestion des données, cette étude propose dans un premier temps de revoir en quoi consiste la gouvernance de données afin de définir comment celle-ci devrait s'opérer dans le domaine de la santé. La première partie prendra donc en revue la notion de gouvernance des données en général ainsi que les principales approches à celle-ci. La deuxième partie entreprendra ensuite une étude détaillée de la fiducie de données afin de déterminer son applicabilité dans le domaine de la santé au Québec. Une revue de la littérature identifiera les principaux indicateurs et principes directeurs qui devront dicter la constitution d'une telle fiducie. Elle identifiera aussi les principaux obstacles et défis à sa constitution. Une analyse détaillée du droit des fiducies du Québec sera enfin effectuée afin de déterminer si le régime québécois peut répondre aux critères identifiés.

Pour résumer très sommairement les principales conclusions du rapport, l'analyse révèle que le droit québécois s'avèrerait des plus convenable pour la constitution d'une fiducie de données dans le domaine de la santé au Québec. Il comprend évidemment toutes les obligations qui sont typiquement reconnues à la charge fiduciaire, mais il assujetti aussi ce dernier au régime de la pleine administration du bien d'autrui qui encadre davantage le rôle du fiduciaire. Il prévoit aussi d'intéressantes mécanismes de contrôle et de surveillance de l'administration fiduciaire qui accorde plus de poids au principe de gouvernance responsable qu'il intègre déjà très bien. Autrement, bien qu'il laisse à désirer au niveau du contrôle et de la surveillance des tiers qui seront éventuellement accordés un droit d'usage aux données, le droit québécois permet néanmoins d'en disposer par le truchement du régime de la responsabilité extracontractuelle. En effet, la flexibilité du véhicule permettra que soient intégrés au sein de sa structure de gouvernance de multiples contrats qui pourront prévoir des obligations à différents niveaux. Ceci permettra au fiduciaire d'effectuer un contrôle sur les usagers éventuels en vertu de son droit d'ester en justice pour tout ce qui relève de la protection des intérêts de la fiducie. Aussi, les personnes ayant subi un préjudice – soit par une administration défaillante du fiduciaire, soit par une utilisation défaillante de leurs données par les usagers ayant été accordés un droit d'usage – pourront poursuivre le responsable en justice en vertu de la responsabilité civile extracontractuelle. Le droit d'action en vertu des lois sur la protection des renseignements personnels demeurera également toujours possible.

Autrement, la fiducie de données québécoise connaîtra certains des autres défis identifiés dans la littérature, mais ceux-ci ne seront pas insurmontables de sorte à écarter la possibilité de sa constitution. Le seul défi potentiellement fatal à sa constitution sera celle en lien avec la nature juridique des données personnelles. En effet, la fiducie québécoise, bien qu'elle soit distincte de par la novation que représente son patrimoine d'affection, demeure toutefois un véhicule assorti d'un patrimoine qui est *par définition* composé de biens au sens légal. Qu'il soit d'affectation ou non, les biens qui le composent doivent être des choses de nature appropriables. Or, tel n'est pas jusqu'à présent la nature des données personnelles, celles-ci se rattachant au droit à la vie privée et étant ainsi des choses de nature *extrapatrimoniale*. Ni les données en tant que telle, ni un droit d'usage quelconque sur celles-ci ne pourraient alors être 'transféré' en fiducie, comme le veut la condition *sine qua non* de la constitution d'une fiducie en droit québécois. Une considération particulière devra donc être portée sur ce point avant d'entreprendre un projet de fiducie de données au Québec, puisqu'advenant un litige quelconque, on risque de ne pas reconnaître le véhicule en tant que fiducie, et ceci risque d'avoir des implications importantes quant aux mécanismes qui demeureront disponibles pour retenir la responsabilité soit du fiduciaire, soit des usagers des données.

# TABLE DES MATIÈRES

<b>INTRODUCTION</b> .....	<b>7</b>
<b>I. EXPOSÉ DE LA PROBLÉMATIQUE</b> .....	<b>7</b>
<b>PARTIE I : LA NOTION DE GOUVERNANCE DES DONNÉES</b> .....	<b>9</b>
<b>I. DES SOLUTIONS ÉQUILIBRÉES POUR UNE MEILLEURE GOUVERNANCE DES DONNÉES</b> .....	<b>9</b>
A. En quoi consiste la gouvernance des données ? .....	9
B. Quelles approches sont envisageables pour une meilleure gouvernance des données ?.....	10
1. Renforcer le cadre réglementaire .....	10
2. Redonner plus de contrôle aux individus en leur reconnaissant la patrimonialité sur leurs données personnelles .....	12
3. Les modèles fiduciaires de gouvernance des données .....	13
<b>PARTIE II : LA FIDUCIE DE DONNÉES COMME OUTIL DE GOUVERNANCE DES DONNÉES DANS LE DOMAINE DE LA SANTÉ</b> .....	<b>15</b>
<b>I. LE DATA TRUST OU LA “FIDUCIE DE DONNÉES” : SUJET DE LA PRÉSENTE ÉTUDE</b> .....	<b>15</b>
A. Genèse de l’idée du data trust et bref introduction de la fiducie légale .....	15
B. Raisons pour lesquelles la fiducie de données suscite intérêt à titre d’outil pour la gouvernance des données .....	16
C. La notion de stewardship comme centrale à l’idée d’une fiducie de données et une gouvernance responsable des données .....	18
D. Les particularités d’une fiducie de données dans le domaine de la santé .....	20
1. Enjeux de gouvernance.....	20
2. Finalité et principes directeurs.....	26
3. Autres indicateurs à titre de meilleures pratiques.....	27
4. Principaux obstacles et défis .....	27
5. Obstacles potentiellement fatals .....	31
<b>PARTIE III : ÉTUDE DÉTAILLÉE DE LA FIDUCIE EN DROIT QUÉBÉCOIS</b> .....	<b>33</b>
<b>I. POUR UNE FIDUCIE DE DONNÉES DANS LE DOMAINE DE LA SANTÉ AU QUÉBEC ?</b> .....	<b>33</b>
A. Les obligations fiduciaires et le principe de gouvernance responsable.....	36
1. Le rôle du fiduciaire : administrateur du bien d’autrui chargé de la pleine administration .....	36
2. Les obligations qui imposent au fiduciaire .....	37
3. Le droit d’action en cas d’administration défailante du fiduciaire.....	39

B. Les mesures de contrôle et de surveillance.....	40
1. L’inventaire, la reddition de compte et la garantie (assurances-responsabilité).....	40
2. Les pouvoirs de surveillance du constituant, du bénéficiaire et de toute autre personne intéressée .....	41
3. La surveillance « des personnes et organismes désignés par la loi » .....	41
C. La responsabilité des tiers .....	42
D. La versatilité et flexibilité du véhicule en général .....	43
1. Versatilité et flexibilité au niveau de la constitution de la fiducie .....	43
2. La possibilité d’apporter des modifications à la fiducie .....	44
3. L’extinction de la fiducie et ses effets .....	45
E. Versatilité et flexibilité eu égard aux principaux acteurs de la fiducie .....	46
1. Le constituant.....	46
2. Le bénéficiaire et la faculté d’élire .....	47
3. Le fiduciaire .....	48
a) L’administration collective .....	48
b) La possibilité de délégation.....	48
F. Les trois grandes catégories de fiducies en droit québécois : laquelle pour une fiducie de données ? .....	49
1. La fiducie personnelle .....	49
2. La fiducie d’utilité privée .....	49
3. La fiducie d’utilité sociale.....	51
G. Une fiducie de données au Québec saura-t-elle relever les défis précités ?.....	53
1. La patrimonialité des données .....	53
2. Financement .....	54
3. Consentement .....	54
4. Les autres défis potentiels.....	54

# INTRODUCTION

## I. Exposé de la problématique

### *Promesses technologiques et protection des intérêts individuels à l'ère des données massives : Comment trouver un juste milieu ?*

Les nouvelles technologies numériques ont connu d'importants avancements au courant des dernières années. Étant à l'aube de l'ère de l'intelligence artificielle<sup>1</sup>, ces dernières ont créé une soif inédite pour les données de toutes sortes. En effet, s'alimentant principalement de mégadonnées, la plupart désignent celles-ci comme le « nouvel or noir »<sup>2</sup> ou le « pétrole du XXI<sup>e</sup> siècle »<sup>3</sup>, et les entreprises qui ont su maîtriser l'art de les exploiter se retrouvent aujourd'hui parmi les plus valorisées en bourse.

Bien que ces technologies soient prometteuses de nombreuses améliorations à nos vies quotidiennes ainsi qu'à plusieurs domaines telle la médecine<sup>4</sup>, le droit<sup>5</sup>, et la pharmacologie<sup>6</sup>, elles engendrent aussi de nombreuses préoccupations. Pour un, la concentration de pouvoir en les plus grands détenteurs de données crée un déséquilibre de pouvoir important avec les individus et le degré de contrôle qu'ils détiennent sur leurs données personnelles,<sup>7</sup> et soulève aussi plusieurs questions en matière de droit de la concurrence et d'*antitrust*.<sup>8</sup> Les pratiques de ces entreprises qui tendent à manipuler leurs utilisateurs à leur profit<sup>9</sup> soulèvent également des questions d'ordre éthique. Il y a aussi lieu de se méfier d'un pouvoir de surveillance étatique qui deviendrait trop large.

1 Max Tegmark, *Life 3.0: being human in the age of artificial intelligence* (New York: Knopf, 2017).

2 « Regulating the internet giants: The world's most valuable resource is no longer oil, but data », *The Economist* (6 mai 2017) en ligne : <<https://tinyurl.com/y39u52kk>> [« Regulating the internet giants », *The Economist* (2017)]; « Digital plurality - Economics: Are data more like gold or like sunlight? », *The Economist* (22 fév 2020) Gale OneFile.

3 Pierre Trudel, « La valeur de nos données de santé », *Le Devoir* (25 août 2020) en ligne : <<https://tinyurl.com/y93vlnmb>> [Trudel, « La valeur de nos données de santé »]; « Fuel of the future; The data economy », *The Economist* (6 May 2017) Gale OneFile.

4 Voir par exemple: Ziad Obermeyer et Emanuel J. Ezekiel, « Predicting the Future - Big Data, Machine Learning, and Clinical Medicine », (2016) 375 *The New England journal of medicine* 13 à 1216.

5 Voir par exemple: Thomas F. Gordon, *The pleadings game: An artificial intelligence model of procedural justice* (Springer Science & Business Media, 2013); Thorne L. McCarty, « Reflections on TAXMAN: An experiment in artificial intelligence and legal reasoning », (1976) 90 *Harv L Rev* 837; « Assessing Contract Terms, Including Force Majeure, Using AI », *McCarthy-Tétrault*, en ligne : <<https://tinyurl.com/yamf3vmh>>.

6 Voir par exemple : Ying Chen, JD Elenee Argentinis et Griff Weber, « IBM Watson: how cognitive computing can be applied to big data challenges in life sciences research », (2016) 38 *Clinical therapeutics* 4.

7 « Free the data serfs! Schumpeter », *The Economist* (24 oct 2020) Gale OneFile.

8 « U.S. government, states launch antitrust lawsuits against Facebook », *CBC.ca* (9 déc 2020) en ligne : <<https://tinyurl.com/yao9wmup>> ; « Facebook, Google to Face New Antitrust Suits in U.S. », *The Wall Street Journal* (30 nov 2020) en ligne : <<https://tinyurl.com/y9oh9rw2>> ; « Regulating the internet giants », *The Economist* (2017), *supra* note 2.

9 Voir par exemple: Adam D. I. Kramer, Jamie E. Guillory, Jeffrey T. Hancock, « Emotional contagion through social networks », (2014) 111 *Proceedings of the National Academy of Sciences* 24 ; Vindu Goel, « Facebook tinkers with users' emotions in news feed experiment stirring outcry », *The New York Times* (29 juin 2014) en ligne : <<https://tinyurl.com/zq9jk7k>> ; Jack M. Balkin, « The Fiduciary Model of Privacy » (2020) 134 *Harv L Rev Forum* 1, à la p 7 [Balkin, « The Fiduciary Model of Privacy »].

Pris ensemble, ce contexte ainsi que les nombreux scandales impliquant des atteintes à la protection des données personnelles (ex. Equifax, Sidewalk Labs, Cambridge Analytica, et les affaires récentes liées à Desjardins<sup>10</sup> ou à Capital One,<sup>11</sup> etc.) ont donné lieu à une importante érosion de la confiance du public au courant des dernières années.

Ainsi, il y a actuellement un effort en cours pour trouver des solutions qui sauront mieux encadrer ces nouvelles technologies et protéger les intérêts individuelles et collectifs, sans toutefois nuire à l'essor de leur plein potentiel.

La fiducie de données fut identifiée comme une telle solution. Prônée pour sa versatilité et sa flexibilité, elle est présentée comme un outil qui permettrait de trouver un juste milieu entre innovation et protection des intérêts individuels dans le cadre d'une stratégie de gouvernance responsable des données. Plusieurs sont ainsi à étudier son applicabilité dans différents secteurs et différentes juridictions, et elle est aussi l'objet de la présente étude. Spécifiquement, nous nous intéressons à savoir si une fiducie de données pourrait être établie au Québec pour la gestion des données dans le domaine de la santé.

Étant donné que ce domaine représente des enjeux et intérêts particuliers au niveau de la gestion des données, elle propose dans un premier temps de revoir en quoi consiste la gouvernance de données afin de définir comment celle-ci devrait s'opérer dans le domaine de la santé. La première partie prendra donc en revue la notion de gouvernance des données en général ainsi que les principales approches à celle-ci. La deuxième partie entreprendra ensuite une étude détaillée de la fiducie de données afin de déterminer son applicabilité dans le domaine de la santé au Québec. Une revue de la littérature identifiera les principaux indicateurs et principes directeurs qui devront dicter la constitution d'une telle fiducie. Elle identifiera aussi les principaux obstacles et défis à sa constitution. Une analyse détaillée du droit des fiducies du Québec sera enfin effectuée afin de déterminer si le régime québécois peut répondre aux critères identifiés.

Comme nous le verrons bien, un des principaux attraits de la fiducie de données s'agit de la versatilité du véhicule. Elle se prête à plusieurs fins et peut être établie dans différents domaines pour nombre de différents objectifs. En effet, c'est sa finalité – soit son affectation principale – qui déterminera en grande partie la structure de gouvernance qu'elle revêtra. Pour cette raison, la revue de la littérature sur la gouvernance des données dans le domaine de la santé aidera à mieux cerner quelle devrait être cette finalité ainsi que les principaux objectifs d'une fiducie de données dans ce domaine.

10 « Fuite de données chez Desjardins : témoigne d'un acheteur de listes », *Radio-Canada* (9 oct 2020) en ligne : <<https://tinyurl.com/ybyonhln>> ; « Vol massif de données personnelles chez Desjardins », *Radio-Canada* (20 mai 2019) en ligne : <<https://tinyurl.com/y93u4hpx>>.

11 « Capital One : des données personnelles de 6 millions de Canadiens ont été volées », *Radio-Canada* (29 juil 2019) en ligne : <<https://tinyurl.com/ycgqmyvc>>.



# PARTIE I : LA NOTION DE GOUVERNANCE DES DONNÉES

## I. Des solutions équilibrées pour une meilleure gouvernance des données

### A. En quoi consiste la gouvernance des données ?

La gouvernance des données s'agit essentiellement de l'activité d'élaborer, d'établir et de surveiller les stratégies, politiques et décisions prises à l'égard des données constituant un actif au sein d'un milieu donné.<sup>12</sup> Elle inclut l'ensemble des pratiques liées aux processus, règles, normes, procédures et responsabilités à l'égard de la gestion des données ; c'est le cadre mis en place pour assurer que les données soient utilisées de manière efficiente et efficace dans l'atteinte des objectifs de l'entité détentrice.<sup>13</sup>

Défini comme tel, on constate que la gouvernance des données n'a pas nécessairement une orientation d'intérêt public, ni exigerait-elle la protection des droits et intérêts des personnes fichées. Bien au contraire, elle gravite principalement alentour des objectifs établis par l'entité en question. Si l'intérêt public ou les droits et intérêts des personnes fichées vont à l'encontre de ces objectifs, et rien n'impose que ces premières soient respectées, ce seront les objectifs établis qui auront préséance.

C'est précisément ce même problème qui est devenu apparent au cours des dernières années : des cadres réglementaires majoritairement mal adaptés à la nouvelle réalité numérique ont facilité la priorisation d'intérêts privés au détriment des intérêts individuels et collectifs. Et c'est pour cette raison qu'il y a actuellement un effort en cours pour trouver des meilleures approches à la gouvernance des données. La prochaine section présentera sommairement les principales approches sous considération.

12 Commission Européenne, Data governance and data policies at the European Commission, Secrétariat Général de la Commission Européenne, juillet 2020, à la p 6.

13 Ibid. Voir aussi: John Ladley, Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program, 2e éd (London: Elsevier Academic Press, 2019) aux pp 27, 44-45 ; Pinsent Masons, Chris Reed (Queen Mary University of London) et BPE Solicitors, Data trusts: Legal and governance considerations (London: Open Data Institute, 2019) à la p 11 [Pinsent Masons et al. « Data trusts»]; Vijay Khatri et Carol V Brown, « Designing data governance » (2010) 53 Commun ACM 1; Kristin Weber, Boris Otto, et Hubert Österle, « One Size Does Not Fit All: A Contingency Approach to Data Governance » (2009) 1:1 J Data and Information Quality 4.

## B. Quelles approches sont envisageables pour une meilleure gouvernance des données ?

### 1. Renforcer le cadre réglementaire

La plupart sont d'accords que la présente approche axée sur le consentement est inadéquate.<sup>14</sup> En effet, le présent cadre réglementaire date d'environ quarante ans et ne reflète plus la réalité numérique d'aujourd'hui<sup>15</sup>; réalité où les individus sont perpétuellement branchés et en quasi-constante interaction avec l'internet des objets. Dans ce monde de *cookies*, géolocalisation, villes intelligentes, etc., il est illusoire de croire que le consentement spécifique de chaque individu pourra être obtenu pour *chacune* de ces interactions. En effet, tel que noté par le professeur Pierre Trudel, le flux des données ne s'agit plus d'un simple rapport entre information et individu mais s'opère plutôt à une échelle beaucoup plus grande, qui échappe souvent à la compréhension de l'individu lui-même.<sup>16</sup> Dans la majorité des cas, l'individu n'aura pas la capacité de déterminer si une politique quelconque de collecte et d'utilisation de renseignements personnels respecte de manière équitable ses préférences à cet égard, s'il prend même le temps de la lire.<sup>17</sup> Il n'a aussi généralement aucun pouvoir de négociation par rapport à ces politiques.<sup>18</sup> Tel que le remarque Teresa Scassa : « *clicking 'I agree' without reading [or understanding] privacy policies is an act of surrender, not of consent* ». <sup>19</sup> Effectivement, il est illusoire de prétendre que dans de tels cas, les individus ont réellement un choix. Soit qu'ils ne prendront pas le temps de lire la politique, soit qu'ils ne pourront la comprendre (ex. est-ce qu'une personne ordinaire saura juger des mérites d'un système de sécurité pour les données ?), ou encore ne comprendront-ils le véritable étendu de leur consentement (i.e. toutes les fins auxquelles leurs données pourront être mises à profit).

Quelle autre approche pourrait alors être envisagée ?

Certains sont d'avis qu'une approche de réglementation d'anticipation est à prioriser.<sup>20</sup> Selon Element AI et Nesta, une telle approche serait plus adaptée à la rapidité de l'évolution des nouvelles technologies que la présente approche réactive.<sup>21</sup> Trois critères fondamentaux sont proposés par ces derniers pour l'élaboration d'une telle approche :

La réglementation doit être inclusive et collaborative : les gens dont les intérêts sont compromis par les enjeux de gouvernance doivent être mobilisés dans l'élaboration de la réglementation.

La réglementation doit être orientée vers l'avenir : c'est-à-dire, elle doit tenir compte du fait que de nouvelles variables pourraient être introduites dans le modèle de gouvernance mis à l'essai et devrait ainsi être suffisamment flexible pour pouvoir s'y adapter.

La réglementation ne doit pas nuire à l'innovation.<sup>22</sup>

14 Element AI et Nesta, « Fiducies de données: Un nouvel outil pour la gouvernance des données » (2019) à la p 13, 30 [Element AI et Nesta, « Fiducies de données »]; Sean McDonald, « Reclaiming Data Trusts », Centre for International Governance Innovation (15 mars 2019) en ligne : <<https://tinyurl.com/y857b2bc>> [McDonald, « Reclaiming Data Trusts »]; Neil M. Richards et Woodrow Hartzog, « A Duty of Loyalty for Privacy Law » (2020); « La protection des données personnelles au Canada à l'ère des données massives », Laboratoire de Cyberjustice (24 juil 2018) en ligne : <<https://tinyurl.com/yd9mp6a3/>> [Cyberjustice, « La protection des données personnelles »].

15 Cyberjustice, « La protection des données personnelles », supra note 14.

16 Trudel, « La valeur de nos données de santé », supra note 3 ; voir aussi Anouk Ruhaak, « Data trusts : What, Why and How », Medium (11 nov 2018) en ligne : <<https://tinyurl.com/y9ypp26k>>.

17 La plupart des politiques de confidentialité sont trop longs et trop complexes pour être comprises par une grande majorité d'individus. Par exemple, seulement 1% de telles politiques d'entreprises figurant au classement Fortune 500 ont été jugées compréhensibles pour les personnes ayant un niveau d'éducation secondaire (Element AI et Nesta, « Fiducies de données », supra note 14 à la p 9).

18 Element AI et Nesta, « Fiducies de données », supra note 14 à la p 9 ; Sean McDonald et Bianca Wylie, « What is a data trust? », Centre for International Governance Innovation (9 oct 2018) en ligne : <<https://tinyurl.com/y7xznz7f>> [McDonald & Wylie, « What is a data trust? »].

19 McDonald & Wylie, « What is a data trust? », supra note 18.

20 Element AI et Nesta, « Fiducies de données », supra note 14 aux pp 11-12.

21 Ibid aux pp 10-11.

22 Ibid aux pp 11-12.

À titre d'exemple, seraient conformes à une telle approche: une réglementation encadrant les fins auxquelles les données peuvent être mises à l'emploi, ou une réglementation qui interdit tout court le consentement à la collecte des données dans des cas définis ou les cas contraires à l'intérêt public.<sup>23</sup>

D'autres aimeraient aussi voir un principe de responsabilité civile *efficace* intégré dans quelconque nouveau cadre réglementaire, qui revêtira un véritable caractère dissuasif.<sup>24</sup> Par exemple, la possibilité d'imposer des sanctions administratives significatives<sup>25</sup>, ou la mise sur pied d'entités de surveillance indépendantes et externes.<sup>26</sup> L'idée étant d'inciter les entités détentrices de données à s'auto-réguler afin d'éviter d'encourir des sanctions découlant d'une gestion inadéquate ou irresponsable des données.

D'autres encore soulèvent la désidentification, la pseudonymisation ou l'anonymisation à titre de techniques qui pourraient être imposées pour mieux protéger les intérêts des personnes fichées.<sup>27</sup> Bien qu'intéressantes, il y a toujours le risque de réidentification à garder en tête lorsque l'on considère de telles approches. Elles pourraient également engendrer des difficultés à l'analyse des jeux de données lorsque, par exemple, le couplage des données s'avérerait utile.<sup>28</sup>

À la lumière de ceci, il semble évident qu'une réforme législative s'impose à plusieurs niveaux. Plusieurs initiatives dans ce sens sont d'ailleurs en cours ou déjà achevées ; par exemple, le nouveau Règlement général sur la protection des données de l'Union européenne, en vigueur depuis le 25 mai 2018, et le Projet de loi n° 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, qui est présentement sous étude détaillée en commission à l'Assemblée nationale du Québec et qui englobe plusieurs des recommandations ci-haut mentionnés. Ce sont de bonnes nouvelles, mais le problème reste néanmoins contemporain malgré le processus législatif qui peut être lent et est aussi souvent imparfait. Ainsi, des solutions plus ponctuelles s'imposent toujours.

23 Ibid à la p 7 ; voir aussi Cyberjustice, « La protection des données personnelles », supra note 14, citant les recommandations de la Commission d'accès à l'information dans son rapport quinquennal de 2016 qui vont dans le même sens. D'ailleurs, c'est l'approche que semble avoir entreprise le Projet de loi n° 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, 1<sup>re</sup> session, 42<sup>e</sup> législature, Québec, 2020 [PL-64] qui, si adopté, permettra la communication de renseignements personnels pour les seules fins prescrites par la loi. Par exemple, pour la recherche, l'étude ou la production de statistiques (aux art 19, 23, 102 et 110).

24 The British Academy, The Royal Society et TechUK, « Data ownership, rights and controls : Reaching a common understanding. Discussions at a British Academy, Royal Society and techUK seminar on 3 October 2018 », à la p 7 ; Gouvernement du Canada, « La Charte numérique du Canada en action : un plan par des Canadiens, pour les Canadiens », Innovation, Science and Economic Development Canada (2019) aux pp 10, 18 ; The Academy of Medical Sciences, « Our data-driven future in healthcare : People and partnerships at the heart of health related technologies » (2018) à la p 5.

25 Cyberjustice, « La protection des données personnelles », supra note 14.

26 Sean McDonald, « Data Review Boards », The Medium (20 mar 2018) en ligne: <<https://tinyurl.com/y9r7e9uo>>.

27 Pinsent Masons et al. « Data trusts », supra note 13 aux pp 9-10.

28 Ibid.

## Quelles autres approches pourraient alors être envisagées ?

### 2. Redonner plus de contrôle aux individus en leur reconnaissant la patrimonialité sur leurs données personnelles

D'autres prônent plutôt une approche qui reconnaîtrait aux individus un titre de propriété sur leurs données personnelles, notamment pour s'attaquer au déséquilibre de pouvoir qui existe entre eux et ceux qui exploitent leurs données. Détenir ses données à titre patrimonial, dit-on, les permettrait d'exercer un meilleur contrôle sur l'utilisation de leurs données en fonctions de leurs intérêts et préférences.<sup>29</sup> L'emploi de la technologie *blockchain*,<sup>30</sup> ou encore la mise sur pied de coopératives de données<sup>31</sup> s'inscrivent dans une telle approche.<sup>32</sup>

Cette approche est toutefois fortement critiquée pour plusieurs raisons.

- Premièrement, pour sa ressemblance à l'approche axée sur le consentement, certains avancent qu'elle ne s'attaquerait pas aux problèmes d'analphabétisme numérique et de complexité qui posent problème à la capacité même des individus de donner un consentement libre et éclairé. En effet, selon la professeure Pamela Samuelson, un des principaux attributs de la propriété – soit l'aliénabilité du titre – aurait plutôt tendance à empirer ces problèmes puisqu'une fois aliéné, l'individu aurait encore moins de contrôle sur ce qui pourrait être fait de ses données, les acquéreurs ayant essentiellement carte blanche de les employer à leur guise une fois le titre transféré.<sup>33</sup>
- Deuxièmement, d'autres encore soulèvent les enjeux éthiques et juridiques en lien avec une reconnaissance patrimoniale des données personnelles.<sup>34</sup> Est principalement en cause ici la marchandisation des données personnelles et le potentiel d'exploitation des personnes vulnérables qui en résulterait. En effet, bien qu'une telle approche semblerait pouvoir répondre à une demande grandissante pour les données, et qu'elle permettrait aussi de remettre l'individu plus au centre du locus de contrôle sur ses données (en lui permettant, par exemple, de choisir à qui vendre ses données, sous quelles conditions, et de recevoir aussi une contrepartie directe à titre de rémunération pour l'aliénation de son titre), elle risque aussi de créer nombre d'effets pervers, tels l'exploitation des personnes vulnérables, ou la sur-représentation de certaines populations ou certains groupes de personnes dans les jeux de données.

29 Voir par exemple Paul M. Schwartz, « Property, Privacy, and Personal Data », (2004) 117 Harv L Rev 7 (Schwartz avance l'idée de la mise sur pied d'un marché pour les données personnelles) ; voir aussi Michele Loi, Paul-Olivier Dehaye et Ernst Hafen, « Towards Rawlsian 'property-owning democracy' through personal data platform cooperatives », (2020) Critical Review of International Social and Political Philosophy (discute de l'idée de coopératives de données gérées collectivement par les individus eux-mêmes ; cette approche s'apparente notamment à l'idée des « bottom-up trusts » proposée par Sylvie Delacroix et Neil D Lawrence, « Bottom-up data Trusts: disturbing the 'one-size-fits-all' approach to data governance », (2019) 9 International Data Privacy Law 4 [Delacroix & Lawrence, « Bottom-up data Trusts »]). Voir aussi : « Il faut inventer un droit patrimonial sur ses données de santé » Le Monde (11 janv 2019) en ligne : <<https://tinyurl.com/y7ostfc5>>.

30 Voir par exemple Guy Zyskind, Oz Nathan et Alex S Pentland, « Decentralizing Privacy: Using Blockchain to Protect Personal Data », (2015) IEEE Security and Privacy Workshops.

31 Delacroix & Lawrence, « Bottom-up data Trusts », supra note 29 à la p 242.

32 Element AI et Nesta, « Fiducies de données », supra note 14 à la p 13.

33 Pamela Samuelson, « Privacy as Intellectual Property? », (2000) 52 Stanf L Rev 5.

34 Voir par exemple: Beate Roessler, « Should personal data be a tradable good? On the moral limits of markets in privacy », dans Beate Roessler et Dorota Mokrosinska (eds), Social Dimensions of Privacy : Interdisciplinary perspectives (Cambridge: Cambridge University Press, 2019) aux pp 141-161 et Pamela Samuelson, « Privacy As Intellectual Property? », supra note 33 (pour les principaux enjeux en lien avec la marchandisation des données personnelles) ; Element AI et Nesta, « Fiducies de données », supra note 14 à la p 13 ; voir aussi Jérôme Béranger et Ryad Bouadi, « Approche éthico-juridique de l'usage des données médicales à caractère personnel » (2014) 2 Les Cahiers du numérique 10 [Béranger & Bouadi, « Approche éthico-juridique »]. Pour une vue plus globale sur la marchandisation de certaines choses dites « hors commerce », voir Michael J. Sandel, What money can't buy: the moral limits of markets (New York : Farrar, Straus and Giroux, 2013) et Deborah Satz, Why some things should not be for sale: The moral limits of markets (Oxford : Oxford University Press, 2012).

- Selon une juriste française, un principe de patrimonialité des données personnelles fut juridiquement exclu en France à plusieurs reprises ; les français ne sont tout simplement pas ‘propriétaires’ de leurs données personnelles. Au contraire, le droit français considère plutôt les données personnelles comme des émanations de la personnalité. La personne ne peut donc en aucun cas en disposer librement ni les vendre. Elles sont des choses désignées strictement hors commerce.<sup>35</sup>

Selon cette même auteure, faire autrement reviendrait aussi à reconnaître la personne comme la plus à même à opérer des choix rationnels en fonction de son meilleur intérêt. Or, tel qu’explicité ci-haut, les enjeux en lien avec le consentement à la collecte et l’utilisation des données échappent souvent à l’individu. En effet, tel que noté par Boyer, ce postulat libéral est celui de la législation américaine, qui n’est partagé ni par le droit français, ni par celui de l’Union européenne.<sup>36</sup>

D’autres ont plutôt considéré la question sous l’angle des chercheurs et scientifiques, à savoir s’il serait approprié d’accorder un droit de propriété à ces derniers pour les données non personnelles ou dépersonnalisées qu’ils recueillent dans le cadre de leurs activités. Pour les adhérents du mouvement vers la science ouverte, la réponse doit être non.<sup>37</sup> Pour eux, ces données devraient plutôt être considérées comme un bien public et devraient ainsi demeurer dans le domaine public afin de mieux faire avancer la recherche, la science et la technologie au bénéfice de tous. Permettre qu’elles soient appropriables (par les chercheurs ou autre entité détentrice) irait non seulement à l’encontre de l’intérêt public, mais risque aussi d’avoir des effets pervers sur la recherche. Par exemple, ceci pourrait avoir comme effet de créer des monopoles du savoir détenus par les plus grands détenteurs de données, ou encore des silos de recherches priorisant les intérêts de ceux qui ont la capacité à payer pour les données nécessaires à la recherche, etc. Les domaines du savoir – et surtout la science – pourraient alors être grandement appauvris par le manque de diversité de perspectives faute d’accorder un accès équitable à tous aux données nécessaires à la recherche.

### 3. Les modèles fiduciaires de gouvernance des données

Les modèles fiduciaires de gouvernance des données ont églament suscité beaucoup d’intérêt. Il existe deux principaux tels modèles : le *information fiduciary* (fiduciaire d’information) prôné principalement par les professeurs Jack Balkin et Jonathan Zittrain<sup>38</sup>, et le *data trust* (fiducie de données), similaire au modèle du fiduciaire d’information de Balkin et Zittrain mais avec des différences importantes qui le rendent distinct en soi. Celles-ci seront abordés en détail dans la prochaine section.

Ces modèles tirent leurs origines de la *common law*, notamment du droit des *trust* et de la notion de *fiduciary duty*. On s’y intéresse surtout pour la possibilité qu’ils offrent d’imposer des obligations fiduciaires à un individu ou une entité quelconque qui détient et gère des données personnelles, peu importe le contexte. Que ce soit en milieux de recherche, dans le secteur public ou privé, ces obligations s’imposeraient pour encadrer la gestion des données personnelles et ainsi orienter la gouvernance de ces dernières, et ce, peu importe que les données aient été consenties ou non.

35 Kim Boyer « Qui est le propriétaire des données de ma santé? », *The Conversation*, (7 fév 2018) en ligne : <<https://tinyurl.com/ya5ostg8>>.

36 Ibid.

37 Mark Phillips et Bartha M Knoppers, « Whose Commons? Data Protection as a Legal Limit of Open Science » (2019) 47 *J Law Med Ethics* 1 [Phillips & Knoppers « Whose Commons? »]; Christian Ohmann et al. « Sharing and reuse of individual participant data from clinical trials: principles and recommendations. » (2017) 7 *BMJ open* 12 e018647 [Ohmann et al. « Sharing and reuse of data from clinical trials »].

38 Selon le professeur Jack Balkin (« Information Fiduciaries and the First Amendment », (2016) 49 *UC Davis L Rev* 1183, à la p 1221 [Balkin, « Information Fiduciaries »]), la notion de l’information fiduciary (fiduciaire d’information) aurait fait ses premières apparences dans le début des années 1990s, dans un article publié par le professeur Kenneth Laudon (Kenneth C. Laudon, « Markets and Privacy », (1996) *Communications of the ACM*). Depuis 2014, le modèle est principalement associé aux professeurs Jack Balkin et Jonathan Zittrain (voir Lina Khan and David Pozen, « A skeptical view of information fiduciaries », (2019) *Harv L Rev* 133, à la p 499 [Khan & Pozen, « A skeptical view »]).

Selon le modèle du fiduciaire d'information de Balkin et Zittrain, tout gestionnaire de données serait tenu, du moment qu'il détient des données personnelles, aux obligations fiduciaires de loyauté, de prudence, de confidentialité, et de toujours agir dans le meilleur intérêt de la personne fichée.<sup>39</sup> Il est ainsi puisque ce modèle conçoit les obligations fiduciaires comme *relationnelles* entre les détenteurs de données et les personnes que ces dernières concernent.<sup>40</sup> On dit relationnel parce que la justification de ces obligations se trouve dans la dynamique de pouvoir entre ces parties, où la personne fichée est placée dans une position vulnérable par rapport au détenteur de ses données puisque ce dernier détient des renseignements sensibles et potentiellement préjudiciables à cette personne.<sup>41</sup> Balkin a initialement conçu de ce modèle en faisant une analogie à la dynamique typiquement retrouvée entre le médecin et son patient, ou l'avocat et son client. Selon Balkin, c'est la nature hautement personnelle et sensible de ces relations qui commande le plus haut degré de responsabilité – soit une obligation fiduciaire – de la partie en pouvoir afin de protéger les intérêts de l'individu en question.<sup>42</sup>

L'idée principale de Balkin et Zittrain est de voir cette même obligation s'imposer aux grandes plateformes digitales (ex. Facebook, Amazon, Google, etc.) et tout autre détenteur de données personnelles afin de les reconnaître à titre de 'fiduciaires d'information'. Ainsi, tout comme les médecins ou avocats sont, en *common law*, tenus à des obligations fiduciaires en vertu du seul fait d'exercer leur profession, les détenteurs de données personnelles seraient aussi tenus à de pareilles obligations du seul fait de la nature de leurs activités.<sup>43</sup>

Le modèle du *data trust* est par contre légèrement différent, en ce qu'il n'exigerait pas, du seul fait d'établir un *data trust*, que les administrateurs du *trust* observent des obligations fiduciaires envers les personnes fichées. En effet, dans une fiducie de données, c'est plutôt la *finalité* qui importe ; c'est envers elle que les obligations fiduciaires devront être observées. Par exemple, si une fiducie de données est établie principalement au profit d'une entreprise pour que celle-ci puisse bénéficier des données détenues en fiducie, les obligations fiduciaires s'appliqueraient pour la seule réalisation de cette finalité ainsi que les modalités stipulées dans l'acte constitutif. Si le respect des droits et intérêts des personnes fichées entrave à l'accomplissement de cette finalité, ou ne fait pas partie des modalités stipulées pour son accomplissement, ils seraient obligatoirement mis de côté (hormis ce qui est obligatoire en vertu de la loi), à défaut de quoi les administrateurs seraient en défaut de leurs obligations fiduciaires. Ainsi, le *data trust* se veut un outil plus flexible que le modèle de Balkin et Zittrain puisqu'il est plus amenable à être modelé à quelque fin désirée. Il s'agit d'un véritable outil pouvant être confectionné *sur mesure*.

Le modèle de Balkin et Zittrain semble ainsi plus attrayant si l'objectif, en recherchant des nouvelles approches à la gouvernance des données, est de fournir de meilleures protections aux intérêts individuels et collectifs.

Mais c'est l'idée du *data trust* qui, malgré les attraits du modèle du fiduciaire d'information, a été nettement plus influente dans les discours sur la gouvernance des données.

Voyons en plus de détails en quoi consiste ce modèle à titre d'outil pour la gouvernance des données.

39 Balkin, « Information Fiduciaries », supra note 37.

40 Paul B Miller et Andrew S Gold, « Fiduciary Governance », (2015) 57 William & Mary L Rev 2, aux pp 537-539 [Miller & Gold, « Fiduciary Governance »]. Lina Khan et David Pozen (Lina Khan and David Pozen, « A skeptical view of information fiduciaries », (2019) Harv L Rev 133, aux pp 499, 508-510) ont critiqué l'analogie aux professions libérales soutenant que contrairement à la dynamique de ces dernières qui est strictement *relationnelle*, celle retrouvée entre une plateforme digitale et ses adhérents est plutôt *impersonnelle*, puisqu'elle n'exige pas comme prérequis à l'exécution du mandat de service (i.e. fournir une plateforme digitale d'un réseau social tel Facebook, ou d'un moteur de recherche tel Google) la divulgation de renseignements personnelles. En revanche, la divulgation de tels renseignements est une condition nécessaire au service du médecin ou de l'avocat puisqu'autrement, ils ne sauraient servir leur patient / client. La nature fondamentalement différente de ces relations soulève, pour Khan et Pozen, d'importantes questions se rapportant à la responsabilité éventuelle d'un tel fiduciaire. En revanche, Miller et Gold (Paul B Miller et Andrew S Gold, « Fiduciary Governance », (2015) 57 William & Mary L Rev 2, aux pp 537-539) remarquent à juste titre que les obligations fiduciaires apparaissent non seulement dans les mandats d'expertise professionnel – qu'ils qualifient de type 'service-relationnel' – mais aussi dans des mandats de type 'gouvernance-institutionnel'. Selon ces auteurs, alors que les fiduciaires des professions libérales sont plutôt des mandats de type *service-relationnel*, l'on retrouve tout aussi souvent des mandats de type *gouvernance-institutionnel* dans des contextes qui, justement, vont au-delà d'une dynamique strictement relationnelle ; par exemple, le devoir fiduciaire imposé aux administrateurs d'une entreprise. Celui-ci exige généralement que les administrateurs exercent leur pouvoir avec compétence, diligence, intégrité et bonne foi, au mieux des intérêts de l'entreprise (par exemple: *Loi canadienne sur les sociétés par actions*, LRC 1985, c C-44, par 122(1)(a)). L'obligation fiduciaire dans ces cas est donc, pour Miller et Gold, *institutionnelle* et non relationnelle (aux pp 544, 548, 552). Ces auteurs ne voient donc aucun obstacle à considérer les plateformes digitales en tant que fiduciaires d'information selon le modèle de Balkin et Zittrain.

41 Balkin, « The Fiduciary Model of Privacy », supra note 9 aux pp 3, 15.

42 Balkin, « Information Fiduciaries », supra note 37.

43 Ibid.

## PARTIE II : LA FIDUCIE DE DONNÉES COMME OUTIL DE GOUVERNANCE DES DONNÉES DANS LE DOMAINE DE LA SANTÉ

### I. Le *Data Trust* ou la « fiducie de données » : sujet de la présente étude

#### A. Genèse de l'idée du data trust et bref introduction de la fiducie légale

L'idée du *data trust* semble avoir fait ses premières apparences vers le début 21<sup>e</sup> siècle, dans des articles publiés en 2003<sup>44</sup> et en 2004<sup>45</sup>, mais c'est surtout depuis 2017 qu'elle a gagné la majorité de ses adeptes. En effet, dans son rapport « *Growing the artificial intelligence industry in the UK* »<sup>46</sup>, le gouvernement du Royaume-Uni positionne la fiducie de données à titre de solution à prioriser pour sa stratégie d'investissement dans l'intelligence artificielle. La littérature scientifique et grise à son sujet abonde depuis ce temps. Il y a aussi un intérêt marqué de la part du grand public, incluant celui du Québec<sup>47</sup> ; soulignons qu'elle fut aussi endossée par le gouvernement du Canada en 2019 dans sa proposition pour moderniser la *Loi sur la protection des renseignements personnels et des documents électroniques*.<sup>48</sup>

Traditionnellement, une fiducie s'agit d'un outil juridique de droit privé pour la gestion et l'administration indépendante d'un patrimoine quelconque, orienté vers une fin définie, celle-ci étant souvent le meilleur intérêt d'une personne en particulier que l'on appelle « bénéficiaire ». Elle est définie formellement comme un « acte juridique par lequel une personne, appelée constituant (« *settlor* »), dans un acte constitutif qui représente sa volonté, transfère à titre onéreux ou gratuit et pour une fin particulière des biens qui lui appartiennent à un patrimoine qu'elle forme et qu'une autre personne, appelée fiduciaire (« *trustee* »), s'engage à détenir et à administrer pour le bénéfice d'un tiers, appelé bénéficiaire (« *beneficiary* »).<sup>49</sup>

44 David E Winickoff et Richard N Winickoff, « The charitable trust as a model for genomic biobanks », (2003) 349 *The New England journal of medicine* 12 (ces auteurs proposaient le trust de la common law pour la gestion d'échantillons déposés en biobanques).

45 Lilian Edwards, « The Problem with Privacy », (2004) 18 *International Review of Law Computers & Technology* 3.

46 Dame Wendy Hall et Jérôme Pesenti, « Growing the artificial intelligence industry in the UK », (Gouvernement du Royaume-Uni, 2017).

47 Voir par exemple : Alex Ryan « Here's how the Quayside data trust should operate », *The Toronto Star*, (24 juin 2019) en ligne : <<https://www.thesstar.com/opinion/contributors/2019/06/24/heres-how-the-quayside-data-trust-should-operate.html>> ; City of Guelph, « Canadian experts guide local data trust pilot » (10 déc 2020) en ligne : <<https://guelph.ca/2020/12/canadian-experts-guide-local-data-trust-pilot/>> ; Anne-Sophie Hulin et Antoine Cossé, « Pour une fiducie de données à la RAMQ », *Le Devoir*, (1 sept 2020) en ligne : <<https://www.ledevoir.com/opinion/idees/585113/pour-une-fiducie-de-donnees-a-la-ramq>>.

48 Gouvernement du Canada, « Renforcer la protection de la vie privée dans l'ère numérique », Innovation, Sciences et Développement économique Canada (21 mai 2019) en ligne : <[https://www.ic.gc.ca/eic/site/062.nsf/fra/h\\_00107.html](https://www.ic.gc.ca/eic/site/062.nsf/fra/h_00107.html)>.

49 Dictionnaire de droit québécois et canadien, 5<sup>e</sup> éd, sub verbo « fiduciaire ».



Le fiduciaire qui s'engage à administrer une fiducie est donc accordé certains pouvoirs pour l'exécution de son mandat, et il est aussi soumis à de nombreuses obligations fiduciaires tel des devoirs de prudence, diligence, loyauté et honnêteté, et de toujours agir dans le meilleur intérêt du bénéficiaire ou de la finalité établie.

## B. Raisons pour lesquelles la fiducie de données suscite intérêt à titre d'outil pour la gouvernance des données

Tel qu'explicité ci-haut, la fiducie de données fut identifiée comme un outil pouvant aider à pallier l'érosion de la confiance du public dans le nouvel environnement numérique en servant à titre d'outil pouvant fournir une meilleure protection des intérêts individuels et collectifs dans la gestion des renseignements personnels et sensibles.

Elle est réévaluée surtout pour sa versatilité et sa capacité à adopter une structure de gouvernance *sur mesure*, tout en intégrant les obligations juridiques qui s'imposent typiquement aux fiduciaires ainsi que des mécanismes de responsabilités claires et bien définies.

Modélisée à partir du *trust* de la *common law*, elle comporte, telle que décrite par ses partisans, toutes les vertus classiques d'une fiducie légale :

- La liberté d'établir une finalité au gré du constituant (la fiducie revêtera différentes formes selon sa finalité établie ; par exemple, la fiducie testamentaire est établie pour administrer un legs au profit d'un héritier, un fonds d'investissement administre un patrimoine au profit des bénéficiaires désignés, une fiducie environnementale administre un territoire foncier principalement dans un but de conservation de sa valeur écologique, etc.) ;
- La liberté d'établir un cadre de gouvernance sur mesure qui découle de la finalité établie (ex. avec un seul ou plusieurs fiduciaires ayant un pouvoir concentré ou diffus, avec responsabilité centralisée ou partagée, avec une structure hiérarchique ou plutôt démocratique, en définissant aussi comment le patrimoine devra être administré et pour quelles fins, etc.)
- Toutes les obligations qui s'imposent typiquement à l'administrateur fiduciaire, soit, les obligations de loyauté et d'honnêteté envers la finalité établie et les devoirs de prudence et de diligence dans l'exécution du mandat d'administration fiduciaire ;
- Un principe de gouvernance responsable rendant le ou les administrateur(s) de la fiducie redevable(s) pour une administration défailante ou irresponsable.<sup>50</sup>

Le gouvernement du Royaume-Uni, dans son rapport de 2017 sur l'IA, a reconnu la fiducie comme outil pouvant assurer une gouvernance des données juste, sécuritaire et équitable.<sup>51</sup> Bien que ceci soit peut-être vrai, il importe de souligner qu'il ne s'agit que d'un résultat possible parmi d'autres. En fait, la fiducie *peut* servir à titre d'outil pour une 'meilleure' gouvernance des données, mais c'est la finalité qui sera déterminante de la façon dont les renseignements seront ultimement gérés. Sa versatilité se veut donc en ce sens aussi un talon d'Achille : rien ne garanti qu'une fiducie *en soi* fournisse une meilleure protection des données et des intérêts individuels et collectifs qui s'y rattachent. Il serait tout aussi possible, par exemple, qu'elle soit établie pour gérer des données (personnelles ou autres) au profit d'une entreprise, sans égard particulier aux intérêts des personnes fichées autre que les obligations qu'impose la loi. Dans un tel cas, les obligations fiduciaires s'appliqueraient donc envers la réalisation de *cette affectation particulière* – soit la gestion des données au profit de l'entreprise désignée.

50 Element AI et Nesta, « Fiducies de données », supra note 14 à la p 14 ; Sean McDonald, « The Fiduciary Supply Chain » dans Centre for International Governance Innovation, « Models for Platform Governance, Data Governance in the Digital Age: A CIGI Essay Series » (2019), à la p 59 [McDonald, « The Fiduciary Supply Chain »].

51 Tel que rapporté par Element AI et Nesta, « Fiducies de données », supra note 14 à la p 17.



C'est pour cette raison que plusieurs ont de la difficulté à définir ce qu'est une 'fiducie de donnée'. Il est généralement compris qu'elle impliquera toutes les caractéristiques typiques d'une administration fiduciaire. Il est aussi compris que sa finalité principale (son 'quoi') s'agira de l'administration d'un patrimoine composé de données. Mais tel qu'expliqué, rien n'est plus certain quand il s'agit de définir son 'pourquoi': administre-t-elle des données pour mieux protéger les intérêts des individus en question ? Ou pour mieux profiter une entreprise ou une autre entité qui pourra s'en servir à des fins commerciales ou autres ? C'est ainsi que la finalité de la fiducie est d'une importance première quand il s'agit de définir ce à quoi elle servira.

C'est aussi pour cette raison que la manière dont elle est définie dans la littérature varie autant. Par exemple :

Certains la conçoivent comme étant établie pour mieux protéger les intérêts des personnes fichées :

- A set of relationships underpinned by a repeatable framework, compliant with parties' obligations, to share data *in a fair, safe and equitable way*, but not necessarily a legal entity or institution.<sup>52</sup>
- A repeatable mechanism or approach to sharing data *in a timely, fair, safe and equitable way*, which does not preclude the data trust taking the form of a legal trust or independent institution.<sup>53</sup>

Alors que d'autres y voient une affectation plus large :

- A legal structure that provides independent stewardship of data<sup>54</sup> (*une structure juridique fournissant des services tiers indépendants de gestion des données*).<sup>55</sup>
- An independent third party with a fiduciary obligation to manage the data according to a well-defined charter.<sup>56</sup>

La conception plus large laisse ouvert la possibilité que le « *well-defined charter* » soit établi dans un intérêt purement privé, sans égard aux intérêts des personnes fichées. La conception plus étroite est par contre implicite quant à la nécessité de prendre en compte les intérêts de toutes les parties concernées. C'est seulement ainsi qu'elle pourrait prétendre être « juste, sécuritaire et équitable ».

Dans tous les cas par contre, la fiducie de données - étant, par définition, une *fiducie* - impliquera nécessairement la conservation et une administration fiduciaire *indépendante*<sup>57</sup> d'un patrimoine composé de données<sup>58</sup>, l'administration fiduciaire étant « *the highest level of obligation that one party can owe to another, [characterized by the highest] degree of impartiality, prudence, transparency and undivided loyalty* »<sup>59</sup>. En effet, selon Jack Hardinges du Open Data Institute (ODI), « data trusts don't aim to enable easier access to data; on the contrary, they offer a solution for providing better controls around how data is accessed, shared and communicated »<sup>60</sup>. Il s'agit simplement de déterminer *dans l'intérêt de qui*.

52 Jeremiah Lau, James Penner et Benjamin Wong, « The Basics of Private and Public Data Trusts », (2020) 2020 Sing J Legal Studies 90 à la p 91 [Lau, Penner & Wong, « Data trust basics »].

53 Alison Paprica et al., « Essential requirements for establishing and operating data trusts : practical guidance co-developed by representatives from fifteen canadian organizations and initiatives », (2020) 5:1 International Journal of Population Data Science 31 à la p 2 [Paprica et al. « Essential requirements for establishing and operating data trusts »].

54 Pinsent Masons et al. « Data trusts », supra note 12 à la p 42.

55 Element AI et Nesta, « Fiducies de données », supra note 14 aux pp 17-18.

56 Philip Dawson, « COVID-19 tracking data should be managed the way data trusts are », Policy Options (20 avr 2020) en ligne : <<https://policyoptions.irpp.org/magazines/april-2020/covid-19-tracking-data-should-be-managed-the-way-data-trusts-are/>>.

57 Selon le ODI, la gouvernance des données (le « *data stewardship* ») s'agit de l'acte de collecter, colliger, et de partager des données, particulièrement en déterminant qui pourra y avoir accès, sous quelles conditions, et au bénéfice de qui. Pour eux, confier la gestion des données à un fiduciaire impliquera *nécessairement* une délégation de pouvoirs au fiduciaire de sorte qu'il pourra effectuer sa gestion de manière *indépendante*. Ainsi le *data stewardship* pour l'ODI signifie une délégation complète des pouvoirs de *contrôle* sur les données à un fiduciaire *indépendant* (Jack Hardinges, « Data Trusts in 2020 », The Open Data Institute (17 mar 2020) en ligne : <<https://theodi.org/article/data-trusts-in-2020/>> [Hardinges, « Data Trusts in 2020 »].

58 « [A] legal structure that provides independent fiduciary stewardship of data » (ibid).

59 Ibid.

60 Ibid.

### C. La notion de *stewardship* comme centrale à l'idée d'une fiducie de données et une gouvernance *responsable* des données

La notion de *stewardship* fut aussi centrale au développement du concept du *data trust*. Une meilleure compréhension de ce terme aidera ainsi à mieux cerner la nature d'une fiducie de données.

En effet, pour désigner la « gouvernance des données », la littérature anglophone emploie presque exclusivement le terme « *data stewardship* ». Selon le ODI, le *data stewardship* s'agit de l'acte de collecter, colliger, et de partager des données, particulièrement en déterminant qui pourra y avoir accès, sous quelles conditions, et au bénéfice de qui.

Le *stewardship* a toutefois une signification particulière se rattachant majoritairement à son usage dans les discours environnementaux pour désigner la gouvernance et la gestion d'une ressource naturelle (ex. un territoire foncier, un bassin d'eau, etc.). Selon Enqvist et al. (2018), la signification du terme est multidimensionnelle. Elle se situe, selon ces auteurs, au nexus entre les notions de prudence (*care*), savoir-faire (*knowledge* et *expertise*), et pouvoir d'agir (*agency* ou *autonomie d'action*).<sup>61</sup> Chacune de ces notions constitue une dimension en soi avec des significations propres à chacun; la Figure 1 illustre bien l'interaction entre celles-ci :

**Figure 1.** Cadre conceptuel illustrant la signification multidimensionnelle du terme «*stewardship*» observée par Enqvist et al. (2018) dans leur revue de la littérature scientifique sur l'emploi de ce terme.<sup>62</sup>



Ainsi, en étudiant cette signification de plus près, la définition suivante du terme *stewardship* pourrait être retenue :

- L'action d'exercer volontairement et intentionnellement un pouvoir d'agir ou de s'animer envers une fin quelconque, avec soin/prudence/diligence, et selon des valeurs et une éthique définie en application d'un savoir-faire ou d'une expertise pertinente à l'activité ou le but en cause.

61 Enqvist et al., « Stewardship as a boundary object for sustainability research : Linking care, knowledge and agency » (2018) 179 *Landscape and Urban Planning*, à la p 24.

62 Dans Enqvist et al, *ibid*, à la p 24.

Compris comme tel, l'on comprend davantage pourquoi la fiducie fut identifiée comme un outil intéressant pour la gouvernance des données : les obligations qui s'imposent typiquement au fiduciaire implique nécessairement un mandat qui devra être effectué avec soin, prudence et diligence, et correspond ainsi très bien à la signification multidimensionnelle du terme *stewardship*.

Mais cela ne dit toujours rien à propos de ce que devrait être la *finalité* d'une fiducie de données. Les notions de *stewardship* ou de *gouvernance fiduciaire* illustrent bien le *comment* mais ils ne disent rien à propos du *pourquoi* d'une fiducie de données. L'administrateur devra-t-il être prudent et diligent dans l'exécution de son mandat pour le bénéfice d'une entreprise désignée à titre de bénéficiaire ? Ou pour celle du public en général ? Devra-t-il tenir compte des intérêts d'un groupe de personnes en particuliers ? Devra-t-il se soucier, par exemple, de la protection de la vie privée des personnes fichées ? C'est ainsi que la finalité d'une fiducie de données prend toute son importance. C'est elle qui dictera l'orientation du mandat du fiduciaire et qui permettra d'évaluer la qualité de son exécution. La versatilité du véhicule fait qu'elle pourra varier au cas-par-cas selon l'intention du constituant ; il sera donc d'importance première qu'elle soit clairement définie. Par exemple, si le constituant veut constituer une fiducie pour assurer une meilleure protection des droits et intérêts des personnes fichées dans la gestion des données répertoriées, ceci devra être clairement établi comme un des objectifs de la fiducie. Autrement, rien ne garanti qu'une fiducie *en soi* visera un tel objectif. Elle pourrait, par exemple, être constituée simplement pour 'faciliter le partage des données à des fins de recherches d'intérêt public'. Le fiduciaire serait alors tenu de réaliser cette seule fin, sans nécessairement devoir tenir compte des droits et intérêts des personnes fichées autre que ce qu'exige la loi. Sa mission première est toujours de réaliser la finalité de la fiducie du mieux possible.

C'est pour cette raison que plusieurs disent que la fiducie de données ne représente qu'une solution temporaire dans l'attente que les cadres réglementaires se développent.<sup>63</sup> Elle pourra faciliter une meilleure protection des droits et intérêts des personnes fichées tant que le constituant ait ceci comme intention, mais ultimement ce seront ces derniers qui pourront l'assurer de manière plus concrète. Néanmoins, même alors que les cadres réglementaires seront finalisés, la fiducie de données pourra aussi toujours servir à titre complémentaire, pour bonifier, par exemple, une réglementation jugée insuffisante.<sup>64</sup>

La fiducie de données ne représente donc pas une panacée. Elle ne sera qu'un seul morceau du casse-tête qui devra composer l'ensemble d'une stratégie de gouvernance des données ; une stratégie qui se veut nécessairement pluridimensionnelle et qui devra inclure un volet réglementaire, l'élaboration de politiques et de standards, l'emploi d'outils efficace, et plus encore.<sup>65</sup>

Ayant établi les principaux fondements d'une fiducie de données, la prochaine section verra en détail ce qu'elle devra représenter dans le domaine de la santé.

63 McDonald, « The Fiduciary Supply Chain », supra note 49 à la p 59.

64 Ibid.

65 McDonald & Wylie, « What is a data trust ? », supra note 17 ; Element AI et Nesta, « Fiducies de données », supra note 14 à la p 7.

## D. Les particularités d'une fiducie de données dans le domaine de la santé

### 1. Enjeux de gouvernance

La gouvernance des données dans le domaine de la santé représente des enjeux particuliers en raison de la nature des activités de ce domaine ainsi que les fins auxquelles les données sont mises à l'emploi.

D'abord, doté d'une forte tradition de recherche, le domaine de la santé a souvent affaire à des données personnelles de nature hautement sensible, mais qui sont néanmoins cruciales pour faire avancer la médecine, les technologies médicales et l'administration du système de santé au bénéfice de tous. En effet, l'analyse efficace de ces données permet d'observer les tendances se rapportant à la santé de la population, de détecter les problèmes en émergence, et de rapidement mettre sur pied des stratégies d'interventions afin de répondre efficacement aux problèmes identifiés comme prioritaires. Cette utilité d'intérêt public est donc généralement reconnue comme fondamentale à la gouvernance des données dans le domaine de la santé. C'est d'ailleurs ce qu'affirme l'Association Médicale Mondiale (AMM) au paragraphe 5 de sa *Déclaration de Taipei*:

---

*La recherche, faisant appel aux bases de données de santé et aux biobanques, peut souvent accélérer significativement une meilleure compréhension de la santé et des maladies, ainsi que de l'efficacité, de l'efficience, de la sécurité et de la qualité des interventions de prévention, de diagnostic et de traitement. La recherche dans le domaine de la santé représente un bien commun au service des patients individuels ainsi que de la population et de la société.<sup>66</sup>*

---

Par ailleurs, Ohman et al. (2017) identifient plusieurs avantages qui découleraient du transfert des données de la santé à un ou plusieurs répertoires centraux, telle une fiducie de données :

- Les équipes de recherche changent ou se dissolvent ; le transfert des données à un répertoire central permettrait donc de prévenir qu'elles soient perdues ;
- Le répertoire pourrait s'acquitter de tout ce qui se rapporte aux aspects administratifs de l'entreposage et du partage des données (ex. sécurité, formatage, couplage, récupération et extraction, traitement des demandes d'accès, etc.) ; des normes et standards généralisés pourraient aussi être développés et imposés à tout répertoire de données, de façon sectorielle ou générale ;
- Entreposer les données dans un répertoire central les rendrait plus facile à découvrir, améliorant ainsi l'efficacité de la recherche et la réactivité aux problèmes émergents ;
- Les répertoires pourraient être établis à plusieurs échelles (i.e. international, régional, national, spécifique à un secteur, institutionnel, etc.).<sup>67</sup>

---

66 Déclaration de l'Association Médicale Mondiale (AMM) sur les considérations éthiques concernant les bases de données de santé et les biobanques, Adoptée par la 53<sup>e</sup> Assemblée générale de l'AMM, Washington 2002 et révisée par la 67<sup>e</sup>ème Assemblée Générale, Taipei, Taiwan, Octobre 2016. [AMM, Déclaration de Taipei].

67 Ohmann et al. « Sharing and reuse of data from clinical trials », supra note 36 aux pp 17-18.

Le transfert des données à un répertoire central pourrait aussi améliorer les inférences qui pourront être retirées de l'analyse des données. Par exemple, en facilitant le couplage des données de la santé avec d'autres types de données, ceci permettrait d'éclairer d'autres domaines de recherche qui ont des besoins d'informations multisectorielles, tels les déterminants socio-économiques de la santé. C'est d'ailleurs l'approche qu'a entreprise le *National Health Service* du Royaume-Uni<sup>68</sup> par la mise en place d'un répertoire central commun où médecins, travailleurs sociaux et hôpitaux travailleront tous à partir d'un même dossier pour chaque patient, ce qui augmentera leur capacité à prendre une approche multifactorielle concertée à la prodigation de soins à leurs patients, tout en assurant un accès contrôlé aux données du répertoire pour des fins déterminées, telle la recherche.<sup>69</sup> Le système est encadré par des ententes de partage des données et un code de conduite inspiré par le *Nuffield Council on Bioethics*.<sup>70</sup>

D'autres soulèvent aussi la question de la non-utilisation des données médicales, à savoir s'il serait éthique même de ne pas se livrer à la recherche de moyens qui permettront mieux de maximiser leur utilité, étant donné l'importance des bases de données complètes pour la production de résultats qui seront non-biaisés et réellement représentatifs de la population.<sup>71</sup>

En revanche, bien que cette utilité d'intérêt public soit d'importance première, est non moins importante la protection des droits et intérêts des individus que concernent ces données. C'est d'autant ce qu'affirme la *Déclaration de Taipei* de l'AMM à ses paragraphes 4 et 6 : elle rappelle l'importance de protéger la dignité, l'autonomie et la vie privée des personnes par l'adoption de règles strictes en matière de protection des données qui reflèteront les normes et standards éthiques nationaux et internationaux en matière de bases de données de santé. La question du consentement demeurera ainsi au centre de tout projet de gouvernance des données dans ce domaine. Non seulement sera-t-elle importante pour respecter la volonté des individus en matière de leur vie privée, mais aussi au niveau de la protection de certaines libertés fondamentales, telle la liberté de conscience. Par exemple, en permettant aux individus de choisir que leurs données soient utilisées à des fins de recherche conformes à leurs croyances.

Des questions importantes seraient alors à soulever par rapport à la validité du consentement recueilli à la source. Par exemple, celui-ci a beau avoir été recueilli 'pour des fins de recherches, d'études ou de statistiques' de façon large, mais si une recherche en question est contraire aux croyances d'un individu, son consentement serait-il tout de même valide ?

Dans les cas où la réponse serait négative, ceci pourrait engendrer des complications pour soustraire les données de l'individu du jeu de données en question. Par exemple, si les données ont été anonymisées ou dépersonnalisées et ensuite partagées à une tierce partie, il pourrait être impossible de les repérer.

Il y a aussi lieu de se demander qui bénéficiera de l'emploi des données médicales afin de pallier, par exemple, le déséquilibre de pouvoir noté ci-haut entre les utilisateurs des données et les personnes fichées.

68 Tel que souligné dans le rapport de BPE Solicitors LLP, commissionné par le Open Data Institute : « Extended ODI Data Trust report : 5, Further use cases to consider », à la p 19.

69 NHS Department of Health & Social Care, « Code of conduct for data-driven health and care technology », (18 juillet 2019) en ligne : <<https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology>>

70 Nuffield Council on Bioethics, « The collection, linking and use of data in biomedical research and health care: ethical issues », (2015) en ligne : <<https://www.nuffieldbioethics.org/wp-content/uploads/Biodata-a-guide-to-the-report-PDF.pdf>>.

71 Jones et al. « The other side of the coin : Harm due to the non-use of health-related data », (2017) *International Journal of Medical Informatics* 97.

Serait à soulever à ce chapitre la question de la patrimonialisation des données médicales, à savoir si le fait d'accorder un droit de propriété aux personnes sur leurs données personnelles les permettrait d'aliéner ce titre ou même d'accorder un droit d'usage (ex. license) sur celles-ci à contrepartie onéreuse, pour ainsi les permettre de bénéficier de manière plus directe de l'emploi de leurs données personnelles. Tel que discuté ci-haut et réitéré par Béranger et Bouadi<sup>72</sup>, cette approche soulève de nombreuses questions tant d'un point de vue éthique que juridique et est considérée par la plupart comme étant inadéquate. Il faudra alors trouver d'autres moyens pour assurer que les bénéfices qui découlent de l'emploi de données personnelles soient distribués de manière équitable.

Serait aussi à soulever à ce chapitre les intérêts des populations minoritaires ou marginalisées sous représentées dans les jeux de données. Pourrait-on affirmer, par exemple, dans le cas d'une fiducie établie dans 'l'intérêt public', que ces personnes bénéficieraient aussi de la recherche et des technologies mises sur point à partir des jeux de données partagées ? Ces dernières seront-elles vraiment représentatifs des besoins et intérêts particuliers de ces personnes de sorte que l'on puisse dire qu'ils en bénéficient également ?

Plusieurs prônent ainsi la mise sur pied de modèles de gouvernance participatifs afin de mieux assurer que la gouvernance des données ainsi que les bénéfices qui en découleront soient équitables.<sup>73</sup> Par exemple, Sylvie Delacroix et Neil Lawrence<sup>74</sup> proposent une approche 'ascendante' ("*bottom-up trust*") par laquelle la participation hâtive, significative et soutenue de toutes parties intéressées est au cœur du fonctionnement d'une fiducie de données, incluant dans l'élaboration de son cadre de gouvernance, de ses procédures et politiques, etc. pour que ceux-ci reflètent réellement les préférences et intérêts des personnes fichées.

Le rapport commissionné par le Open Data Institute endosse aussi une telle approche, mais souligne néanmoins l'importance de se soucier de l'efficacité d'un outil quelconque pour la gouvernance des données.<sup>75</sup> Il ne faudrait pas, par exemple, que l'utilisation efficace des données soit entravée par une structure de gouvernance trop lourde. La prise en compte de multiples intérêts pourrait ainsi paralyser le fonctionnement efficace d'une fiducie de données. Ceci serait donc à pondérer dans la mise sur pied d'une fiducie de données, idéalement en adoptant un cadre de gouvernance équilibré.

En dernier lieu, mais non moins important, sera le besoin de se soucier de la confiance du public en le projet envisagé. Tel que souligné par Béranger et Bouadi,<sup>76</sup> cette confiance est non seulement essentielle à la collecte des données en premier lieu, elle est aussi fondamentale à la relation soignant-patient par le billet du secret médical. Élément essentiel au rôle du médecin, il ne faudrait pas que cette confiance soit brimée par une gestion inadéquate des données des patients.

Villanueva *et al.* (2019)<sup>77</sup> ainsi que Cook-Deegan, Majumder et McGuire (2019)<sup>78</sup> identifient les principaux éléments essentiels à l'obtention de cette confiance, soit :

- des entités dévouées à la transparence et à la sécurité ;
- qui accorderont aux individus un contrôle adéquat sur leurs données personnelles;
- qui porteront un haut degré d'attention à la qualité des données colligées ;
- et qui intégreront un principe de gouvernance responsable avec des responsabilités claires et bien définies et des personnes qui seront imputables en cas de faute ou négligence dans la gestion des données.

72 Béranger & Bouadi, « Approche éthico-juridique », supra note 34 aux pp 117-18.

73 Element AI et Nesta, « Fiducies de données », supra note 14 à la p 15.

74 Delacroix & Lawrence, « Bottom-up data Trusts », supra note 29.

75 Pinsent Masons et al., « Data trusts », supra note 12 à la p 42.

76 Béranger & Bouadi, « Approche éthico-juridique », supra note 34 aux pp 109-112.

77 Villanueva et al., « Genomic Data-Sharing Practices » (2019) 47 J Law Med Ethics 1.

78 Robert Cook-Deegan, Mary A Majumder et Amy L McGuire, « Introduction: Sharing Data in a Medical Information Commons », (2019) 47 J Law Med Ethics 1.

Ces critères sont aussi largement similaires à ceux établis par l'AMM<sup>79</sup> à titre de principes qui devraient gouverner toute initiative de gouvernance des données, soit : la transparence, la protection des droits et intérêts des individus, la participation et l'inclusivité des parties intéressées de manière significative, et un principe de gouvernance responsable.

- Au chapitre de la transparence, ceci s'appliquerait tant au niveau des procédures et politiques qu'au niveau du traitement des demandes d'accès aux données (en dévoilant, par exemple, l'identité des parties demanderes, la raison pour leur intérêt aux données, et la décision rendue sur la demande)<sup>80</sup> ;
- Au chapitre de la protection des droits et intérêts des individus, serait intégral à ce principe la mise en place de mécanismes pour assurer la sécurité des données ainsi que des moyens pour permettre le respect d'un droit de retrait et à la transférabilité des données.<sup>81</sup> Il pourrait alors être nécessaire de prévoir l'emploi de technologies qui permettraient de retracer les données d'un individu en question advenant le retrait de son consentement. En ce qui a trait à la sécurité des données, celle-ci devrait être assurée selon les meilleures pratiques existantes ; plusieurs modèles sont disponibles à cet effet à titre de référence.<sup>82</sup>
- En ce qui a trait à la participation et l'inclusivité du public et des parties intéressées, telle que noté ci-haut, celle-ci devrait inclure une attention particulière portée aux minorités ainsi qu'aux personnes et communautés marginalisées ou vulnérables.<sup>83</sup> Aussi, l'engagement des parties intéressées devrait être hâtive et soutenu tout au long de l'existence d'un projet de gouvernance des données.<sup>84</sup> L'on recommande, par exemple, la mise sur pied d'un conseil de fiduciaire représentatif,<sup>85</sup> ou même de plusieurs comités de représentants au sein de la structure de gouvernance de la fiducie, qui inclurait des pouvoirs concrets tels des droits de vote ou autre<sup>86</sup>. Il y aurait aussi idéalement participation active dans la définition des objectifs de la fiducie ainsi que dans l'élaboration des règles qui dicteront l'accès aux données et les usages qui pourront en être fait ;<sup>87</sup>

79 AMM, Déclaration de Taipei, supra note 66 aux para 9, 17, 20.

80 Paprica et al. « Essential requirements for establishing and operating data trusts », supra note 53 aux pp 4-5 ; Willison et al., « Participatory governance over research in an academic research network : the case of Diabetes Action Canada », (2019) 2019 BMJ Open 9e026828 à la p 4 [Willison et al., « Participatory governance »] ; Jack Teng et al, « Sharing linked data sets for research: results from a deliberative public engagement event in British Columbia, Canada » (2019) 4 International Journal of Population Data Science 1 à la p 7 [Teng et al., « Sharing linked data sets »] ; Ohmann et al. « Sharing and reuse of data from clinical trials », supra note 36, aux pp 11, 14.

81 Element AI et Nesta, « Fiducies de données », supra note 14 à la p 15.

82 Paprica et al. « Essential requirements for establishing and operating data trusts », supra note 53 aux pp 2, 4 dénomment plusieurs tels cadres de référence. Par exemple, les principes de gouvernance d'Elinor Ostrom ou ceux du cadre FAIR de Wilkinson et al., « The FAIR Guiding Principles for scientific data management and stewardship. Sci Data » (2016) 3,160018 ; les « Five Safes » (F. Ritchie « The "Five Safes": a framework for planning, designing and evaluating data access solutions » (2017) Zenodo ; les principes TRUST (Lin D, Crabtree et al., « The TRUST Principles for digital repositories » (2017) Scientific Data 7 ; et plusieurs autres : Burton PR et al., « Data Safe Havens in health research and healthcare » (2015) 31 Bioinformatics 20 ; Global Alliance for Genomics & Health, « Framework for responsible sharing of genomic and health-related data » (2014) Toronto: Global Alliance for Genomics & Health, en ligne : <<https://tinyurl.com/yb7f8jry>> ; Ipsos MORI, « The one-way mirror: public attitudes to commercial access to health data » (2016) UK: Wellcome Trust, en ligne : <<https://tinyurl.com/y7dyemla>> ; Open Data Institute, Designing Trustworthy Data Institutions, (London, UK: Open Data Institute, 2020), disponible en ligne : <<https://tinyurl.com/y9n87t2a>>.

83 AMM, Déclaration de Taipei, supra note 66 au para 17.

84 Paprica et al. « Essential requirements for establishing and operating data trusts », supra note 53 aux pp 3, 5 ; Willison et al., « Participatory governance », supra note 80 à la p 4 ; Pam Carter, Graeme T Laurie et Mary Dixon-Woods, « The social licence for research: why care.data ran into trouble », (2015) 41 Journal of Medical Ethics 5 [Carter et al., « The social license for research »].

85 Element AI et Nesta, « Fiducies de données », supra note 14 à la p 27.

86 Voir par exemple le modèle de gouvernance développé par Willison et al., « Participatory governance », supra note 80 aux pp 4-6.

87 Aidan Peppin, « Doing good with data: what does good look like when it comes to data stewardship? », Ada Lovelace Institute, Nuffield Foundation (3 sept 2020) en ligne : <<https://www.adalovelaceinstitute.org/blog/what-does-good-look-like-data-stewardship/>>.



- En ce qui a trait au principe de gouvernance responsable, en sus de ce qui fut mentionné ci-haut, celui-ci inclura idéalement un cadre de dirigeants accessibles au public et réactifs à leurs interpellations ainsi que des mécanismes internes de grief et de résolution des différends.<sup>88</sup> Une formation de tous ceux qui auront affaire aux données colligées, incluant ceux à qui l'on accordera l'accès, pourrait aussi être envisagée afin de s'assurer que tous soient au fait des règles et procédures entourant la gestion et l'utilisation des données.<sup>89</sup> L'emploi d'ententes d'utilisation ainsi que des ententes de *provision* des données est aussi recommandé afin d'assurer le respect des règles et procédures, de la finalité globale du cadre de gouvernance, ainsi que de toutes autres normes ou standards établis pour assurer la qualité et la fiabilité des données colligées.<sup>90</sup> Des sanctions *significatives* pourraient aussi être prévues pour davantage inciter le respect de ces ententes et inspirer confiance au public et aux parties intéressées quant à l'efficacité de ces mécanismes. Certains soulèvent tout de même que de tels mécanismes seraient insuffisants au chapitre de la protection des droits des individus puisque ces derniers n'auraient aucun droit d'action en vertu de telles ententes, faute d'en être partie.<sup>91</sup> D'autres soutiennent qu'il serait néanmoins possible de leur accorder un tel droit par une stipulation explicite à cet effet dans le cadre de ces ententes.<sup>92</sup> Aussi, la voie d'action en vertu des lois sur la protection des renseignements personnelles ou sensibles serait également toujours possible.<sup>93</sup> Des mécanismes de surveillance et de contrôle sont aussi recommandés afin d'assurer le respect de ces ententes et de prévenir les utilisations illicites ou contraire à l'éthique.<sup>94</sup> Certains sont toutefois d'avis que de tels mécanismes seraient trop onéreux au niveau des coûts et du temps et devraient alors plutôt être entrepris par l'État.<sup>95</sup> Bien qu'il n'y ait aucun consensus sur ce point,<sup>96</sup> il est tout de même suggéré que des vérifications périodiques soient effectuées pour vérifier la conformité avec les termes stipulés dans ces ententes.<sup>97</sup>

Pour Carter et al. (2015)<sup>98</sup> ainsi que Paprica et al. (2020)<sup>99</sup>, la perception du public sera tout aussi importante au chapitre de la confiance du public. En effet, même si une stratégie de gouvernance des données met tous les éléments nécessaires en place pour être digne de confiance, le public n'en sera convaincu tant qu'elle ne reflètera pas les valeurs de réciprocité et de non-exploitation, et qu'elle ne soit fondée sur une participation purement volontaire et orientée vers une finalité d'intérêt public. Il sera ainsi nécessaire d'entreprendre des actions concrètes pour engager le public et les sensibiliser par rapport aux mesures mis en place qui correspondent à ces critères.<sup>100</sup>

88 Pinsent Masons et al. « Data trusts », supra note 12 à la p 36.

89 Ibid.

90 Ohmann et al. « Sharing and reuse of data from clinical trials », supra note 36, aux pp 11, 15 ; Paprica et al. « Essential requirements for establishing and operating data trusts », supra note 53 aux pp 3, 5 ; Teng et al., « Sharing linked data sets », supra note 78 à la p 7 ; Pinsent Masons et al. « Data trusts », supra note 12 aux pp 26-28, 34, 44, 46.

91 Pinsent Masons et al. « Data trusts », supra note 12 à la p 36.

92 Ibid.

93 Ibid.

94 Pinsent Masons et al. « Data trusts », supra note 12 à la p 31.

95 Teng et al., « Sharing linked data sets », supra note 78 à la p 7.

96 Ibid.

97 Pinsent Masons et al. « Data trusts », supra note 12 aux pp 8, 39-40.

98 Carter et al., « The social license for research », supra note 84.

99 Paprica et al. « Essential requirements for establishing and operating data trusts », supra note 53 à la p 6.

100 Dans leur étude du cas d'usage de Care.data, une fiducie de données mis en place dans le domaine de la santé au R.U., Carter et al., « The social license for research », supra note 84 soulignent un nombre de lacunes du projet à ces égards qui, pour eux, avaient ultimement conduit à l'échec du projet. Selon ces auteurs, malgré la structure de gouvernance adéquate mise en place, un manque de transparence, des campagnes de sensibilisation qui furent perçues comme trompeur, un manque d'engagement du public et des principales parties intéressées et une perception de conflit d'intérêts furent fatal au projet.



Ainsi, pour résumer, revêtent une importance égale dans la gouvernance des données dans le domaine de la santé :

- D'une part, le respect des droits des individus ainsi que la prise en compte des intérêts des diverses parties intéressées par le billet d'une gouvernance transparente, responsable, digne de confiance, et orientée vers une finalité d'intérêt public ; une participation active et collaborative de ces dernières devra aussi être priorisée ;
- Et d'une autre part, une utilisation efficace et efficiente des données qui permettra que soit retiré leur plein potentiel au bénéfice de tous.

Le respect des lois et règlements en vigueur sera évidemment incontournable, mais peu importe, la protection des droits et intérêts des individus devra être au cœur d'un exercice de gouvernance des données dans le domaine de la santé, notamment en portant une attention particulière à la qualité du consentement recueilli à la source et en prévoyant également un droit de retrait et un droit à la transférabilité des données.

Se rajoutent à ceci les raisons principales mis en relief dans la section précédente quant aux raisons pour lesquelles la fiducie de données fut identifiée comme un outil intéressant pour la gouvernance des données, soit :

- une administration fiduciaire indépendante<sup>101</sup> d'un patrimoine composé de données ; l'administration fiduciaire étant « the highest level of obligation that one party can owe to another, [characterized by the highest] degree of impartiality, prudence, transparency and undivided loyalty »<sup>102</sup>.

Pour reprendre encore une fois les propos de Jack Hardinges du Open Data Institute : « data trusts don't aim to enable easier access to data; on the contrary, they offer a solution for providing better controls around how data is accessed, shared and communicated »<sup>103</sup>. Les propos de Bartha M. Knoppers et de Mark Phillips du *Centre de génomique et politiques* de l'université McGill vont dans le même sens. Dans leur article « Whose Commons? » publié dans *The Journal of Law, Medicine & Ethics* en 2019, ceux-ci avancent que la gouvernance des données dans le domaine de la santé devrait viser tant la protection des données que le principe de la science ouverte.<sup>104</sup> Ce double objectif appelle donc à la mise sur pied d'outils de gouvernance qui seront essentiellement équilibrés tenant compte de tous les enjeux ci-haut mentionnés.

101 Voir *supra* note 57.

102 Hardinges, « Data Trusts in 2020 », *supra* note 57.

103 *Ibid.*

104 Phillips & Knoppers « Whose Commons? », *supra* note 37 à la p 110.

## 2. Finalité et principes directeurs

À la lumière de ce qui fut mis en relief jusqu'à maintenant, il est possible de résumer les principales caractéristiques que devra revêtir une fiducie de données dans le domaine de la santé en ce qui suit :

- Un outil qui pourra assurer une gouvernance fiduciaire indépendante des données qui sera juste, sécuritaire et équitable ;
- Qui sera en mesure de pallier l'érosion de la confiance du public eu égard la gestion de leurs données personnelles et à la protection de leurs droits et intérêts ;
- Qui sera versatile et flexible afin de permettre l'élaboration d'une structure de gouvernance *sur mesure* et inspiré de la notion de *stewardship*, notamment en revêtant les éléments suivants :
  - La possibilité d'instaurer des contrôles adéquats sur l'accès, le partage et la communication des données ;
  - La possibilité d'établir une structure de gouvernance participative et collaborative pour la gestion des données à titre de biens communs ;
  - Tout en intégrant les obligations juridiques qui s'imposent typiquement aux fiduciaires, incluant des mécanismes de responsabilités claires et bien définies.
- Qui sera toutefois *équilibré* afin de permettre l'innovation et le développement du plein potentiel des nouvelles technologies numériques, notamment :
  - En facilitant un accès et partage rapide des données autant que nécessaire ;
  - En permettant le développement de bases de données complètes et, idéalement, interconnectées ;
  - Tout en minimisant autant que possible le fardeau administratif et les coûts connexes à la gestion des données.<sup>105</sup>

Ceci étant, il est aussi raisonnable d'avancer qu'elle devrait être établie avec les doubles objectifs de faciliter le partage des données et leurs utilisation à des fins d'intérêts public en accordant autant d'importance à la protection des droits et intérêts des personnes fichées et des parties intéressées.

Ces critères serviraient ainsi pour guider l'élaboration du cadre de gouvernance d'une fiducie de données dans le domaine de la santé.

<sup>105</sup> Ohmann et al. « Sharing and reuse of data from clinical trials », supra note 36 aux pp 15, 17 ; Teng et al., « Sharing linked data sets », supra note 78 aux pp 7-8 ; Element AI et Nesta, « Fiducies de données », supra note 14 aux pp 11-12.

### 3. Autres indicateurs à titre de meilleures pratiques

En sus de ce qui fut mentionné ci-haut, les éléments suivants ont aussi été retenus à titre de meilleures pratiques :

- Une structure de gouvernance des données dans le domaine de la santé devrait inclure des dispositions sur :
  - la nature des données contenues dans la base ; l'obtention soit d'un consentement adéquat, soit d'une autre justification légale pour la collecte et le partage des données ; la manière dont les données seront documentées et traçables conformément au consentement des personnes concernées ; des critères et procédures concernant l'accès, le partage ainsi que le couplage des données de santé (ex. désidentification, formatage, contrôles de la qualité, etc.); la ou les personnes désignées responsables de la gouvernance ; les mesures de sécurité afin de prévenir les accès non autorisés ou les partages inappropriés; les procédures pour reprendre, si nécessaire, contact avec les participants ; les procédures d'enregistrement et de traitement des demandes et des réclamations ; la durée de stockage ; l'élimination et la destruction des données ; la fin de vie du répertoire et la manière dont les données seront traitées dans le cas d'une dissolution, d'un changement dans la forme juridique ou de l'affectation principale du répertoire initialement conçu.<sup>106</sup>
- Les exécutants chargés de la gestion des données devraient être des personnes qualifiées et compétentes eu égard la nature complexe des tâches qu'implique leur rôle (ex. pour apprécier les mérites des demandes d'accès aux données, des propositions de recherche, etc.).<sup>107</sup> La mise sur pied d'un comité de contrôle ou d'un comité d'éthique est recommandé<sup>108</sup> ; d'autres ont aussi recommandé la mise sur pied d'un nouvel ordre professionnel en matière de gouvernance des données, afin d'assurer un contrôle des connaissances et la disponibilité d'un bassins de professionnels qualifiés.<sup>109</sup>

### 4. Principaux obstacles et défis

Un des plus importants obstacles en lien avec l'établissement d'une fiducie pour la gouvernance des données de santé est celui du consentement. La plupart des régimes sur la protection des renseignements personnels exigent que le consentement soit volontaire, libre et éclairé, ce qui implique normalement un avis de toutes les fins pour lesquelles les données seront utilisées. Or, en envisageant la mise sur pied de répertoires massifs conçus pour colliger des données à long-terme, justement pour permettre qu'elles soient utilisées à plusieurs fins, certains soulignent avec raison qu'il serait presque impossible de faire en sorte que le consentement à la source soit complètement éclairé, vu l'impossibilité de prédire toutes les fins auxquels les données pourraient éventuellement servir.<sup>110</sup>

Tel que mentionné ci-haut, un consentement large peut être recueilli à la source (ex. 'pour des fins de recherches, d'études ou de statistiques'), mais ceci ne sera pas nécessairement suffisant pour assurer le respect de la liberté de conscience des personnes fichées. Par exemple, dans les cas où leurs données seraient utilisées dans le cadre de recherches ou d'études contraires à leurs croyances ou valeurs. Ceci serait à considérer dans l'élaboration des avis d'obtention du consentement à la source.

106 AMM, Déclaration de Taipei, supra note 66 au para 21.

107 Teng et al., « Sharing linked data sets », supra note 78 aux pp 6-7 ; Ohmann et al. « Sharing and reuse of data from clinical trials », supra note 36, aux pp 18-19 ; Element AI et Nesta, « Fiducies de données », supra note 14 à la p 27 ; AMM, Déclaration de Taipei, supra note 66 au par 23.

108 Element AI et Nesta, « Fiducies de données », supra note 14 à la p 27 ; AMM, Déclaration de Taipei, supra note 66 au par 19 ; Ohmann et al. « Sharing and reuse of data from clinical trials », supra note 36, aux pp 7, 12, 14.

109 Element AI et Nesta, « Fiducies de données », supra note 14 à la p 27 ; Teng et al., « Sharing linked data sets », supra note 78 aux pp 6-7.

110 Pinsent Masons et al. « Data trusts », supra note 12 aux pp 21-22, 58 ; Ohmann et al. « Sharing and reuse of data from clinical trials », supra note 36, aux pp 19-20.

D'autres soulignent aussi le frein que pourraient représenter les cadres réglementaires au partage des données : jusqu'à maintenant, la tendance fut d'interdire les usages secondaires ou les partages des données colligées pour toutes fins autres que celle pour laquelle les données furent initialement colligées. Les opposants de cette approche remarque que ceci contraste drastiquement avec la tendance d'aujourd'hui qui se dirige plutôt vers la science ouverte, et qui nécessite que soit permis la réutilisation des données pour des fins non-nécessairement prévues à l'origine.<sup>111</sup>

La *Déclaration de Taipei* de l'AMM fourni d'intéressantes indications à cet effet. À ses paragraphes 12, 14 et 15 elle stipule :

---

*12. Si les données ou le matériel biologique sont collectés et stockés dans une base de données de santé ou une biobanque pour des utilisations multiples et indéfinies, le consentement est valable uniquement si les personnes concernées ont été informées de manière adéquate sur:*

- *L'objet de la base de données de santé ou de la biobanque ;*
- *Les risques et contraintes associés à la collecte, au stockage et à l'utilisation des données et du matériel;*
- *La nature des données ou du matériel à collecter ;*
- *Les procédures de retour des résultats y compris des découvertes fortuites ;*
- *Les règles d'accès à la base de données de santé ou à la biobanque;*
- *La manière dont la vie privée est protégée;*
- *Les dispositifs de gouvernance tels que stipulés dans le paragraphe 22;*
- *Le fait que dans les cas où les données et le matériel sont rendus non identifiables, la personne n'est plus en mesure de savoir ce qui est fait de ses données/matériel et ne peut plus retirer son consentement. [ sic ]*
- *Leurs droits fondamentaux et les mesures de sauvegarde énoncées dans cette Déclaration; et*
- *Le cas échéant, l'utilisation commerciale et le partage des bénéfices, la propriété intellectuelle et le transfert de données ou de matériel à d'autres institutions ou à des pays tiers.*

*14. Les personnes ont le droit de demander et d'obtenir des informations sur leurs données et leur utilisation ainsi que de faire corriger les erreurs ou omissions. Les bases de données de santé et les biobanques devraient adopter des mesures adéquates pour informer les personnes concernées sur leurs activités.*

*15. Les personnes ont le droit à tout moment et sans crainte de représailles de modifier leur consentement ou de demander le retrait de leurs données identifiables d'une base de données de santé et de leur matériel biologique d'une biobanque. Ceci s'applique à l'utilisation future des données et du matériel biologique.*

---

Ces indications pourraient ainsi être suivis dans l'élaboration des avis d'obtention du consentement à la source, tant que les lois en vigueur n'écartent une telle approche.

---

111 Phillips & Knoppers « Whose Commons? », supra note 37 ; Ohmann et al. « Sharing and reuse of data from clinical trials », supra note 36.

D'autres obstacles potentiels qui ont été soulevés sont :

- **Le manque de précision dans la législation sur ce qui permettrait le partage des données.** Selon les observations de Bubela et al. (2019) du domaine de la santé ontarien, le manque de précision du terme « données non identifiable » – et pour qui la loi permettait le partage – a créé une culture d'aversion au risque parmi les détenteurs de données, qui préfèrent restreindre l'accès aux données alors même que la loi permettrait le partage.<sup>112</sup>
- **Une culture d'aversion au risque généralisée** envers le partage des données et envers un plus haut degré d'intégration des données, en raison du manque de confiance dans les institutions chargées d'en assurer une protection adéquate.<sup>113</sup>
- **Un cadre réglementaire généralement trop stricte**, par exemple : si le partage ou l'utilisation secondaire ne sont permis qu'à des fins de recherche, et non, par exemple, aux fins visant l'élaboration de politiques fondées sur les faits ; si le couplage des données personnelles avec des données administratives ou autres données non-personnelles est interdit ; ou encore si la loi est trop prescriptive en ce qu'elle permet le partage à ou entre les seules entités désignées par la loi.<sup>114</sup>
- **La difficulté de garantir un droit à la révocation du consentement ou à la transférabilité** dans les cas où il serait impossible de retracer les données d'un individu en particulier (ex. si les données furent désidentifiées).<sup>115</sup>
- **Les défis d'ordre logistique**, tels : des techniques de stockage et de récupération des données mal adaptées à la recherche longitudinale ; des difficultés à faire des liaisons entre différents types de données qui exigent différents niveaux d'approbation pour l'accès (ex. données administratives, données diagnostiques, etc.).<sup>116</sup>
- **L'obligation d'avoir au moins un bénéficiaire désigné.** Par exemple, le fait que le *trust* de la common law, sauf pour le *charitable trust*, ait obligatoirement un ou des bénéficiaires désignés, faisant qu'il ne pourrait être établi pour une finalité strictement d'intérêt public.<sup>117</sup>
- **L'administration paralysée par une structure trop participative ou collaborative.** Par exemple, dans un cas où chacune des parties intéressées serait accordée un droit de vote : si celles-ci sont trop nombreuses, l'administration risque de devenir trop lourde en raison du besoin de tenir compte de leurs multiples intérêts et attentes, qui seront vraisemblablement parfois incompatibles et inconciliables.<sup>118</sup> Une solution proposée fut l'idée de permettre le développement d'un réseau de plusieurs petites fiducies, chacune avec des modalités différentes correspondant à un groupe précis de parties prenantes, ou à un secteur en particulier.<sup>119</sup>
- **Un problème de fragmentation des données.** En revanche, le développement d'un réseau composé de plusieurs plus petite fiducies risque de causer un problème de fragmentation des données et ainsi d'anéantir les bénéfices espérés du fait d'avoir un vaste nombre de données colligées dans un même répertoire. Ceci risque aussi de réduire l'utilité des données si le partage entre les différentes fiducies est rendu impossible en raison de modalités incompatibles.<sup>120</sup>

112 Tania Bubela et al., « Medical Information Commons to support learning healthcare systems : examples from Canada », (2019) 47 J Law Med Ethics 1 aux pp 98-99 [Bubela et al., « Medical Information Commons »].

113 Ibid.

114 Compute Ontario, ICES et ORION, « Building Ontario's Next-Generation Smart Cities Through Data Governance, Part 1 : Health Data Safe Haven » (2019), aux pp 17-21 [Compute Ontario et al., « Building Ontario's Next-Generation Smart Cities »].

115 Element AI et Nesta, « Fiducies de données », supra note 14 à la p 27.

116 Bubela et al., « Medical Information Commons », supra note 112 aux pp 100-101.

117 Pinsent Masons et al. « Data trusts », supra note 12 à la p 12.

118 Element AI et Nesta, « Fiducies de données », supra note 14 à la p 16.

119 Ibid à la p 26.

120 Ibid ; Teng et al., « Sharing linked data sets », supra note 78 aux pp 7, 9.

- **L'incongruence inter-juridictionnelle.** Ceci pourrait décourager le partage des données entre provinces et avec d'autres pays.<sup>121</sup> Ceci pourrait aussi mener à la réplication du problème des paradis fiscaux. Reconnaissant que les données représentent énormément de valeur, il pourrait y avoir un incitatif à les placer dans des juridictions plus favorables à leur exploitation selon les ambitions des détenteurs.<sup>122</sup>
- **Les délais de constitution.** Pour constituer un *charitable trust* en Ontario par exemple, l'on remarque que le délai est d'au moins un an pour l'obtention du statut d'organisme charitable.<sup>123</sup>
- **L'inflexibilité potentiel.** Il fut remarqué à quelques reprises, mais sans plus de justification, que les fiducies de données ne s'avèreraient pas un bon outil vu la meilleure flexibilité représentée par d'autres véhicules juridiques.<sup>124</sup> Ainsi, il faudrait faire une analyse comparative des différents véhicules dans une juridiction donnée afin de déterminer celle qui serait la plus convenable au chapitre du besoin de flexibilité.
- **L'atteinte à la crédibilité de la fiducie faute de pouvoir contrôler l'usage après partage.** Des préoccupations ont été soulevées par rapport au contrôle de l'usage des données une fois partagées.<sup>125</sup> L'on se demande par exemple, si les exigences de confidentialité suivront les données entre les mains des tiers.<sup>126</sup> Est-ce que ces tiers pourront eux-même partager ces données ? Pourront-ils même les revendre à profit ? Les utiliser à des fins autres que celles consenties ? En réponse à ces préoccupations, les suggestions vont tous dans le sens de les répondre avec les règles, procédures et mécanismes mis en place dans le cadre de l'établissement de la structure de gouvernance (ex. dans le cadre d'une entente d'usager ou d'un code de conduite prenant la forme d'une entente multilatérale, l'on pourrait exiger la conformité à un minimum de standards éthiques de recherche,<sup>127</sup> interdire le repartage et la réidentification, définir en quoi constitue une utilisation adéquate des données, exiger une formation sur la sécurité et l'utilisation adéquate, prévoir des pénalités en cas de non-respect, etc.)<sup>128</sup> ;
- **L'incertitude face à un rôle potentiel de surveillance imposé au fiduciaire.** Tel que mentionné ci-haut, certains prétendent qu'un tel rôle serait un usage inapproprié de ressources et du temps du fiduciaire ;<sup>129</sup>

121 Bubela et al., « Medical Information Commons », supra note 112 à la p 98.

122 McDonald, « Reclaiming Data Trusts », supra note 14.

123 Compute Ontario et al., « Building Ontario's Next-Generation Smart Cities », supra note 114 à la p 17.

124 Pinsent Masons et al. « Data trusts », supra note 12, aux pp 29-30 ; Compute Ontario et al., « Building Ontario's Next-Generation Smart Cities », supra note 114 aux pp 15-16.

125 Pinsent Masons et al. « Data trusts », supra note 12, à la p 26; Teng et al., « Sharing linked data sets », supra note 78 aux pp 7-8 ; Ohmann et al. « Sharing and reuse of data from clinical trials », supra note 36.

126 Pinsent Masons et al. « Data trusts », supra note 12, à la p 26.

127 Teng et al., « Sharing linked data sets », supra note 78 aux pp 7-9.

128 Ibid ; Ohmann et al. « Sharing and reuse of data from clinical trials », supra note 36 ; Pinsent Masons et al. « Data trusts », supra note 12, à la p 26.

129 Teng et al., « Sharing linked data sets », supra note 78 à la p 7.

- **Financement.** Vu la versatilité du véhicule, le financement d'une fiducie de données pourrait être assuré de nombreuses différentes façons selon qu'elle est à vocation commerciale ou non, selon la nature de ses activités, etc.<sup>130</sup> Une fiducie de données dans le domaine de la santé sera vraisemblablement à vocation non-commerciale, vu l'importance qu'elle soit vouée à une finalité d'intérêt public et qu'elle représente aussi des valeurs de non-exploitation. Elle nécessitera néanmoins un financement adéquat afin de maintenir ses fonctions de gestion des données<sup>131</sup> et elle risque ainsi de connaître les mêmes difficultés que connaissent les biobanques en cette matière.<sup>132</sup> Celles-ci, consituées majoritairement en tant qu'organisme à but non lucratif, connaissent selon Caulfield et al. (2014)<sup>133</sup> des pressions importantes en lien avec un financement majoritairement à court-terme provenant des bailleurs de fonds principaux tels les université, les hôpitaux et le gouvernement. Cette insécurité financière les poussent ainsi à rechercher un financement plus stable auprès du secteur privé, ce qui entrave évidemment leur capacité à demeurer des institutions axées uniquement sur l'intérêt public.

Afin de sécuriser un financement plus stable, certains ont suggéré que le financement pourrait provenir de licences éventuellement octroyées pour l'utilisation des données.<sup>134</sup>

D'autres encore soulèvent la question de la rémunération du fiduciaire, à savoir s'il agirait-il à titre gratuit ou non. Selon la loi des *trusts* en common law, les fiduciaires n'ont pas le droit de tirer profit des biens détenus en fiducie, à moins que l'acte constitutif de la fiducie en dispose autrement.<sup>135</sup> Lau, Penner et Wong souligne par contre que bien que ceci soit vrai, la loi des *trusts* reconnaît tout de même au fiduciaire le droit d'être rémunéré.<sup>136</sup> Ainsi selon eux, cette question ne devrait pas poser de problèmes peu importe si la fiducie est à vocation commerciale ou non.<sup>137</sup>

## 5. Obstacles potentiellement fatals

Le premier obstacle potentiellement fatal à la constitution d'une fiducie de données au Québec s'agit de la question des bénéficiaires. Selon le rapport commissionné par le ODI, les juridictions sous étude dans le cadre de leur rapport devaient nécessairement avoir un ou des bénéficiaires désignés pour constituer une fiducie. Il serait alors impossible de l'affecter à une finalité d'intérêt public. Les auteurs l'avaient donc exclu pour cette raison.<sup>138</sup> Ils soulignèrent tout de même la possibilité qu'elle soit constituée en *charitable trust*, mais estimaient cette forme tout aussi inappropriée en raison des contraintes trop nombreuses de ce véhicule en particulier.<sup>139</sup> Ils n'ont toutefois donné aucune explication supplémentaire. Compute Ontario, l'ICES et ORION endossent aussi cette position dans leur rapport sur les fiducies de données, réitérant que d'autres structures légales seraient plus appropriées en raison de leur plus grande flexibilité, sans non plus donner davantage d'explications.<sup>140</sup> Ainsi, nous retenons de ceci simplement qu'il sera essentiel qu'une fiducie puisse être constituée sans bénéficiaires et dans un but d'intérêt public, et qu'elle devra revêtir une forme flexible.

130 Element AI et Nesta, « Fiducies de données », supra note 14 à la p 15 ; Paprica et al. « Essential requirements for establishing and operating data trusts », supra note 53 à la p 5.

131 Ohmann et al. « Sharing and reuse of data from clinical trials », supra note 36, à la p 7.

132 Timothy Caulfield et al., « A review of the key issues associated with the commercialization of biobanks » (2014) 1 Journal of Law and the Biosciences 1.

133 Ibid.

134 Element AI et Nesta, « Fiducies de données », supra note 14 à la p 15.

135 Pinsent Masons et al. « Data trusts », supra note 12, à la p 58.

136 Lau, Penner & Wong, « Data trust basics », supra note 52 à la p 94.

137 Ibid.

138 Pinsent Masons et al. « Data trusts », supra note 12, à la p 12.

139 Pinsent Masons et al. « Data trusts », supra note 12, à la p 60.

140 Compute Ontario et al., « Building Ontario's Next-Generation Smart Cities », supra note 114 aux pp 15-16.

Le deuxième obstacle potentiellement fatal à la constitution d'une fiducie de données au Québec s'agit de la question de la patrimonialité des données. En effet, dans la plupart des cas, la constitution d'une fiducie implique *nécessairement* le transfert d'un ensemble de biens (au sens légal) pour être détenu en fiducie. Le rapport commissionné par le ODI est clair à cet égard :

---

*[...] data cannot constitute property in the legal trust sense and thus cannot form the basis of a legal trust in any of the legal systems which have a concept of trust law.<sup>141</sup> [...] Expert commentators agree that in the current state of the law it is highly unlikely that a court will classify information or data as a species of conventionally understood property.<sup>142</sup>*

---

Le titre du droit de propriété est central à cette opération : s'il n'y a pas de biens à gérer et administrer, il ne peut tout simplement pas avoir de fiducie faute d'objet. Puisque les données ne sont pas, jusqu'à présent, appropriables, il n'existe tout simplement pas de 'titre' à transférer, donc pas de fiducie possible.

Plusieurs remarquent néanmoins que les données sont déjà reconnues à titre d'actif extrêmement précieux dans l'économie mondiale.<sup>143</sup> En effet, tel que mentionné dans l'introduction de ce rapport, elles constituent le fondement du modèle d'affaires des compagnies ayant les plus grandes capitalisations boursières au monde. Selon les propos du professeur Pierre Trudel, « [c]ette ressource doit être dotée d'un statut moins naïf que celui qui est prévu par les lois actuelles ». <sup>144</sup> Ritter & Mayer (2019) vont encore plus loin en essayant d'opérationnaliser le concept des données en tant que biens. Pour eux, les données deviennent appropriables du moment qu'elles sont enregistrées sur un support fixe.<sup>145</sup> McFarlane (2019)<sup>146</sup> prend une voie différente en soutenant que ce serait plutôt les droits des individus en lien avec leurs données qui pourraient être transférés en fiducie. Il remarque, par exemple, que des droits de créances peuvent être détenus en fiducie. Il raisonne que dans la mesure que les droits en vertu des lois sur la protection de la vie privée sont corrélatives d'obligations imposées aux contrôleurs des données, que ces droits constituent une forme de créance et pourraient ainsi être détenus en fiducie. Pour Lau, Penner et Wong, c'est encore plus simple : il est un principe élémentaire en droit des *trusts* que tout droit ayant une valeur pécuniaire peut être détenu en fiducie.<sup>147</sup> Ainsi, dans la mesure que les données ont incontestablement une valeur économique, elles pourraient être détenues en fiducie. Ils avancent par exemple que des licences et droits d'accès aux données pourraient être détenus en fiducie.<sup>148</sup> Ils reconnaissent toutefois que les droits extrapatrimoniaux ne pourraient être détenus en fiducie puisqu'ils sont inaliénables et donc incessibles.<sup>149</sup> Ainsi, contrairement à ce que prétendait McFarlane, ces droits ne pourraient être détenus en fiducie faute de pouvoir être 'transférés'. C'est aussi ce qu'avait remarqué monsieur Lionel Smith, le civiliste consulté par Lau, Penner et Wong dans le cadre de leur recherche : « puisque la loi sur les fiducies encadre exclusivement un patrimoine affecté à une fin particulière, par définition, une fiducie au Québec ne peut contenir que des droits patrimoniaux ». <sup>150</sup>

141 Pinsent Masons et al. « Data trusts », supra note 12, à la p 12.

142 Pinsent Masons et al. « Data trusts », supra note 12, à la p 26. Ce rapport renvoie le lecteur aux références suivantes : Jeffrey Ritter et Anna Mayer, « Regulating Data as Property: A New Construct for Moving Forward », (2018) 6 Duke Law & Technology Rev 220 [Ritter et Mayer, « Data as Property »] ; Oxford v. Moss (1979) 68 Cr App Rep 183.

143 Klaus Schwab et al., « Personal data: The emergence of a new asset class. Opportunities for the telecommunications industry », World Economic Forum (2011) en ligne : <[http://www3.weforum.org/docs/WEF\\_ITTC\\_PersonalDataNewAsset\\_Report\\_2011.pdf](http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf)>.

144 Trudel, « La valeur de nos données de santé », supra note 3.

145 Ritter et Mayer, « Data as Property », supra note 142 à la p 260.

146 Ben McFarlane, « Data Trusts and Defining Property », University of Oxford Faculty of Law (29 oct 2019) en ligne : <<https://tinyurl.com/ybzkwjy>>.

147 Lau, Penner et Wong, « Data trust basics », supra note 52 à la p 102.

148 Ibid à la p 16.

149 Ibid à la p 14.

150 Ibid.



## PARTIE III : ÉTUDE DÉTAILLÉE DE LA FIDUCIE EN DROIT QUÉBÉCOIS

### I. Pour une fiducie de données dans le domaine de la santé au Québec ?

Ayant établis les indicateurs clés d'une fiducie de données dans le domaine de la santé, cette section procèdera à une analyse détaillée du droit des fiducies du Québec afin de déterminer s'il permettrait l'établissement d'une fiducie qui correspondra aux critères établis.

À cet égard, il importe de souligner d'emblée que le droit québécois reflète très bien les obligations qu'implique typiquement la charge de fiduciaire ainsi que le principe de gouvernance responsable tel qu'explicité dans la deuxième partie de ce rapport. Notamment, le fiduciaire est tenu d'agir de manière impartiale et indépendante, avec la prudence et diligence d'une personne raisonnable placée dans les mêmes circonstances, et ce toujours avec honnêteté et loyauté envers la finalité de la fiducie et les meilleurs intérêts de celle-ci. Il sera aussi redevable pour la qualité de son administration envers les bénéficiaires ainsi que les tierces parties, et ce malgré toute stipulation contraire, les obligations qui imposent au fiduciaire étant d'ordre public.

Le fiduciaire sera aussi tenu à certaines charges en vertu du régime de la pleine administration du bien d'autrui, et comme il sera vu dans la prochaine section, celles-ci ne poseront pas de conflit avec ce qui serait attendu d'un fiduciaire chargé d'administrer un patrimoine composé de données. En effet, l'orientation première de la charge de la pleine administration est *la finalité de la fiducie* ; les obligations qui en découlent seront donc interprétées en fonction de la seule réalisation de cette dernière, toute obligation contraire pouvant alors être écartée pour autant que cette finalité soit licite.

Le régime québécois prévoit en outre des mécanismes de surveillance et de contrôle de l'administration fiduciaire, ce qui renforce davantage le principe de gouvernance responsable. Le mécanisme de surveillance institutionnelle des fiducies d'utilité sociale (FUS) par les « personnes ou organismes désignés par la loi » est notamment intéressant eu égard aux préoccupations soulevées quant à une telle charge qui serait possiblement imposée au fiduciaire et qui serait alors un usage inapproprié des ressources de la fiducie. En effet, ce mécanisme évacue cette préoccupation en prévoyant déjà la surveillance institutionnelle. Malheureusement par contre, ses promesses sont anéantis par le fait que le mécanisme demeure largement inopérant : il ne s'agit que d'un simple renvoi, aucune loi n'existant à ce jour prévoyant l'existence d'un tel organisme autre que la *Loi sur les sociétés de fiducie et les sociétés d'épargnes*<sup>151</sup> qui s'applique principalement aux sociétés de fiducie se livrant à des activités d'institution financière. Une fiducie de données ne bénéficierait ainsi d'aucune surveillance institutionnelle ; elle devra plutôt se contenter des autres mécanismes prévus par le *Code civil du Québec (CcQ)*<sup>152</sup>, soit, la surveillance du constituant, du bénéficiaire, et de toute autre personne intéressée. Des mécanismes supplémentaires pourraient par contre aussi être prévus dans l'acte constitutif ; par exemple, des vérifications périodiques de la conformité avec les normes et procédures établis pour la gestion des données de la fiducie.

Les prochaines sections verront ces points en détail. Sera aussi vu en détail la possibilité qu'offre le droit québécois de tenir les tiers responsables advenant une utilisation défaillante des données auxquelles ils furent accordés un droit d'usage. Comme il sera vu, ceci s'opèrera majoritairement par la voie du droit contractuel, en exécution des divers contrats qui seront établis pour régir l'utilisation des données. La flexibilité du véhicule de la fiducie québécoise permettra que de tels contrats soient intégrés dans la structure même de la fiducie. D'ailleurs, la flexibilité du véhicule sera aussi analysée en détail, spécifiquement au niveau de sa constitution, des possibilités d'y apporter des modifications, et de ses modalités d'extinction. Eu égard aux critères établis ci-haut, il deviendra clair que le droit québécois offre un degré suffisant de flexibilité à la fiducie sans toutefois être trop permissif de sorte qu'elle risque être complètement dénaturée de son affectation originale. En effet, elle est relativement facile à constituer, n'exigeant aucune formalités autre que celles s'appliquant à la nature de l'acte constitutif en question. Il est toutefois fortement recommandé que sa constitution soit attestée par un écrit, vu le niveau de détail qu'il sera nécessaire de mettre en relief quant à sa finalité, sa structure de gouvernance, et les normes et procédures encadrant la gestion des données, incluant le partage de celles-ci. L'écrit permettra d'établir des balises claires quant aux responsabilités du fiduciaire et évitera toute confusion quant à celles-ci advenant un litige.

Cette section se terminera par une analyse des trois grandes catégories de fiducie prévu en droit québécois : la fiducie personnelle, la fiducie d'utilité privée (FUP), et la fiducie d'utilité sociale (FUS). Étant donné l'importance du critère qu'une fiducie de données soit affecté à l'intérêt public et représente les valeurs de réciprocité et de non-exploitation, seules la FUS et la FUP à vocation non-commerciale et sans bénéficiaires directs ont été retenus comme convenables pour constituer une fiducie de données. Les deux peuvent exister sans bénéficiaires et peuvent être à durée perpétuelle, ce qui sera nécessaire dans le cas d'une fiducie de données vu l'importance de veiller à la sécurité des données pendant la vie entière de la fiducie. L'absence de bénéficiaires assurera que les données qui composent le patrimoine fiduciaire ne seront jamais aliéner de celui-ci. Aussi, la FUS est par définition affectée à une finalité d'intérêt général, mais la FUP peut l'être aussi, bien que de manière indirecte. Comme il sera vu plus loin, la variante non-commerciale et sans bénéficiaire de cette dernière est constituée principalement dans le but de procurer un avantage indirect à une personne ou à un groupe de personnes désignées. Ces personnes pourraient très bien être les « scientifiques ou chercheurs » désignés de façon large comme pouvant jouir de l'avantage d'utiliser les données détenus par la fiducie. Ensuite, des balises précises

151 RLRQ c S-29.02.

152 RLRQ c CCQ-1991 [CcQ].

quant aux usages qu'ils pourront en faire pourraient s'occuper de l'aspect d'intérêt public. Par exemple, en consacrant dans les ententes d'usager qu'ils ne pourront utiliser les données qu'à des fins d'intérêt public. Autrement, il ne suffirait que de mener une campagne de sensibilisation du public afin d'inspirer confiance à celui-ci que la fiducie est réellement affectée à une finalité d'intérêt public.

Ainsi, à tout égard, le droit québécois des fiducies semble très bien correspondre aux critères établis dans la deuxième partie de ce rapport pour la constitution d'une fiducie de données dans le domaine de la santé.

Ceci étant dit, elle ne sera pas à l'abri des exigences se rapportant au consentement ni celles qu'impose la loi quant au partage et à l'utilisation des données ; elle devra dans tous les cas se conformer aux exigences légales en vigueur. Elle sera non plus à l'abri d'une culture d'aversion au risque généralisé quant au partage des données médicales ; si tel s'avère être le cas au Québec, elle devra entreprendre les efforts nécessaires pour sensibiliser le public et lui inspirer confiance quant à ses activités. Elle aura aussi à composer avec les autres défis précités, tels les défis d'ordre logistique, le problème de fragmentation, l'incongruence inter-juridictionnelle, et la difficulté de garantir un droit à la révocabilité du consentement ou au transfert des données. Elle ne connaîtra toutefois pas de défis en lien avec un délai de constitution : comme il sera vu plus loin, la fiducie québécoise peut être constituée sans formalités et existe du moment que le fiduciaire accepte son mandat d'administration de la fiducie. Aussi, tel que noté, elle peut tout à fait exister sans bénéficiaire nommé et revêt une flexibilité suffisante pour lui permettre de s'adapter aux changements qui surviendront. Le pouvoir accordé au fiduciaire d'ester en justice pour tout ce qui concerne la protection des intérêts de la fiducie fournit aussi un mécanisme concret qui permettra le contrôle des tiers quant à l'usage qu'ils feront des données partagées. La surveillance de ces derniers serait tout de même à prévoir, le droit québécois des fiducies ne prévoyant aucun mécanisme par défaut à cet effet. Il y aurait ainsi la même incertitude quant à savoir si un tel rôle devrait être imposé au fiduciaire ou non. Autrement, la fiducie québécoise serait non plus à l'abri des problèmes de financement observés dans les autres banques de données de la santé et les biobanques.

Quant au seul obstacle potentiellement fatal à la constitution d'une fiducie de données en droit québécois, comme il sera vu plus loin, la fiducie québécoise ne s'y échappera pas : son patrimoine, bien qu'étant un patrimoine d'affectation sans titulaire quelconque, est néanmoins composé de *biens*, qui sont par définition des choses appropriables. Or, l'état actuel du droit québécois – en considérant les données personnelles comme rattachées au droit à la vie privée – laisse vraisemblablement entendre que les données personnelles sont de nature extrapatrimoniale, et ne sont donc pas appropriables. Ainsi, ni les données en tant que tel, ni un droit d'usage quelconque sur celles-ci ne pourrait être 'transférés' au patrimoine fiduciaire comme le veut la condition *sine qua non* de la constitution d'une fiducie en droit québécois. Ceci devra donc être considéré avec soin avant d'entreprendre un projet de fiducie de données au Québec puisqu'advenant un litige, on risque de ne pas reconnaître une telle entité à titre de fiducie faute de rencontrer les critères pour sa constitution. Ceci aurait des implications importantes au niveau des mécanismes qui demeureraient disponibles pour tenir soit le 'fiduciaire', soit les tiers responsables d'un préjudice quelconque.

## A. Les obligations fiduciaires et le principe de gouvernance responsable

### 1. Le rôle du fiduciaire : administrateur du bien d'autrui chargé de la pleine administration

Le fiduciaire est la personne (physique ou morale) chargée de détenir et d'administrer le patrimoine fiduciaire aux fins stipulées dans l'acte constitutif. Il a la maîtrise et l'administration exclusive du patrimoine fiduciaire<sup>153</sup> et sa mission première sera de réaliser l'affectation de la fiducie. Pour se faire, il sera assujéti, dès son acceptation du mandat de fiduciaire, au régime de la pleine administration du bien d'autrui du *Code civil*<sup>154</sup> et dès lors, il sera chef en tête de cette mission et redevable pour la qualité de son administration.

Son obligation principale en tant qu'administrateur sera de veiller à l'administration des biens ainsi qu'à la réalisation de la finalité de la fiducie.<sup>155</sup> Il sera aussi, en principe, chargé de conserver le patrimoine fiduciaire, de le faire fructifier, et, soit de l'accroître, soit de l'administrer en vue de réaliser l'affectation de la fiducie.<sup>156</sup>

L'obligation de conserver ne sera pas incompatible avec ce qui serait attendu d'une fiducie de données dans le domaine de la santé. En effet, la conservation des données, afin qu'elles puissent servir aux fins établies par la fiducie, sera une de ses principales raisons d'être.

L'obligation de conserver comprend notamment l'obligation d'entreprendre toute action nécessaire ou utile au maintien de l'usage du bien composant le patrimoine fiduciaire<sup>157</sup> selon les usages prescrites par l'acte constitutif et l'affectation de la fiducie.<sup>158</sup> Donc si, par exemple, l'usage utile des données est défini, dans l'acte constitutif, comme comprenant le partage efficace et efficient de celles-ci à x fins, et que ceci implique nécessairement que les données soient entreposées, répertoriées, formatées, etc. selon des normes et standards définis, l'obligation de conserver pourrait comprendre la conservation des données en ce sens. La conservation pourrait aussi impliquer un volet de sécurité des données si un des objectifs est la protection de la vie privée. Cette obligation s'avérerait donc très intéressante pour la constitution d'une fiducie de données dans le domaine de la santé au Québec.

En ce qui a trait à l'obligation de faire fructifier, celle-ci ne devrait non plus poser de problèmes. Bien que la fructification s'entend normalement de l'action de faire produire un bénéfice avec un souci de rentabilité,<sup>159</sup> le fiduciaire y serait seulement tenu dans la mesure que la poursuite du but de la fiducie l'exigent.<sup>160</sup> Une fiducie de données dans le domaine de la santé sera vraisemblablement à vocation non commerciale et affectée à un intérêt public, donc l'obligation de faire fructifier tomberait simplement, faute de compatibilité avec le but de la fiducie. Néanmoins, l'obligation de faire fructifier pourrait aussi être interprétée comme une simple obligation d'augmenter les bénéfices retirés des données détenues en fiducie, sans souci pour la rentabilité. Par exemple, si une fiducie de données a comme double objectif de faciliter le partage des données tout en assurant la protection des intérêts individuels et collectifs, l'obligation de faire fructifier pourrait se traduire en une obligation d'assurer que les données soient mises à l'emploi à des fins utiles, en conformité avec ce qui est stipulé comme fins prescrites dans l'acte constitutif. Ainsi, les « bénéfices retirés des données » seraient augmentés sans égard à une rentabilité quelconque.

153 CcQ, supra note 152 art 1278 al 1.

154 Ibid art 1278 al 2.

155 Ibid art 1265.

156 Ibid art 1306.

157 Ferland (Succession de Ferland) c Albert, 2019 QCCS 98.

158 Jacques Beaulne, *Droit des fiducies*, 3e éd. (Montréal, Wilson et Lafleur, 2015) au para 295 [Beaulne, « Droit des fiducies »].

159 Ministère de la Justice, *Commentaires du ministre de la Justice - Le Code civil du Québec*, t 1, Québec, Les Publications du Québec, 1993, art 1306.

160 CcQ, supra note 152 art 1306 in fine.

En ce qui concerne l'obligation d'accroître le patrimoine, puisque celle-ci serait incompatible avec une fiducie de données dans le domaine de la santé, elle serait simplement écartée au profit de son alternatif, soit, l'obligation d'administrer les données en vue de réaliser l'affectation de la fiducie.<sup>161</sup>

## 2. Les obligations qui imposent au fiduciaire

Le régime de la pleine administration accordée au fiduciaire des pouvoirs larges mais ceux-ci ne sont pas sans limites.

Premièrement, le fiduciaire doit toujours agir en conformité avec la loi ainsi que les obligations et limites qui lui sont imposés par l'acte constitutif.<sup>162</sup> Notamment en ce qui a trait à la loi, celle-ci lui impose non seulement le respect de toute loi, de tout règlement ou de toute autre stipulation légale se rapportant à la protection des données personnelles et du droit à la vie privée (ex. les exigences se rapportant au consentement, à la collecte et à la communication des données personnelles), mais aussi tout ce qui se rapporte à la charge de la pleine administration du bien d'autrui, soit, les obligations générales d'agir avec impartialité,<sup>163</sup> prudence, diligence, honnêteté et loyauté, et ce toujours dans le meilleur intérêt du bénéficiaire ou de la fin poursuivie par la fiducie.<sup>164</sup> Ces obligations sont *d'ordre public* et s'appliquent ainsi malgré toute stipulation contraire.<sup>165</sup> L'acte constitutif ne saurait alors en disposer autrement par une clause exonératoire de responsabilité<sup>166</sup> ; toute clause à l'effet contraire serait simplement prononcée nulle de nullité absolue et réputée non écrite. Ainsi que les prescriptions comprises dans l'acte constitutif, bien qu'elles dicteront en plus grand détail en quoi consiste le mandat du fiduciaire, devront toujours respecter ces plus grandes obligations de principe imposées au fiduciaire.

En ce qui concerne l'obligation d'agir avec impartialité, celle-ci s'applique à l'égard des bénéficiaires et exige que le fiduciaire évite d'agir d'une manière susceptible d'être favorable à un ou certains bénéficiaires au détriment des autres. Cette obligation sera alors impertinente à une fiducie de données puisque celle-ci sera vraisemblablement sans bénéficiaires.

En ce qui a trait aux obligations de prudence et de diligence, celles-ci s'appliquent à l'exécution même du mandat du fiduciaire, qui inclut la charge de la pleine administration ainsi que toutes les prescriptions stipulées dans l'acte constitutif. Il s'agit notamment d'une obligation de *moyens*, appréciée selon la norme de conduite objective et abstraite de la personne normalement avisée, placée en semblables circonstances.<sup>167</sup> L'appréciation de la qualité de l'administration du fiduciaire aura donc tendance à varier selon les circonstances particulières en question.

Il y a un certain débat à savoir si cette appréciation varierait aussi en fonction du niveau d'expertise ou des connaissances d'un fiduciaire en particulier. Par exemple, advenant qu'il faille soulever la responsabilité du fiduciaire pour une faute quelconque, serait-il permis de tenir compte de son niveau d'expertise en gestion des données personnelles afin d'apprécier la gravité de sa faute et la proportion dans laquelle il sera tenu responsable ?

Selon le professeur Jacques Beaulne, la réponse serait oui. Si le fiduciaire possède en outre une compétence particulière dans la gestion des biens en question, la norme de référence précitée permettrait qu'on en tienne compte et que soit appliquée une norme d'un gestionnaire professionnel de données personnelles.<sup>168</sup> Ceci n'est pas toutefois certain vu les enseignements de l'arrêt *Peoples*.<sup>169</sup> En effet, ce que le professeur Beaulne propose ressemble davantage à l'analyse « objective subjective » qui pré-

161 Ibid art 1306 ; l'article 1306 CcQ le justifierait également.

162 Ibid art 1308 al 1.

163 Ibid art 1317.

164 Ibid art 1309 ; Commentaires du ministre, supra note 159 art 1309.

165 Bell c Molson, 2015 QCCA 583 aux para 90-91.

166 Ibid aux para 96-98.

167 Commentaires du ministre, supra note 159 art 1309.

168 Beaulne, « Droit des fiducies », supra note 155 au para 305.

169 Magasins à rayons Peoples inc. (Syndic de) c. Wise, [2004] 3 RCS 461.

valait antérieurement à cet arrêt, alors que depuis, c'est plutôt l'analyse de la norme objective qui doit prévaloir, cette dernière ne demandant normalement pas de tenir compte des compétences, aptitudes ou caractéristiques personnelles d'un administrateur donné, mais plutôt simplement des circonstances relatives à son rôle et à sa position au sein de la société.<sup>170</sup> Par exemple, il serait admis, selon cette norme, de tenir compte des connaissances *normalement différentes* entre des administrateurs internes et externes, puisque ceci dépend de circonstances externes à la personne en soi et serait donc véritablement une analyse objective. Ainsi il n'est pas certain qu'un fiduciaire particulièrement bien formé pour la gestion de données personnelles soit désavantagé par son expertise au niveau de sa responsabilité. Soit qu'il serait, selon la position du professeur Beaulne, tenu à un plus haut standard équivalent à celui de son niveau d'expertise, soit qu'il ne serait tenu qu'à un standard jugé raisonnablement adéquat eu égard aux circonstances et au rôle d'un fiduciaire de données en général.

En ce qui a trait aux obligations d'agir avec honnêteté et loyauté, et ce toujours dans le meilleur intérêt du bénéficiaire ou de la fin poursuivie par la fiducie, celles-ci sont fondamentales et orientent l'ensemble des activités du fiduciaire. Elles impliquent notamment l'obligation de toujours agir « en bon père de famille »<sup>171</sup> et aussi d'éviter tous conflits d'intérêt, non seulement en ne choisissant jamais son intérêt personnel au détriment de celle de la fiducie, mais également en évitant de se placer dans une situation où il aurait à choisir entre les deux.<sup>172</sup> Ces obligations se traduiraient, par exemple, en l'obligation de donner au bénéficiaire tous les renseignements utiles susceptibles d'influer sur la volonté du fiduciaire de maintenir l'administration, de la modifier, ou d'y mettre fin (nous verrons plus loin les modifications qu'il est possible d'apporter à la fiducie incluant ce qui peut l'éteindre).<sup>173</sup> Il ne doit aussi jamais prendre les biens fiduciaires de la fiducie pour le siens<sup>174</sup> ni les utiliser à son profit.<sup>175</sup>

Finalement, en ce qui a trait à l'indépendance du fiduciaire, celle-ci va de soi avec la nature de son rôle : il a la maîtrise entière et exclusive du patrimoine de la fiducie dès l'acceptation de son mandat.<sup>176</sup> Aussi dès lors, le constituant sera complètement dessaisi des biens transférés en fiducie<sup>177</sup> et personne ne détiendra de droit réel sur ces derniers – ni le constituant, ni le fiduciaire, ni le bénéficiaire.<sup>178</sup> En effet, le patrimoine fiduciaire est un véritable patrimoine d'affectation sans titulaire quelconque.

Ces obligations correspondent ainsi très bien avec le principe de gouvernance responsable qui serait attendu d'une fiducie de données. Le fiduciaire agira de manière impartiale et indépendante et sera tenu d'être prudent et diligent dans son administration et toujours honnête et loyal envers la finalité de la fiducie et les meilleurs intérêts de celle-ci. Il sera aussi redevable pour la qualité de son administration, et ce malgré toute stipulation contraire. Qui pourra par contre le tenir responsable en cas d'une administration défailante ? La prochaine section examine cette question en détail.

170 Jean-Philippe Latreille et Emmanuel Sala, « La diligence raisonnable : une norme en évolution », *Ratio*, Lavery, no 27, 2015.

171 Commentaires du ministre, *supra* note 159 art 1309.

172 CcQ, *supra* note 152 art 1310 al 1.

173 Commentaires du ministre, *supra* note 159 art 1309.

174 CcQ, *supra* note 152 art 1313.

175 *Ibid* art 1314.

176 *Ibid* art 1278 al 1, 1265.

177 *Ibid* art 1265.

178 *Ibid* art 1261.

### 3. Le droit d'action en cas d'administration défailante du fiduciaire

Le droit d'action en cas d'administration défailante du fiduciaire à l'une ou l'autre de ses obligations est bien défini lorsqu'il y a un bénéficiaire dans le dessin de la fiducie. En effet, lorsqu'un bénéficiaire subit un préjudice d'une administration défailante du fiduciaire, il pourra tenir ce dernier personnellement responsable<sup>179</sup> et obtenir des dommages-intérêts à titre de réparation s'il y a lieu.<sup>180</sup>

Le *Code civil* est toutefois moins clair lorsqu'il s'agit de reconnaître un tel droit à un tiers. Par exemple, advenant une brèche de sécurité aux données causée par une administration négligente du fiduciaire, et compromettant ainsi la vie privée de toutes les personnes fichées, le fiduciaire pourrait-il être tenu personnellement responsable de réparer les dommages subis par ces personnes ?

Le *Code civil* n'accorde pas explicitement un droit d'action aux tiers pour poursuivre le fiduciaire en justice.

Il prévoit que le fiduciaire sera personnellement responsable lorsqu'il agit en excès de ses pouvoirs ou par une administration clandestine.<sup>181</sup> Il accorde aussi un droit de surveillance explicite au constituant, au bénéficiaire (s'il y a), et à toute autre personne intéressée de contraindre le fiduciaire à exécuter ses obligations ou à faire un acte nécessaire à la fiducie, ou encore de l'enjoindre à s'abstenir de tout acte dommageable à la fiducie.<sup>182</sup> Ces mêmes personnes peuvent aussi saisir le tribunal pour obtenir la destitution d'un fiduciaire défailant<sup>183</sup> ou pour attaquer les actes faits par le fiduciaire en fraude du patrimoine fiduciaire ou des droits du bénéficiaire.<sup>184</sup> Mais il ne dit rien à l'effet d'un droit explicite reconnu aux tiers de le poursuivre en justice afin d'obtenir réparation en raison d'une administration fautive.

Malgré le silence du *Code civil* à cet égard, la jurisprudence confirme qu'il est possible de tenir un fiduciaire personnellement responsable pour une administration défailante, même alors qu'il agit à l'intérieur de ses pouvoirs. Ceci est confirmé par un jugement rendu par la Cour du Québec en 2009<sup>185</sup> ainsi que par la Cour d'appel en 2015<sup>186</sup>. Le professeur Sylvio Normand est aussi du même avis :

---

*« [Le fiduciaire] n'est pas personnellement responsable à l'égard des tiers. Toutefois, il peut engager sa responsabilité personnelle lorsqu'il ne respecte pas les obligations auxquelles il est tenu par la loi (1309 C.c.Q.) ou lorsqu'il excède ses pouvoirs (1319-1320 C.c.Q.) ».*<sup>187</sup>

---

Le droit d'action des tiers s'opèrera donc vraisemblablement par le truchement de la responsabilité extracontractuelle ; les tierces personnes ayant subi un préjudice en raison d'une administration défailante d'un fiduciaire devraient pouvoir poursuivre ce dernier en justice pour obtenir réparation en vertu du régime de la responsabilité civile extracontractuelle. Aussi, pour les préjudices impliquant une atteinte à un droit protégé par les lois sur les renseignements personnels, les tiers auraient aussi vraisemblablement toujours un droit d'action en vertu de ces lois d'obtenir une réparation pour le préjudice subi.

179 Ibid art 1322 : « Le bénéficiaire ne répond envers les tiers du préjudice causé par la faute de l'administrateur dans l'exercice de ses fonctions qu'à concurrence des avantages qu'il a retirés de l'acte. En cas de fiducie, ces obligations retombent sur le patrimoine fiduciaire ».

180 Ibid art 1318.

181 Ibid aux art 1319, 1320

182 Ibid art 1290 al 1.

183 Ibid.

184 Ibid art 1290 al 2.

185 9098-6159 Québec inc. c Fiducie familiale Mailhot, 2009 QCCQ 1954, dispositif : le fiduciaire qui commet une faute dans l'exercice de ses fonctions peut être poursuivi personnellement.

186 Bell c Molson, 2015 QCCA 583, au para 138 : « un administrateur doit être poursuivi personnellement si on lui réclame des dommages-intérêts pour une faute dans son administration », citant les propos des auteurs Madeleine Cantin-Cumyn et Michelle Cumyn dans *L'administration du bien d'autrui* (Cowansville : Édition Yvon Blais inc., 2014) à la p 387.

187 Sylvio Normand, *Introduction au droit des biens*, 3e éd (Montréal : Wilson & Lafleur, 2020) à la p 464 : « [Le fiduciaire] n'est pas personnellement responsable à l'égard des tiers. Toutefois, il peut engager sa responsabilité personnelle lorsqu'il ne respecte pas les obligations auxquelles il est tenu par la loi (1309 C.c.Q.) ou lorsqu'il excède ses pouvoirs (1319-1320 C.c.Q.) ».

Le principe de gouvernance responsable semble donc bien enraciné en droit québécois des fiducies. Le droit de surveillance reconnu non seulement au constituant mais à toute autre personne intéressée permettra d'assurer, pour autant qu'il soit exercé efficacement, que le fiduciaire exécute ses obligations conformément à ce qui lui est attendu. L'acte constitutif pourrait inclure à cet égard des modalités spécifiques quant à l'exercice de ce pouvoir de surveillance, justement afin d'assurer qu'il soit adéquatement mis à l'emploi. Autrement, advenant qu'une surveillance faille à détecter une administration fautive, il sera néanmoins toujours possible de tenir le fiduciaire personnellement responsable, dans la mesure qu'il agissait contrairement aux obligations qui lui sont imposées soit par la loi, soit par l'acte constitutif.

## B. Les mesures de contrôle et de surveillance

Outre les obligations explicitées ci-haut, le *Code civil du Québec* prévoit aussi un certain nombre de mesures de contrôle et de surveillance qui permettront d'encadrer davantage l'administration fiduciaire.

### 1. L'inventaire, la reddition de compte et la garantie (assurances-responsabilité)

L'inventaire, la reddition de compte et la garantie pourraient servir à titre d'outils supplémentaires pour améliorer le contrôle d'une fiducie de données.

L'inventaire et la reddition de compte sont des outils de nature statique qui permettront de fournir aux intéressés un portrait de l'administration de la fiducie à un moment précis. Pour l'inventaire, il s'agit d'une liste complète de tous les biens qui composent le patrimoine fiduciaire. Il *peut* être constitué dès la création de la fiducie et *peut* être mis à jour à une fréquence désirée tout au long de la vie de la fiducie. En effet, tenir inventaire n'est pas obligatoire et devra donc être prévu – incluant ses modalités – dans l'acte constitutif.<sup>188</sup> Sinon, il peut aussi être demandé par un bénéficiaire ou par toute autre personne intéressée.<sup>189</sup> Son utilité repose en la capacité de mieux détecter un détournement ou une aliénation interdite des biens de la fiducie, et de le prouver le cas échéant.<sup>190</sup> Il serait donc utile à cet effet pour maintenir un contrôle adéquat sur les données personnelles qui composeraient éventuellement le répertoire d'une fiducie de données.

En ce qui a trait à la reddition de compte, celle-ci s'agit essentiellement d'un portrait comptable de la fiducie. Elle est obligatoirement présentée annuellement<sup>191</sup> ainsi qu'à la fin de la fiducie,<sup>192</sup> mais peut aussi être demandée à tout moment pendant sa durée.<sup>193</sup> Elle sera typiquement présentée au bénéficiaire,<sup>194</sup> mais en l'absence de bénéficiaires – dans le cas d'une FUS par exemple – il est raisonnable de penser que l'acte constitutif pourra en prévoir autrement. Bien que ne rajoutant rien à l'égard du contrôle sur les données personnelles, il s'agirait tout de même d'un outil utile pour le contrôle de l'administration de la fiducie en général.

188 CcQ, supra note 152 art 1324.

189 Ibid.

190 Beaulne, « Droit des fiducies », supra note 155 au para 366.

191 CcQ, supra note 152 art 1351.

192 Ibid art 1363 al 1.

193 Ibid art 1364.

194 Ibid art 1363 al 1.



Pour ce qui est de la garantie, celle-ci constitue plutôt une mesure de protection du patrimoine de la fiducie contre une administration défaillante du fiduciaire, et ce tout au long de la durée de la fiducie. Elle est intéressante puisque comme le remarque le professeur Beaulne, même s'il est vrai que le fiduciaire est responsable de sa négligence et de ses fautes, il est souvent illusoire de penser que les dégâts puissent véritablement être réparés.<sup>195</sup> La garantie permettrait donc de souscrire, par exemple, une assurance-responsabilité pour compenser les dommages le cas échéant.<sup>196</sup> Elle devra toutefois être imposé au fiduciaire par une stipulation à cet effet dans l'acte constitutif, n'étant que purement facultative.<sup>197</sup> Cette option serait intéressante notamment pour les fiducies de données, puisque les dommages en lien avec les fuites de données sont généralement importants.

## **2. Les pouvoirs de surveillance du constituant, du bénéficiaire et de toute autre personne intéressée**

Les mesures de surveillance que prévoit le *Code* sont de deux sortes : les mesures générales applicables à toute fiducie, et celles spécialement prévues pour les fiducies d'utilité privée (FUP) et les fiducies d'utilité sociale (FUS).

En ce qui a trait aux mesures applicables à toute fiducie, celles-ci se retrouvent aux articles 1290 et 1291 CcQ et constituent essentiellement des pouvoirs de surveillance et de contrôle accordés au constituant, au bénéficiaire ainsi qu'à toute autre personne intéressée. Pour l'article 1290 CcQ, celui-ci est d'ordre public et permet, tel que mentionné ci-haut, à ces derniers d'agir contre le fiduciaire pour soit le contraindre à exécuter ses obligations ou à faire un acte nécessaire, soit l'enjoindre de s'abstenir de tout acte dommageable à la fiducie, ou encore, pour obtenir sa destitution ou attaquer ses actes fait en fraude du patrimoine fiduciaire ou des droits des bénéficiaires. L'article 1291 CcQ permet plutôt au tribunal d'autoriser les prénommées d'agir à la place du fiduciaire, dans les cas où, sans motif suffisant, il refuse ou néglige d'agir ou en est empêché.

## **3. La surveillance « des personnes et organismes désignés par la loi »**

Pour ce qui sont des mesures applicables spécialement aux FUP et FUS, *en outre* des mesures générales, ces espèces de fiducie sont aussi soumises à la surveillance « des personnes et organismes désignés par la loi ». <sup>198</sup> En concret il s'agit d'un régime de surveillance institutionnelle ambitieux avec beaucoup de potentiel, mais qui, malgré ses aspirations, demeure à présent largement inopérant vu la quasi-inexistence totale de telles lois désignant ces dites personnes et organismes.<sup>199</sup> Au moment de l'écriture du présent rapport, un seul exemple d'une telle loi fut retrouvé,<sup>200</sup> soit la *Loi sur les sociétés de fiducie et les sociétés d'épargne*<sup>201</sup>, qui s'applique aux sociétés de fiducie se livrant à des activités d'institution financière.

195 Beaulne, « Droit des fiducies », supra note 155 au para 364.

196 CcQ, supra note 152 aux art 2498-2504.

197 Ibid art 1324 ; Beaulne, « Droit des fiducies », supra note 155 au para 364.

198 Ibid art 1287 al 2.

199 Ceci est selon les observations contenu dans la plus récente édition de l'ouvrage *Droit des fiducies* du professeur Jacques Beaulne, qui date de 2015. Une recherche exhaustive ne fut toutefois effectuée donc une mise à jour s'imposerait où pertinent.

200 Ibid.

201 RLRQ c S-29.02.

Ces mesures sont intéressantes pour assurer une surveillance adéquate du fiduciaire. Pris en compte avec les obligations fiduciaires qui imposent au fiduciaire, la fiducie québécoise semble effectivement pouvoir bien intégrer un principe fort adéquat de gouvernance responsable pour la gouvernance des données. Toutefois, ces mesures n'ajoutent rien à la préoccupation non moins importante de surveiller les bénéficiers-usagers à qui l'on accordera accès aux données. Ces mesures devront donc largement s'opérer par la faculté d'élire du fiduciaire, la stipulation d'inaliénabilité ainsi que les conditions d'accès et d'utilisation des données imposées aux bénéficiaires, et les pouvoirs reconnus au fiduciaire d'entreprendre toute action nécessaire à protéger les intérêts de la fiducie, par exemple, de révoquer un droit d'accès à un bénéficiaire défaillant ou même de le poursuivre en justice si nécessaire et approprié. Comme il fut soulevé plus haut, l'on pourrait alors penser à intégrer des devoirs de surveillance dans l'acte constitutif, tels des audits périodiques. Ces devoirs pourraient être imposés au fiduciaire, ou à un comité de fiduciaire, ou à tout autre entité établi dans le cadre de la structure de gouvernance de la fiducie.

À ces égards, la fiducie québécoise semble pouvoir s'accorder très bien avec les besoins de surveillance et de contrôle explicités ci-haut.

### C. La responsabilité des tiers

Il y aussi lieu de se questionner sur la responsabilité des tiers advenant qu'ils utiliseraient les données de la fiducie à des fins autres que celles permises par la fiducie.

Les tiers devront être accordés accès et usage des données selon des conditions prescrites dans l'acte constitutif de la fiducie. Celles-ci permettront au fiduciaire de déterminer qui exactement pourra obtenir accès aux données, sous quelles conditions, pour quelles fins, etc. Ces prescriptions (dans la mesure qu'elles sont pertinentes) devront aussi être transcrites dans les contrats d'accès et d'utilisation des données qui seront conclus avec les usagers éventuels. Il pourrait s'agir, par exemple, d'ententes d'utilisation, d'un code de conduite, d'une combinaison de ces derniers, ou de tout autre forme de contrat pour autant que les obligations des usagers soient clairement définis et consentis. Se faisant, le fiduciaire sera plus à même d'exercer avec efficacité son pouvoir d'ester en justice au nom de la fiducie pour toute action visant à protéger les intérêts de la fiducie. En effet, le *Code civil* lui reconnaît ce pouvoir, qui lui permet d'exercer tous les droits qu'un propriétaire pourrait exercer afin de protéger ses biens, ainsi que tout recours contre les actes susceptibles de nuire à l'accomplissement de la fin poursuivie par la fiducie, y compris les recours en injonction.<sup>202</sup> Rappelons aussi que s'il néglige ou est empêché d'agir alors qu'il serait nécessaire, le constituant, un autre bénéficiaire ou toute autre personne intéressée pourra obtenir l'autorisation du tribunal pour ester en sa place.<sup>203</sup>

Qui plus est, il sera aussi possible d'inclure une stipulation d'inaliénabilité dans l'acte constitutif pour davantage contrôler le repartage des données par les usagers autorisés. Selon le professeur Jacques Beaulne, ceci sera possible en autant que la fiducie ait été constituée à titre gratuit,<sup>204</sup> et elle demeurerait valide pour toute la durée de la fiducie.<sup>205</sup> Il sera par contre nécessaire de publier cette stipulation pour la rendre opposable aux tiers.<sup>206</sup> Ainsi, dans l'éventualité qu'un usager céderait à un tiers son droit d'utiliser les données de la fiducie, il sera premièrement tenu responsable en vertu de son contrat d'utilisation, qui interdira le repartage aux tiers non autorisés, et la stipulation d'inaliénabilité permettra en outre de garder les données hors la portée du tiers non autorisé, qu'il ait été de bonne foi ou non.

202 Commentaires du ministre, supra note 159 art 1316 ; Beaulne « Droit des fiducies », supra note 155 au para 302.

203 CcQ, supra note 152 art 1291.

204 Ibid art 1212.

205 Ibid art 1212 al 3 in fine ; Beaulne « Droit des fiducies », supra note 155 au para 260.

206 Ibid art 1214, 2649 ; Beaulne « Droit des fiducies », supra note 155 au para 262.

## D. La versatilité et flexibilité du véhicule en général

### 1. Versatilité et flexibilité au niveau de la constitution de la fiducie

En ce qui a trait à la versatilité et la flexibilité du véhicule, le droit québécois semble bien se prêter à ces critères.

D'abord, la fiducie québécoise est relativement facile à constituer. Elle peut être établie par contrat (à titre gratuit ou onéreux), par testament, par la loi ou, lorsque la loi l'autorise, par jugement.<sup>207</sup> Dans le cas d'une fiducie de données, l'établissement pourrait donc se faire par contrat, vraisemblablement à titre gratuit vu la nature non patrimoniale des données.

Ensuite, selon la Cour suprême du Canada dans l'arrêt *Banque de Nouvelle-Écosse c Thibaut*,<sup>208</sup> il n'y a que trois éléments essentiels à la constitution d'une fiducie au Québec :

1. Le transfert des biens du patrimoine d'une personne à un patrimoine d'affectation
2. L'affectation des biens à une fin particulière
3. L'acceptation par un fiduciaire

Ces critères sont largement une reprise de celles énoncées aux articles 1260 à 1264 CcQ.

La consécration de sa constitution dans un écrit n'est donc pas absolument nécessaire, mais est tout de même fortement recommandée afin que puissent être clairement définis toutes les modalités de la fiducie, l'identité du / des fiduciaire(s), leurs devoirs et obligations, les normes et standards qui devront être respectés pour l'entreposage et le partage des données, les critères de sélection des usagers, les modalités de sélection des usagers (ex. approbation de la proposition de recherche par un comité d'éthique formellement intégré à la structure de la fiducie), etc. En effet, à la lumière de ce qui fut mis en relief dans la première partie de ce rapport, la constitution d'une fiducie de données – surtout dans le domaine de la santé – n'est pas à approcher à la légère si le résultat désiré est véritablement une gouvernance *responsable* des données. L'architecture de sa structure devra être bien pensée vu le critère voulant une gouvernance participative et collaborative ainsi que les contrats connexes qui relèveront de sa structure pour contrôler l'usage des données par les tiers autorisés. Vu la complexité de la tâche il serait alors fort préférable que le tout soit circonscrit dans un écrit. Ainsi l'acte constitutif lui-même constituerait cet écrit.

Celui-ci ne serait soumis à aucunes formalités sauf celles s'appliquant à la nature de l'acte en question.<sup>209</sup> Ainsi, puisqu'une fiducie de données dans le domaine de la santé sera vraisemblablement constituée par donation, son acte constitutif devra se conformer aux règles de formes de l'acte de donation.

Pour ce qui est du transfert des biens au patrimoine d'affectation, celui-ci est consacré dans l'acte constitutif de la fiducie et s'opère instantanément, dès l'acceptation du mandat par le fiduciaire.<sup>210</sup> De par le seul fait de son acceptation, il y a donc à la fois : création de la fiducie (et donc du patrimoine d'affectation), extinction du droit de propriété du constituant sur les biens transférés, et engagement du fiduciaire en tant qu'administrateur de la fiducie. Ainsi, contrairement aux préoccupations soulevées par rapport au *charitable trust* en common law, il n'y aurait pas de délai en lien avec la création d'une fiducie de données en droit québécois, et non pas plus même s'il s'agit d'une fiducie d'utilité sociale, l'espèce de fiducie en droit québécois qui vise un intérêt général sans qu'il soit nécessaire d'avoir un ou des bénéficiaires nommés. Cette espèce sera analysée plus en détail plus loin, cette section portant principalement sur la flexibilité et la versatilité de l'outil.

207 Ibid art 1262.

208 [2004] 1 RCS 758 au para 31.

209 Beaulne, « Droit des fiducies », supra note 155 aux para 120, 131.

210 Ibid aux para 152-152.1

Il y a également une grande flexibilité eu égard à l'établissement des objectifs de la fiducie. Étant constitué à partir d'un contrat, les constituants auraient essentiellement carte blanche pour établir quelque finalité ou objectifs qu'il soit, pour autant qu'ils soient licites. L'acte constitutif pourrait donc intégrer tous les principes directeurs notés ci-haut, tel, une gouvernance fiduciaire indépendante, juste, sécuritaire, équitable, participative et collaborative, transparente, etc. Ces principes constitueront ainsi à la foi l'orientation de la gouvernance fiduciaire ainsi que son affectation, soit le but poursuivi par la fiducie. Comme il sera vu plus loin, cette finalité sera aussi tributaire de l'espèce de fiducie, qui peut être soit personnelle, soit d'utilité privée, ou encore d'utilité sociale.<sup>211</sup>

## **2. La possibilité d'apporter des modifications à la fiducie**

Le *Code* prévoit la possibilité d'apporter certaines modifications à la fiducie qui semblent, à premier égard, lui accorder un degré de flexibilité suffisant pour pouvoir s'adapter à des nouvelles circonstances, exigences ou intérêts, sans pour autant être si permissif pour permettre des modifications qui risqueraient de complètement dénaturer la fiducie de la volonté initiale du constituant.

Pour un, il est toujours possible d'augmenter le patrimoine fiduciaire en lui ajoutant des biens, sans créer de nouveaux constituants ni d'autres effets sur la fiducie.<sup>212</sup> Comme il sera vu plus loin, ces derniers ont certains pouvoirs dans le cadre de l'administration de la fiducie, qui ne sont pas toutefois accordés à ceux qui rajouteront à son patrimoine après sa constitution. Aussi, les biens ajoutés n'acquiert pas de statut différent aux autres biens ; tous se confondent dans le patrimoine fiduciaire et sont administrés conformément aux dispositions de l'acte constitutif.<sup>213</sup> Ceci permettrait donc à une fiducie de données d'acquérir des données pour les ajouter à son répertoire, ce qui serait favorable, eu égard aux avantages explicités ci-dessus, à l'atteinte de ses objectifs.

Autrement, il est aussi possible d'apporter des modifications à l'affectation de la fiducie, ainsi qu'à son administration, sous certaines conditions.

Pour ce qui sont des modifications à son affectation, celles-ci sont en réalité interdites par le code. En effet, les seuls cas où il est possible de modifier l'affectation d'une fiducie sont lorsque l'affectation initiale devient virtuellement impossible à réaliser. Et même alors, on ne permet pas que soit simplement substituée une affectation pour une autre – au contraire, la fiducie dont l'affectation devient impossible ou trop onéreuse à réaliser sera tout simplement éteinte.<sup>214</sup> Il est seulement permis exception à cette règle pour les FUS : dans de pareils cas, au lieu d'éteindre une FUS, on permettra plutôt de lui substituer un but qui se rapproche le plus possible du but original. La demande devra en être faite au tribunal et c'est ce dernier qui en décidera ultimement. La raison pour cette exception étant que l'on reconnaît l'importance du rôle d'intérêt général que jouent normalement les FUS, et donc le législateur a plutôt préféré de les permettre de perdurer en perpétuité au lieu d'éteindre une institution avec beaucoup de valeur sociale.<sup>215</sup>

Si par contre, la volonté initiale du constituant demeure réalisable, il sera interdit de modifier l'affectation de la fiducie. En effet, dans tous les cas où cette volonté demeure réalisable, les seules modifications permises seront celles visant l'adoption de nouvelles mesures qui permettront de mieux respecter la volonté initiale du constituant, ou de mieux favoriser l'accomplissement de la fiducie. C'est cette seule exception qui est permise à l'article 1294 CcQ. Selon les commentaires du ministère de la justice à cet article, l'on pourrait s'en prévaloir pour, par exemple, modifier le nombre de fiduciaires, leurs pouvoirs, ou tout autre aspect de leur administration ; on pourrait également prolonger la durée de la fiducie si pas initialement constituée à perpétuité.

211 CcQ, supra note 152 art 1266.

212 Ibid art 1293.

213 Ibid.

214 CcQ, supra note 152 aux art 1294 al 1, 1296 al 2.

215 Beaulne, « Droit des fiducies », supra note 155 aux para 400, 401.1.

Ainsi dans tous les cas, malgré la grande flexibilité qu'on lui accorde au niveau de sa constitution, il semble être très difficile d'apporter des modifications à une fiducie une fois constituée. Ceci n'est pas par contre nécessairement négatif, puisque cela n'accorderait qu'un contrôle supplémentaire sur les activités d'une fiducie de données, et assurerait le respect de la volonté initiale de ses constituants. Si on prend un exemple pratique, par exemple, pour comparaison : l'on dénonce souvent le fait que les plateformes digitales changent très souvent leurs politiques de confidentialité. Certes, c'est l'avantage du véhicule corporatif – à cet égard il jouit effectivement d'une plus grande flexibilité que la fiducie. Par contre ces modifications fréquentes à leurs politiques n'inspire vraisemblablement pas la confiance du public à leur égard. Pour cette raison, un cadre plus fixe, mais plus stable, pourrait être préférable. En revanche, pour ce qui est de la capacité d'une fiducie de s'adapter à un environnement réglementaire en évolution, ceci ne devrait non plus poser problème au fonctionnement de la fiducie. D'abord, il est entendu qu'une fiducie – comme toute entité – doit se conformer aux lois et règlements en vigueur. Autrement, son fonctionnement serait bel et bien entravée. Or, le droit québécois des fiducies permet les modifications qui visent mieux favoriser l'accomplissement de la fiducie. Il serait difficile de prétendre qu'une modification visant à rendre une fiducie de données conforme à des nouvelles mesures réglementaires ne soit pas une mesure visant à mieux permettre son accomplissement – en effet, ne pas permettre une telle modification risquerait de la paralyser.

Le droit québécois semble donc permettre un degré suffisant de flexibilité à la fiducie pour sa constitution et pour les modifications qui pourraient s'avérer nécessaires pendant sa durée.

### **3. L'extinction de la fiducie et ses effets**

Qu'en est-il des possibilité de mettre fin à une fiducie ? Dans le cas d'une fiducie de données, une existence à perpétuité serait probablement souhaitable puisqu'une plus grande stabilité inspirera davantage de confiance au public. Ceci serait aussi souhaitable au niveau du consentement en lien avec les données ; s'il fut accordé, par exemple, en lien express avec une fiducie donnée, le transfert des données à une autre entité risque d'être compliqué.

Selon l'alinéa 2 de l'article 1296 CcQ, une fiducie peut s'éteindre par l'arrivé de son terme (soit celui consacré dans l'acte constitutif, soit celui imposé par la loi, pour les fiducies personnelles seulement), par l'avènement d'une condition comprise dans l'acte constitutif, ou par le fait de l'extinction du but de la fiducie, soit parce qu'elle fut réalisée, soit parce qu'elle devient désormais impossible à atteindre. La fiducie peut aussi être éteinte par la renonciation ou la caducité du droit de tous les bénéficiaires aux avantages du patrimoine fiduciaire.<sup>216</sup>

En ce qui concerne une fiducie de données, les bénéficiaires seront probablement toujours indéterminés, bien qu'ils puissent être élus ou désignés selon des critères objectifs. Cette dernière modalité d'extinction de la fiducie est donc impertinente à la fiducie de données. Au regard des deux premières par contre, celles-ci semblent pouvoir offrir des balises adéquates à la vie d'une fiducie de données. La possibilité d'inclure une clause prévoyant l'extinction sur l'avènement d'une condition permettrait aux constituants d'incorporer leur volonté à ce niveau ; autrement, elle ne serait éteinte que si sa finalité devient irréalisable, ce qui semble aussi être souhaitable.

En ce qui à trait aux effets de l'extinction, ceux-ci sont tributaires de l'espèce de fiducie en question. Nous traitons de ceux applicables aux FUP ainsi qu'aux FUS étant donné qu'il serait possible de constituer une fiducie de données sous ces deux formes.

216 CcQ, supra note 152 art 1296 al 1.

Pour les FUP seulement, sur extinction de la fiducie il devra premièrement avoir remise des biens de la fiducie par le fiduciaire à « ceux qui y ont droit ». <sup>217</sup> Selon le professeur Beaulne, ceux / celui-ci s'agit du bénéficiaire ultime de la fiducie, désigné comme tel dans l'acte constitutif, qui peut être une personne physique ou morale, ou encore un organisme désigné comme ayant droit final. <sup>218</sup> Et à défaut d'un bénéficiaire final désigné, les biens seront dévolus au constituant ou à ses héritiers. <sup>219</sup> Si une fiducie de données est constituée en tant que FUP, il serait donc nécessaire de bien réfléchir à qui seront dévolus les données advenant son extinction.

En ce qui concerne la FUS, sur extinction les biens devront plutôt être dévolus soit à une autre fiducie, soit à une personne morale, ou encore à tout autre groupement de personnes ayant une vocation se rapprochant le plus possible de celle de la fiducie éteinte. <sup>220</sup> La désignation de l'entité bénéficiaire sera faite par le tribunal, mais sur la recommandation du fiduciaire.

Dans ces deux cas (la FUP et FUS), même qu'il soit bien que la dévolution du patrimoine fiduciaire – et donc des données personnelles – serait contrôlée, ceci risque de poser des problèmes au niveau du consentement. Par exemple, que faire si les personnes fichées s'opposent à ce que leurs données soient dévolues à quelconque autre entité ou personne ? Permettrons alors qu'elles soient détruites ? Ceci serait en contravention directe avec les obligations qui imposent au fiduciaire en tant qu'administrateur chargé de la pleine administration, notamment celui de conserver le patrimoine. Certes il est vrai que cette obligation s'applique à titre supplétif seulement <sup>221</sup> : le fiduciaire y est seulement tenu dans la mesure que l'intérêt du bénéficiaire ou la poursuite du but de la fiducie l'exigent. Mais serait-il permis d'opter pour la destruction du patrimoine au lieu de sa dévolution avenant l'extinction de la fiducie ? Étant donné que c'est le tribunal qui doit prononcer l'extinction et la dévolution, il n'est pas certain qu'il lui soit possible de plutôt détruire les données. Tout dépendant de l'importance de ce facteur, ceci pourrait exclure la fiducie québécoise comme option pour la gouvernance des données.

## E. Versatilité et flexibilité eu égard aux principaux acteurs de la fiducie

### 1. Le constituant

Le droit des fiducies du Québec permet aussi une grande flexibilité au niveau des principaux acteurs de la fiducie. Pour un, le constituant – soit celui qui crée la fiducie en transférant des biens qui lui appartiennent au patrimoine de la fiducie <sup>222</sup> – peut être une personne physique ou morale, et il peut en avoir qu'un seul ou plusieurs, pour autant qu'il ait la capacité de conclure l'acte qui constituera la fiducie. <sup>223</sup> Il serait donc tout à fait possible, par exemple, pour une institution de recherche universitaire de créer une fiducie de données pour la gestion des données recueillies dans le cadre des recherches effectuées sous son égide. Il pourrait y avoir une seule fiducie ou plusieurs selon les facultés, domaines de recherche, projets ou études spécifiques, etc. Celles-ci pourraient aussi conçues (si plusieurs) avec l'intention de faciliter le partage des données entre elles. Elles pourraient donc être mise sur pied avec une structure et des règles de gouvernance qui assureront leur compatibilité. Ceci est aussi vrai pour le partage inter-frontalier : une fiducie de données pourraient être conçue spécialement pour permettre se genre de partage et donc adopter une structure de gouvernance en conséquence. Elle ne pourrait, par contre, contrevir aux lois et règlements du Québec, ni d'aucune autre juridiction qui lui impose, donc la possibilité de partage inter-frontalier demeurerait limité à cet égard.

217 Ibid art 1297 al 1.

218 Beaulne, « Droit des fiducies », supra note 155 aux para 473-473.1.

219 CcQ, supra note 152 art 1297 al 2.

220 Ibid art 1298.

221 Ibid art 1306 in fine.

222 CcQ, supra note 152 art 1260.

223 Beaulne « Droit des fiducies », supra note 155 au para 188.

Il est aussi possible au constituant de cumuler les fonctions de bénéficiaire ou de fiduciaire en se désignant ainsi, pour autant qu'il respecte les conditions de l'article 1275 CcQ,<sup>224</sup> soit, qu'il agisse conjointement avec un fiduciaire impartial qui n'est ni constituant, ni bénéficiaire.<sup>225</sup> Une institution de recherche qui crée une fiducie de données pourrait donc rester active au sein de la gouvernance de la fiducie si tel est son désir. Agir conjointement ne signifie pas toutefois que les décisions soient obligatoirement prises de manière unanime entre fiduciaires conjoints.<sup>226</sup> S'il y a divergences d'opinion entre cofiduciaires par exemple, l'unanimité ne s'imposera pas, mais ils devront tout de même toujours agir en fonction des obligations qui imposent aux fiduciaires,<sup>227</sup> notamment, celle de toujours agir dans le meilleur intérêt du bénéficiaire ou de l'accomplissement de la fin poursuivie par la fiducie, et celle de loyauté, qui lui oblige de toujours demeurer en absence de conflit d'intérêts.<sup>228</sup>

## 2. Le bénéficiaire et la faculté d'élire

Au niveau du bénéficiaire – soit celui destiné à profiter des biens ou de l'existence de la fiducie – il n'est pas obligatoire qu'il existe dans le dessin de la fiducie. En effet, le droit québécois permet qu'une fiducie puisse exister en l'absence totale d'un bénéficiaire. De façon générale, la raison d'être de la fiducie est toujours orientée alentour de sa finalité, qui peut ou pas viser à procurer un avantage à une personne en particulier.<sup>229</sup> La fiducie d'utilité sociale, par exemple, est constituée dans un but d'intérêt général,<sup>230</sup> et n'a donc pas de bénéficiaire désigné. Elle pourrait toutefois, en raison de son affectation, avoir des bénéficiaires non individuellement identifiés mais tout de même *déterminables* à partir de critères objectifs.<sup>231</sup> Ce serait, par exemple, d'une FUS vouée à l'entretien d'un gît pour les personnes sans-abri – les bénéficiaires seraient alors toutes les personnes sans-abri, élus à partir de critères objectifs établis dans l'acte constitutif et par l'exercice de la faculté d'élire reconnu au fiduciaire.<sup>232</sup>

Dans le cas d'une fiducie de données dans le domaine de la santé, celle-ci sera vraisemblablement sans bénéficiaires tout court vu le besoin de maintenir un contrôle absolu sur l'utilisation et toute communication des données personnelles détenues par la fiducie. Les données seraient donc conservées dans le patrimoine de la fiducie à perpétuité ou pour un terme défini selon les besoins identifiés au moment de la constitution de la fiducie.

Si l'on prend, par exemple, l'idée d'une bibliothèque constituée en tant que fiducie sans bénéficiaires. Les livres s'apparenteraient aux données détenues en fiducie. Le droit de consulter et d'emprunter les livres pourrait être ouvert au grand public ou restreint à un ou certains groupes en particuliers. Ceux qui seront accordés de tels droits devront d'abord être membres de la bibliothèque. Ils devront aussi respecter les conditions d'utilisation des livres, soit, de ne pas les abîmer et de les rapporter intacts et à l'intérieur d'un certain délai. Une fiducie de données pourrait revêtir un fonctionnement similaire. Les 'membres' pourraient être les chercheurs, de façon large ou restreint à certains milieux, par exemple, en excluant les chercheurs du secteur privé, ou en excluant ceux ne rencontrant pas tel ou tel principe éthique ou autre critère établi dans l'acte constitutif, etc.

224 CcQ, supra note 152 art 1276.

225 Commentaires du ministre, supra note 159 art 1268.

226 Beaulne « Droit des fiducies », supra note 155 au para 291.

227 Voir *Canada Trust c Gabriel*, [1993] QJ no 99 (QL) (en cas de divergence d'opinion entre cofiduciaires à propos des placements, l'opinion du cofiduciaire, qui est également bénéficiaire, doit prévaloir).

228 CcQ, supra note 152 aux art 1309, 1310.

229 Ibid art 1260.

230 Ibid art 1270.

231 Beaulne, « Droit des fiducies », supra note 155 aux para 223-24.

232 Ibid aux para 235 ; CcQ, supra note 152 art 1282.



### 3. Le fiduciaire

En ce qui a trait au fiduciaire, celui-ci peut être une personne physique ou morale,<sup>233</sup> et le constituant peut en désigner un seul ou bien plusieurs, qui devront alors effectuer leur administration de manière collective. Rien n'empêcherait donc de choisir un fiduciaire, ou même un conseil de fiduciaire, avec tel ou tel compétences et qualités souhaitables pour l'administration effective d'une fiducie de données.

#### a. L'administration collective

En ce qui concerne l'administration collective, le *Code civil du Québec* propose un régime aux articles 1332 à 1338 mais à titre supplétif seulement, donc il serait possible d'en disposer autrement dans l'acte constitutif.<sup>234</sup> Il serait ainsi tout à fait possible d'élaborer une structure de gouvernance d'une fiducie de données composée d'un conseil de fiduciaires, par exemple, avec des comités siégeant à titre de conseillers ou autre, et d'accorder à ces entités un pouvoir décisionnel ou tout autre pouvoir, pour autant que le tout soit bien circonscrit dans l'acte constitutif. Ceci permettrait donc à la fiducie québécoise de répondre non seulement au critère de la flexibilité, mais aussi à celle d'une gouvernance participative et collaborative.

#### b. La possibilité de délégation

Le fiduciaire peut aussi, qu'il soit seul fiduciaire ou non, déléguer ses fonctions ou encore se faire représenter par un tiers mais *pour un acte déterminé* seulement ; il ne pourrait par exemple le faire de façon générale pour la conduite de l'administration, ni pour l'exercice d'un pouvoir discrétionnaire, sauf si la délégation est à un coadministrateurs. Étant donné les préoccupations entourant les qualifications et compétences d'un éventuel fiduciaire d'une fiducie de données à traiter les demandes d'accès aux données et juger de la qualité de leur usage, il serait probablement préférable d'éviter la délégation de fonctions. Heureusement, les articles 1337 et 1338 CcQ sont aussi que supplétif, donc l'acte constitutif pourrait en disposer autrement ; en permettant, par exemple, la délégation pour certains actes seulement, et dans des cas bien circonscrit, si l'on veut tout de même permettre au fiduciaire d'exercer cette faculté dans les cas appropriés. Et la responsabilité n'est aussi pas pour autant affectée par la délégation : si le mandataire commet une faute dans l'exercice du pouvoir délégué, le bénéficiaire qui en subi préjudice pourra répudier ces actes et aussi exercer tout autre recours disponible contre le mandataire, même si la délégation fut valide.<sup>235</sup> En revanche, le fiduciaire pourrait aussi avoir à répondre, mais seulement du soin avec lequel il a choisi son mandataire et la qualité des instructions qu'il lui a donné.<sup>236</sup>

233 CcQ, supra note 152 art 1274.

234 Beaulne, « Droit des fiducies », supra note 155 au para 309, 339.

235 CcQ, supra note 152 art 1338.

236 Ibid art 1337 al 2.



## F. Les trois grandes catégories de fiducies en droit québécois : laquelle pour une fiducie de données ?

Le *Code civile du Québec* dénomme trois espèces de fiducies en droit québécois : la fiducie personnelle, la fiducie d'utilité privée, et la fiducie d'utilité sociale.<sup>237</sup> Quelles d'entre elles pourraient servir pour constituer une fiducie de donnée ?

### 1. La fiducie personnelle

Celle-ci est constituée dans le but de procurer un avantage à une personne déterminée ou déterminable<sup>238</sup> ; l'avantage est donc nécessairement personnel et individuel, d'où sa nomenclature. Elle aura donc nécessairement un ou des bénéficiaires. Elle est aussi obligatoirement constituée à titre gratuit (par donation ou testament) et peut avoir un terme maximal de cent ans<sup>239</sup>

Puisqu'un des critères fondamentaux d'une fiducie de données est qu'elle soit constituée dans un but d'intérêt général, et que la fiducie personnelle ne permettrait pas ceci, celle-ci ne s'avèrerait pas une forme convenable pour une fiducie de données.

### 2. La fiducie d'utilité privée

La fiducie d'utilité privée (FUP) se décline en deux grandes catégories : celle constituée à vocation commerciale,<sup>240</sup> et celle constituée à vocation non-commerciale.<sup>241</sup> Dans tous les cas, elle peut être perpétuelle ou à durée déterminée<sup>242</sup> et est nécessairement affecté à un but de nature privé.<sup>243</sup>

Statuons d'abord sur la nécessité d'être affecté à un but de nature privé. Ceci serait-il incompatible avec une fiducie de données dans le domaine de la santé? Pas nécessairement. Une telle fiducie pourrait, par exemple, être constituée pour la gestion des données dans le cadre d'un projet de recherche en particulier. Ainsi l'accès aux données pourrait être restreinte à seules les parties participant à ce projet. Son affectation serait donc de nature privé, bien que les résultats du projet puissent tout de même être bénéfique pour le public en général. Cette espèce de fiducie semble donc compatible avec une fiducie de données dans le domaine de la santé, même si, tel qu'établi par les critères dans la première partie de ce rapport, il serait préférable que cette dernière ait une finalité claire d'intérêt public, pour l'obtention de sa licence sociale.

Pour ce qui est des différents types de FUP, elle peut être à vocation commerciale mais ceci ne sera pas compatible avec une fiducie de données. Autrement, elle peut aussi être à vocation non-commerciale, et ce soit sans bénéficiaire, soit avec bénéficiaire mais de manière indirecte seulement. Dans ces deux derniers cas, elle peut être constituée à titre gratuit ou onéreux.<sup>244</sup>

Celle à vocation non-commerciale peut être constituée à titre gratuit ou onéreux<sup>245</sup> et peut être soit sans bénéficiaire, soit avec bénéficiaires mais de manière indirecte seulement. Dans ce dernier cas, on dira plutôt qu'elle est constituée dans le but de procurer un avantage *indirect* à une personne ou à un groupe de personnes (bénéficiaires indirects).<sup>246</sup>

237 Ibid art 1266.

238 Ibid art 1267.

239 Ibid aux art 1271, 1272.

240 Ibid art 1269

241 Ibid art 1268

242 Ibid art 1273

243 Commentaires du ministre, supra note 159 art 1268.

244 CcQ, supra note 152 art 1268 CcQ

245 Ibid art 1268 CcQ

246 Commentaires du ministre, supra note 159 art 1268.

Dans le cas où il y a absence totale de bénéficiaire, sa finalité est essentiellement de réaliser une affectation voulue par le constituant et qui concerne certains actes matériels en rapport avec un bien, mais qui ne comporte aucun véritable avantage pour qui que ce soit.<sup>247</sup> L'on pourrait penser, par exemple, à une fiducie constituée par un défunt pour l'entretien de ses animaux de compagnie après sa mort. Dans le deuxième cas (FUP avec bénéficiaires indirects), on dira plutôt qu'elle est constituée dans le but de procurer un avantage *indirect* à une personne ou à un groupe de personnes (bénéficiaires indirects).<sup>248</sup> On parle ici d'une affectation qui concerne principalement un bien de nature privé, mais qui est spécifiquement affecté à un usage déterminé. L'on pensera ainsi, par exemple, à une fiducie constituée pour gérer un chalet au bénéfice des employés d'une entreprise,<sup>249</sup> ou encore à une fiducie environnementale constituée pour créer une réserve de conservation de la faune à partir d'un terrain privé.<sup>250</sup>

Est-ce que l'un ou l'autre de ces deux types pourrait constituer une fiducie de données dans le domaine de la santé ?

La FUP à vocation non-commerciale de type sans bénéficiaire semble inappropriée. En effet, bien qu'elle n'engendrerait pas de questionnement en lien avec une marchandisation des données personnelles, il est difficile de penser à des situations où des données personnelles de santé seraient confiées à une telle fiducie. Par exemple, dans le cas d'une telle fiducie, la seule raison de l'affectation serait vraisemblablement leur conservation. Autrement, pourquoi confier des données en fiducie si personne n'est pour en bénéficier ? Certes, la sécurité et la protection des données seraient ainsi assurés, mais à quoi bon si les données ne servent à nulle autre fin ? Ce serait l'équivalent de les mettre dans un coffre-fort, ce qui rendrait impertinent le fait de les collectées en premier lieu. Or, la raison pour laquelle nous collectons des données est *en premier lieu pour les utiliser* – à des fins de recherche, de statistique, d'analyse de marché, de tendances, d'efficacité opérationnelle, etc. Que les données soient affectées à une fin *utile* est donc la *sine qua non* d'une fiducie de données. La FUP à vocation non-commerciale sans bénéficiaire s'avèrerait donc vraisemblablement inadéquate pour cette raison.

Qu'en est-il toutefois de la FUP à vocation non-commerciale *mais avec 'bénéficiaires' indirects* ? Réfléchissons-y en reprenant, par exemple, le cas de la fiducie environnementale constituée pour créer une réserve faunique à partir d'un terrain privé. Dans un tel cas, le terrain privé a une valeur en soi – sa valeur écologique – sans qu'il soit nécessaire de l'utiliser à une fin quelconque. Sa valeur écologique existe du seul fait de l'existence de la propriété foncière, sans qu'il soit nécessaire d'y apporter quelque action que ce soit, à part peut-être des actions d'entretien afin de conserver cette valeur écologique. Le public *pourrait* l'utiliser et en bénéficier par ricochet (ex. en permettant chasse, randonnée, raquette, ski de fond, etc.), mais le terrain conserve sa valeur *qu'on s'en serve ou non*. Pourrait-on dire de mêmes des données ? Hormis la question sur la nature juridique des données, il n'est pas possible d'ignorer le fait que celles-ci ont une valeur économique *réelle*. Il est donc raisonnable de prétendre que oui, en effet, les données ont une valeur en soi, *du moment qu'elles puissent servir à quelque chose*. Ceci étant, dans la mesure qu'une FUP de type non-commerciale et sans bénéficiaire direct « est constituée *dans le but de procurer un avantage indirect* à une personne ou à un groupe de personnes », <sup>251</sup> il est raisonnable de penser qu'une fiducie de données dans le domaine de la santé pourrait être constituée à ce titre. En réalité, il n'y aurait pas de véritable bénéficiaire mais simplement un 'groupe de personnes' à qui serait procuré l'avantage d'utiliser les données pour les fins stipulées dans l'acte constitutif.

247 Beaulne, « Droit des fiducies », supra note 155 à la p 100.

248 Commentaires du ministre, supra note 159 art 1268.

249 Beaulne, « Droit des fiducies », supra note 155 aux pp 100-101.

250 Beaulne, « Droit des fiducies », supra note 155 à la p 101.

251 Commentaires du ministre, supra note 159 art 1268.

L'on pourrait penser, par exemple, à « un groupe de personne » en désignant de façon large 'les chercheurs et scientifiques voulant se servir des données à des fins de recherche ou de statistique'. De nombreux contrôles pourraient être instaurés par la suite, par exemple, une condition d'usage à l'effet que nul ne pourra entreprendre des actions susceptibles à déprimer la valeur du bien ou le revendre à profit. Et tout comme ceux qui bénéficieront indirectement de la gestion de la réserve faunique devront respecter les mécanismes de contrôles qui seraient mis en place (ex. un système de réservation pour contrôler l'accès), les usagers d'une fiducie de données pourraient avoir à se plier à de mêmes types de contrôles (ex. demander l'accès à un jeu de données en particulier selon tel ou tel critères d'intérêt). Pour ces raisons, il est fort raisonnable de croire qu'une FUP à vocation non-commerciale et sans bénéficiaires directs pourrait très bien servir à constituer une fiducie de données.

Il y a toutefois deux obstacles potentiels auxquels l'on pourrait penser :

- Le fait que cette espèce de fiducie concerne principalement l'affectation d'un bien *de nature privé*. Cela nous ramènerait encore à la question de la nature juridique des données, à savoir si elles sont appropriables ou non. Tel que mentionné précédemment, cette question ressort du cadre de la présente étude demeurera ainsi en suspens.
- Le fait que la confiance du public fut identifiée comme un des critères essentiels au succès de tout projet de gouvernance des données, qui, tel que soulevé dans la première partie de ce rapport, sera principalement atteinte en affectant la fiducie à une finalité *d'intérêt public*.

Or, tel qu'explicité ci-haut, c'est la plutôt la *combinaison* des facteurs suivants qui déterminera si une fiducie sera apte à obtenir sa licence sociale : des valeurs de réciprocité et de non-exploitation fondée sur une participation purement volontaire et au service de l'intérêt public. Ceci étant, il n'est pas inconcevable de penser que le public appuierait l'idée d'une fiducie à vocation *non-commerciale* ayant comme affectation principale la protection et la conservation de la valeur des données, tout en procurant un avantage *indirect* à un groupe de personnes bien défini (par ex. des chercheurs avec des projets de recherche rencontrant tel ou tel critères), et le tout étant vraisemblablement assorti d'un cadre de gouvernance qui inclura des contrôles d'accès, d'usage, et d'autres encore. En effet, bien que cette espèce de fiducie soit constituée principalement pour procurer un avantage à un groupe de personnes défini, ceci n'exclut pas la possibilité qu'elle bénéficie *aussi* l'intérêt public. Il ne suffira de s'assurer que les chercheurs ou scientifiques qui jouiront de l'avantage de pouvoir utiliser les données de la fiducie ne pourront le faire *qu'à des fins qui bénéficieront aussi le public*. L'acte constitutif ainsi que les ententes d'utilisation pourrait par exemple inclure une stipulation à cet effet. Ceci servirait ensuite à titre de critère de sélection pour l'élection des personnes à qui l'on accordera un droit d'usage.

Cette espèce de fiducie semble donc très bien pouvoir servir afin de constituer une fiducie de données dans le domaine de la santé.

### **3. La fiducie d'utilité sociale**

Qu'en est-il de la FUS ? Celle-ci est prônée comme une option intéressante pour les personnes et collectivités non commerciales cherchant une solution adéquate pour la protection ainsi que la gouvernance collective de divers types de biens, d'immeubles et même de milieux naturels, au bénéfice de l'intérêt public. En effet, elle est par définition et donc nécessairement constituée dans un but d'intérêt général, notamment à caractère culturel, éducatif, philanthropique, religieux ou scientifique.<sup>252</sup> Pour ces seuls critères, la FUS semble pouvoir être convenable pour constituer une fiducie de données. Celle-ci pourrait bien se livrer à un but d'intérêt général de nature scientifique par exemple.

<sup>252</sup> Cc0, supra note 152 art 1270 ; Beaulne, « Droit des fiducies », supra note 155 au para 117.

En ce qui à trait au bénéficiaires de la FUS, tout comme pour la FUP à vocation non-commerciale et avec bénéficiaires indirects, ceux-ci ne sont en fait jamais individuellement nommés dans l'acte constitutif. La FUS est en effet plutôt constituée au bénéfice de l'ensemble de la population ou à une partie importante de celle-ci. Il n'est toutefois pas impossible de la restreindre à une personne à choisir parmi ce public, par l'exercice du fiduciaire de sa faculté d'élection selon des critères objectifs établis dans l'acte constitutif.<sup>253</sup> Il serait donc tout à fait possible « d'élire » des bénéficiaires-usagers à qui l'on accorderait un accès au répertoire et un droit d'usage des données.

Aussi, tout comme pour la FUP, elle peut être perpétuelle ou avoir un terme<sup>254</sup>, et peut être constituée par acte à titre gratuit ou onéreux. Elle s'avère donc ni plus ni moins avantageuse à ces égards non plus. Elle lui est aussi permise, pour qu'elle puisse s'assurer d'un financement accessoire, de s'adonner à une activité commerciale, pour autant que ce soit purement à but non lucratif.<sup>255</sup>

En ce qui à trait aux effets de son extinction – soit, la dévolution des données à soit une autre fiducie, soit à une personne morale, ou encore à tout autre groupement de personnes ayant une vocation se rapprochant le plus possible de la sienne – ceux-ci sont similaires à ceux de la FUP. Certes, pour cette dernière l'on prévoit plutôt la remise aux « ayants droits », mais ceux-ci peuvent être une personne physique ou morale, ou encore même un organisme. Pour autant qu'ils soient bien désignés dans l'acte constitutif. Ceci revient donc essentiellement au même que pour la FUS, la seule différence étant que le patrimoine d'une FUS sera *par défaut* dévolu à une fiducie/personne morale/organisme avec une vocation similaire à la sienne, alors que celui d'une FUP ira plutôt au constituant faute d'avoir désigné les ayants droits finaux. Ainsi dans les deux cas, l'acte constitutif permet de régler les effets de l'extinction d'une façon ou d'une autre, sauf pour la question d'une destruction potentielle des données si tel est le désir, question qui s'applique autant à la FUS qu'à la FUP. Autrement, la FUS peut faire tout ce qui est prévu dans son acte constitutif, sous réserve des autres limites ci-haut exposés.

Pour ces raisons elle paraît tout aussi convenable pour constituer une fiducie de données que la FUP à vocation non-commerciale et sans bénéficiaires directs.

La FUS aurait aussi le même souci que cette dernière eu égard au problème en lien avec la patrimonialité des données. La FUS a toutefois un léger avantage au niveau de son affectation. En effet, puisqu'elle est nommée « à utilité sociale » et qu'elle doit nécessairement être affecté à un intérêt général, elle obtiendrait peut-être plus facilement la confiance du public et ainsi sa licence sociale identifiée comme essentiel au succès de tout projet de gouvernance des données, et ce surtout dans le domaine de la santé. Il n'est pas par contre inconcevable de croire qu'une FUP à vocation non-commerciale et sans bénéficiaires directs pourrait obtenir une même telle licence. Avec une campagne de sensibilisation adéquate auprès du public, ainsi qu'une transparence par rapport à sa structure et un engagement hâtif et soutenu du public et des parties intéressées, incluant leur participation active à la gouvernance-même de la fiducie, elle pourrait en toute semblance très bien obtenir une même telle licence. D'autant plus que la FUP ne serait pas restreinte par les finalités prescrites du *Code civil*.

Vu d'ensemble, la FUS et FUP semblent essentiellement offrir les mêmes avantages et revêtir les mêmes inconvénients, cette dernière semblant par contre légèrement plus avantageuse au niveau de la flexibilité de son affectation, et cette première, au niveau de sa capacité à inspirer confiance au public.

253 Commentaire du ministre, supra note 159 art 1270 CcQ ; Beaulne, « Droit des fiducies », supra note 155 au para 117.

254 CcQ, supra note 152 art 1273.

255 Ibid art 1270.

## G. Une fiducie de données au Québec saura-t-elle relever les défis précités ?

### 1. La patrimonialité des données

Tel qu'explicité dans la première partie de ce rapport, les données personnelles ne sont pas, jusqu'à présent, reconnues en tant que biens. Or, la fiducie québécoise est par définition constituée d'un patrimoine composés de biens affectés à une finalité particulière. La particularité de la fiducie québécoise par contre, par rapport au droit des fiducies des autres juridiction, est que son patrimoine en est un d'affectation sans véritable titulaire. En effet, certains auteurs parlent ainsi d'une véritable mutation du droit de propriété lorsque des biens sont transférés en fiducie.<sup>256</sup> Alors que la théorie classique de la propriété s'explique par la relation qui existe entre le titulaire du droit – le sujet – et son objet – le droit de propriété – la théorie du patrimoine d'affectation doit plutôt se comprendre en termes de pouvoirs et non de droits, puisqu'il n'y a tout simplement pas de titulaire dans cette dernière. Tel que noté ci-haut, personne ne détient un droit de propriété quelconque sur les biens détenus en fiducie. Ni le fiduciaire, ni le constituant, ni les bénéficiaires n'ont de droit réel sur ces biens.<sup>257</sup> Le transfert en fiducie fait que le droit de propriété n'existe tout simplement plus – il s'évapore. C'est pourquoi certains soutiennent qu'on ne peut ainsi parler de transmission de droit mais que l'on doit plutôt parler d'une mutation du droit de propriété puisqu'en réalité, il y a *passage* des biens d'une dimension (celle de la théorie classique de la propriété) à une autre (celle de la théorie du patrimoine d'affectation), et ainsi une véritable *transformation* des droits en pouvoirs.<sup>258</sup>

Ceci est-il susceptible d'évacuer le problème posé par la qualification juridique des données personnelles en tant que non-biens ?

En théorie, la réponse devrait être non. Peu importe que le patrimoine fiduciaire québécois soit d'affectation, reste qu'il s'agit tout de même d'un patrimoine qui *par définition* est composé de biens.<sup>259</sup> Or, les données personnelles restent jusqu'à présent des choses et non des biens.

Il n'y a toutefois pas de contestation sur le fait que ces choses représentent beaucoup de valeur. La nature de l'administration fiduciaire semble aussi être des plus compatible avec les critères établis pour la gouvernance responsable des données de la santé. Malgré cela, il est toujours tout aussi incertain qu'une fiducie composée de données soit valablement reconnu par les tribunaux advenant un litige. Si les données ne sont que de simple choses, il ne peut pas y avoir transfert de 'biens' quelconque du patrimoine d'une personne au patrimoine fiduciaire ; il ne peut non plus y avoir affectation de 'biens' à une fin particulière. Les deux premiers critères de la Cour suprême pour la constitution d'une fiducie ne seraient donc pas rencontrés, et il n'est donc pas certain qu'une telle fiducie soit reconnue par les tribunaux. Les implications de ceci advenant un litige éventuel devraient donc être bien considérées avant d'aller de l'avant avec la mise sur pied d'une fiducie de données, dans le domaine de la santé ou tout autre domaine.

256 Voir par exemple : Beaulne, « Droit des fiducies », supra note 155 aux para 157, 187.

257 CcQ, supra note 152 art 1261.

258 Ibid art 1260 in fine.

259 Ibid art 1261.

## 2. Financement

Une fiducie de données connaîtra vraisemblablement les mêmes problèmes que les biobanques en termes de financement. Devant viser un intérêt public et représenter les valeurs de réciprocité et de non-exploitation, elle devra certainement être constituée à vocation non-commerciale, ce qui exclura toute possibilité de générer un profit de l'octroi des droits d'utilisation des données. Il ne serait pas par contre interdit d'exiger une modeste contrepartie pour ces derniers, en autant qu'elle soit pour des fins de subsistance seulement. Tel que noté ci-haut, il est permis que la FUS se livre à une activité commerciale en autant que ce soit à but non lucratif.<sup>260</sup> Elle pourrait donc prévoir une telle activité afin de se sécuriser un financement de subsistance. Certains ont par exemple suggéré l'octroi de licences d'utilisation des données pour contrepartie.<sup>261</sup> Ainsi des moyens de financement sont possibles; il resterait à déterminer dans quelle mesure ils pourront combler les besoins financiers de la fiducie.

## 3. Consentement

La fiducie ne sera pas à l'abri des exigences se rapportant au consentement ni de toute autres exigences légales entourant la collecte, la communication et l'utilisation des données personnelles. Elle devra donc dans tous les cas se conformer à de telles exigences. En théorie par contre, le consentement suit les données, donc tant que les fins consenties ne sont pas incompatibles avec les usages que permettront la fiducie, le consentement restera valide et ne devrait poser de problème ni au transfert des données au patrimoine fiduciaire, ni à leur partage subséquent pour les fins non-incompatibles.

## 4. Les autres défis potentiels

En ce qui a trait au manque d'uniformité dans la législation provinciale et internationale, ceci restera un défi au partage des données tant et autant que les cadres réglementaires entourant la gestion de données personnelles seront incompatibles. Il en va de même pour la communication des données entre différentes fiducies s'il y a fragmentation ainsi que les défis posés par une culture d'aversion au risque généralisé quant au partage des données médicales ; si tel s'avère être le cas au Québec, elle devra entreprendre les efforts nécessaires pour sensibiliser le public et lui inspirer confiance quant à ses activités.

Elle aura aussi à composer avec les autres défis précités, tels les défis d'ordre logistique, le problème de fragmentation, l'incongruence inter-juridictionnelle, et la difficulté de garantir un droit à la révocabilité du consentement ou au transfert des données.

Elle ne connaîtra toutefois pas de défis en lien avec un délai de constitution : comme il a été vu ci-haut, la fiducie québécoise peut être constituée sans formalités et existe du moment que le fiduciaire accepte son mandat d'administration de la fiducie. Aussi, tel que noté, elle peut tout à fait exister sans bénéficiaire nommé et revêt une flexibilité suffisante pour lui permettre de s'adapter aux changements qui surviendront. Le pouvoir accordé au fiduciaire d'ester en justice pour tout ce qui concerne la protection des intérêts de la fiducie fournit aussi un mécanisme concret qui permettra le contrôle des tiers quant à l'usage qu'ils feront des données partagées. La surveillance de ces derniers serait tout de même à prévoir, le droit québécois des fiducies ne prévoyant aucun mécanisme par défaut à cet effet. Il y aurait ainsi la même incertitude quant à savoir si un tel rôle devrait être imposé au fiduciaire ou non. Autrement, la fiducie québécoise serait non plus à l'abri des problèmes de financement observés dans les biobanques.

<sup>260</sup> Ibid art 1270.

<sup>261</sup> Sean McDonald et Keith Porcaro, « The Civic Trust », Medium (4 août 2015) en ligne : <<https://medium.com/@digitalpublic/the-civic-trust-e674f9aeab43>>.



OBSERVATOIRE INTERNATIONAL  
SUR LES IMPACTS SOCIÉTAUX  
DE L'IA ET DU NUMÉRIQUE