3. DE NOUVELLES RECOMMANDATIONS POUR L'INTERNET DES OBJETS

Dans la section 2.3.4, nous avons relevé six questions à résoudre entourant l'Internet des objets et la protection de la vie privée. Dans ce chapitre, nous répondons à ces questions et nous en tirons des recommandations à l'attention du gouvernement, des entreprises et du secteur professionnel.

3.1 Doit-on prioriser le laisser-faire, la législation nationale ou la législation internationale entourant l'Internet des objets?

Dans le contexte actuel, la meilleure solution semble être une législation québécoise qui soit sensible et attentive aux législations en vigueur dans les États environnants et les grands partenaires commerciaux du Québec (les autres provinces canadiennes, les États-Unis, le Mexique, l'Europe, etc.). Actuellement, le laisser-faire quant au marché des objets connectés n'est pas judicieux.

D'une part, comme mentionné au chapitre 2, l'industrie des objets connectés est aux prises avec un problème d'action collective, où chaque acteur n'a pas intérêt individuellement à concevoir des objets sécuritaires, respectant certains standards de vie privée, et ainsi de suite. Or, la situation collective qui en résulte est au désavantage tant de l'industrie que des citoyens. Une meilleure option, tant pour l'industrie que pour les citoyens, est que des règles et des sanctions s'appliquent à toutes les entreprises. Conformément à ce qui précède, si nous voulons une industrie des objets connectés qui bénéficie au plus grand nombre (selon le principe d'utilité collective), on ne peut pas simplement laisser l'industrie des objets connectés à elle-même.

L'État pourrait créer un organisme chargé de déterminer si les entreprises développant des objets connectés respectent un certain nombre de critères (que nous relèverons dans le reste de ce document). Au sein de telles institutions, des experts de différents domaines (génie, droit, sécurité informationnelle, etc.) pourraient établir et actualiser les normes appropriées à respecter dans la conception d'objets connectés.

Cette approche, axée sur la certification, est très courante dans de nombreux secteurs d'activité. La certification pourrait avoir pour objectif d'autoriser la vente ou d'assurer la conformité des objets connectés, à l'instar du travail réalisé par Santé Canada pour les médicaments, les aliments, et ainsi de suite. Mais la certification pourrait aussi avoir pour but de signaler au consommateur que certaines normes ont été respectées par le fabricant. Pensons au programme de certification « Energy Star », qui informe les consommateurs du rendement énergétique des électroménagers qu'ils se procurent.

Si l'État veut s'appuyer sur des mécanismes institutionnels déjà en place, il pourrait aussi avoir recours au système professionnel. Au Québec, les ordres professionnels veillent à protéger le public, ce qui peut inclure la protection de la vie privée. De nouveaux actes réservés à certains professionnels pourraient jouer ce rôle. Présentement, le système professionnel encadre plusieurs pratiques, de la conception de plans pour construire des bâtiments à la prolongation des ordonnances d'un traitement médical. Étrangement, rien n'est prévu pour la gestion des données personnelles. N'importe qui peut donc s'improviser spécialiste de la gestion des données personnelles.

Des actes comme la conception d'outils de collecte de données personnelles, ou la délivrance d'attestations de conformité pour les outils de collecte de données, pourraient être réservés aux ingénieurs en logiciels[53].

53 Nous mentionnons spécifiquement l'Ordre des ingénieurs du Québec parce que, sur les 46 ordres professionnels existants au Québec, c'est le seul dont les membres sont appelés à concevoir des objets connectés.

Conformément à ce qui précède, il faudrait veiller à ce que ces ingénieurs aient une formation adéquate en matière d'enjeux éthiques soulevés par les objets connectés, ou qu'ils soient accompagnés par des experts de différents domaines pour bien cerner ces enjeux (ou les deux). Selon le principe de protection du public, central au système professionnel québécois, un ingénieur en logiciels qui manquerait à ses responsabilités de protection de la vie privée ferait l'objet de sanctions ou perdrait ses privilèges de pratique.

Plusieurs experts ont souligné le fait que la création de privilèges de pratique pour les ingénieurs en logiciels ne dénouera pas tous les problèmes décrits dans ce document (par exemple, cela n'améliorera pas la qualité du consentement, un point dont il a été question à la section 3.3). C'est, au mieux, une *partie* de la solution. Malgré tout, le recours au système professionnel est une forme d'intervention peu complexe, qui s'appuie sur des mécanismes institutionnels existants. Pour cette raison, ce type d'intervention devrait au moins être étudié.

Quel que soit le type d'intervention retenu par l'État québécois, il faut souligner que les éventuelles politiques québécoises seront plus facilement applicables si les principaux partenaires économiques du Québec ont des politiques similaires. Ce problème est particulièrement saillant dans certains secteurs, comme le transport. Par exemple, supposons qu'un autocar connecté de la marque X ne puisse pas être vendu au Québec parce qu'il fait fi d'un certain nombre de lois quant au respect de la vie privée. Or, supposons que les règles québécoises ne s'appliquent pas aux États-Unis, et qu'une compagnie américaine faisant affaire au Québec possède des autocars de la marque X. Dans un tel scénario hypothétique, le législateur fera face à un dilemme : ou bien il laisse l'entreprise américaine utiliser ses autocars en sol québécois, ou bien il la soumet aux règles québécoises. Dans les deux cas, un conflit se dessine : ou bien les règles québécoises en vigueur ne seront pas pleinement appliquées (et inéquitables à l'égard des entreprises locales), ou bien les conditions réglementaires spécifiques du Québec dissuaderont certaines entreprises étrangères d'offrir leurs services dans la province. Des problèmes similaires pourront être observés avec n'importe quel objet connecté circulant d'un pays à l'autre.

Ainsi, la législation québécoise devrait idéalement être sensible à celles de ses principaux partenaires d'affaires, notamment le Canada et les États-Unis. Une législation cohérente d'un État à l'autre facilite la mise en vigueur des politiques retenues (ce qui s'accorde mieux avec le critère d'effectivité). Cela ne signifie pas pour autant que le Québec doive imiter la législation de ses partenaires commerciaux. Le Québec peut être innovant et tenter de convaincre ses principaux partenaires commerciaux d'adopter des politiques communes en matière de données collectées dans les objets connectés[54]. Mais ultimement, même en l'absence d'un accord sur des règles communes, le Québec a intérêt à légiférer ou à s'assurer que les règles en vigueur sont respectées.

Établir des politiques cohérentes avec celles de nos principaux partenaires commerciaux peut être un casse-tête. Dans un souci de simplifier la tâche au gouvernement du Québec, la Commission a rédigé le présent document avec cet objectif de cohérence en tête. Par exemple, le Commissariat à la protection de la vie privée du Canada a récemment publié un rapport sur la réforme des lois sur la vie privée (2019). Les recommandations du présent document sont cohérentes avec celles du Commissariat : elles sont neutres sur le plan technologique[55], sont soucieuses d'une application simple et efficace[56], accordent de l'importance au consentement de qualité sans s'y limiter[57], rappellent l'importance du principe de proportionnalité[58], et ainsi de suite.

54 Pensons, à titre comparatif, aux politiques audacieuses de certains États américains, comme la Californie, pour réduire les émissions de gaz à effet de serre produites par les voitures. La question qui se pose pour les décideurs est de savoir s'il est préférable d'innover ou d'attendre que d'autres États mettent des politiques similaires en place. Cette question dépasse le cadre du présent document.
55 Comme suggéré par le Commissariat (2019, p. 11).
56 *Ibid.*, p. 13.
57 *Ibid.*, p. 14.
58 *Ibid.*, p. 15.

Recommandation 1
La Commission recommande au gouvernement du Québec de se coordonner avec ses principaux partenaires commerciaux pour adopter des lois et des standards encadrant la collecte de données par l'Internet des objets.

Recommandation 2
Afin de protéger la vie privée des citoyens, la Commission recommande au gouvernement du Québec d'étudier la possibilité de créer un mécanisme de certification des objets connectés. Différentes possibilités s'offrent au gouvernement du Québec quant à la mise en place et au mode de gestion de ce mécanisme. À des fins d'illustration, la Commission en souligne trois : (i) Un nouvel organisme indépendant réunissant des experts de différents domaines, comme le génie, le droit et la sécurité informationnelle, pourrait être responsable de cette certification. (ii) Un organisme existant ayant un mandat connexe pourrait aussi, grâce à un mandat supplémentaire et à de nouvelles ressources, être responsable de cette certification. (iii) Des membres des ordres professionnels pourraient être responsables de la délivrance d'attestations de conformité pour les outils de collecte de données personnelles.

3.2 Qui assume les responsabilités éthiques associées à l'Internet des objets?

On ne peut pas raisonnablement s'attendre à ce que les consommateurs soient totalement responsables de la protection de leur vie privée et des données qu'ils transmettent via les objets connectés. Plutôt que d'imposer cette charge aux individus, il serait plus judicieux de responsabiliser les institutions étatiques et les compagnies développant ces objets.

Les consommateurs sont constamment sollicités pour donner leur consentement sur divers sujets. Le consommateur responsable idéal devrait lire attentivement tous ses contrats, toutes les conditions d'utilisation des objets et logiciels qu'il utilise et comprendre tous les termes et tous les énoncés contenus dans ces politiques.

Par exemple, supposons que le consommateur responsable idéal veuille utiliser l'application photo d'une grande compagnie de vente en ligne. S'il est pleinement responsable, il devra lire attentivement un document juridique (rédigé en anglais) et maîtriser tous les termes techniques et légaux contenus dans le document[59]. Si le document compte plus d'une dizaine de pages, il lui faudra au moins une heure pour le lire (mais si le document a un indice de complexité élevé, il pourrait devoir y consacrer plus de temps)[60]. Ensuite, le consommateur responsable idéal pourrait avoir terminé de lire tous ces documents et, s'il accepte les clauses du contrat en toute connaissance de cause, utiliser cette application. Naturellement, dès que les documents juridiques seront mis à jour, le consommateur devra répéter l'exercice.

Nous pourrions dire la même chose à propos des entreprises qui vendent des objets connectés. À l'instar des consommateurs, les entreprises rattachées aux commerces de détail devraient aussi être au fait de toutes ces subtilités juridiques.

59 Pensons aux licences logicielles tierces d'Amazon Photos, disponibles à cette adresse : https://s3-us-west-2.amazonaws.com/customerdocumentation/Amazon+Photos/Third+Party+Licenses.html (page consultée le 16 avril 2019). Voir aussi Allhoff et Henschke (2018, p. 57).
60 La complexité des conditions d'utilisation peut être mesurée de différentes manières. Par exemple, Luger, Moran et Rodden (2013) ont proposé un indice de complexité qui prend en compte le nombre de phrases, la longueur moyenne des phrases et le nombre de mots polysyllabiques. Selon cet indicateur, les conditions d'utilisation et les politiques de confidentialité de certaines entreprises sont plus complexes que des ouvrages classiques comme la *Bible*, *Guerre et Paix* ou *Les Misérables*.

Cet idéal de la consommation (ou de la vente) responsable est inefficace et difficilement atteignable. Les consommateurs et les commerçants n'ont pas tous les mêmes connaissances techniques pour lire et comprendre des conditions d'utilisation détaillées. Et ceux qui disposent de ces connaissances ne devraient pas avoir à prendre une part déraisonnable de leur temps pour lire, apprendre et démêler tous les documents juridiques en cause. L'utilité collective l'oblige : la perte de temps et d'énergie résultant de la responsabilisation excessive des consommateurs et des commerçants crée plus de coûts que de bénéfices.

On peut donc s'attendre à ce qu'un encadrement provienne des États et protège utilisateurs et commerçants, quelles que soient les conditions d'utilisation propres à un objet connecté. En d'autres termes, le consommateur devrait pouvoir supposer qu'il dispose de certaines protections juridiques, et non devoir vérifier au cas par cas si ces protections sont prévues dans les conditions d'utilisation d'un objet connecté spécifique.

Recommandation 3
Le fardeau de la protection de la vie privée ne devrait pas revenir exclusivement aux citoyens et aux utilisateurs d'objets connectés. La Commission recommande plutôt au gouvernement du Québec d'instaurer des protections minimales par défaut des données collectées par les objets connectés.

Recommandation 4
La Commission recommande au gouvernement du Québec de favoriser l'approfondissement des connaissances touchant les méthodes de protection de la vie privée pour les objets connectés. À titre d'illustration, le gouvernement pourrait subventionner, via les Fonds de recherche du Québec, des projets de recherche sur cette question.

3.3 Comment améliorer la qualité du consentement?

Comme l'indiquent les orientations développées dans la section 3.2, l'idéal du consommateur pleinement responsable n'est sans doute pas atteignable. Cependant, des mesures devraient être mises en place pour améliorer, autant que possible, la qualité du consentement. Après tout, le consentement libre, éclairé et continu demeure un facteur clé du respect de l'autonomie des agents.

Des politiques doivent être mises de l'avant pour que les consommateurs d'objets connectés aient plus facilement accès aux informations pertinentes et aux paramètres de transfert de données. Ces politiques auront aussi pour effet de réduire la charge mentale des consommateurs et des vendeurs d'objets connectés, ce qui augmente l'utilité collective.

À titre indicatif, nous proposons ici trois exemples concrets de méthodes pour faciliter l'accès aux informations pertinentes et aux paramètres de transfert de données. La Commission ne montre aucune préférence entre ces méthodes. Le but est de dégager différentes options pour améliorer la qualité du consentement et réduire la charge mentale des acteurs concernés, et d'en cerner les forces et les faiblesses.

1. **Des règles entourant l'étiquetage.** À l'instar de l'étiquetage sur les vêtements pour informer les consommateurs des matériaux et de l'entretien, sur les appareils de cuisson et les électroménagers pour informer les consommateurs de la consommation énergétique, ou du tableau de la valeur nutritive sur les aliments[61], le gouvernement pourrait mettre en place une politique d'étiquetage des objets connectés. Par exemple, une étiquette standardisée pourrait être apposée à un endroit précis du véhicule. Elle pourrait rendre saillantes certaines informations de base, comme les types de données transmises, le chiffrement des données ou les protocoles de sécurité employés. Elle pourrait aussi indiquer si le fabricant a satisfait à certaines normes internationales[62]. Le fait que ces informations soient facilement consultables améliore la qualité du consentement, puisque l'utilisateur est mieux en mesure de repérer les informations pertinentes pour prendre une décision éclairée. Cependant, cette solution pourrait être difficile à appliquer aux objets partagés. Prenons l'exemple des véhicules connectés : certains modes de transport partagés, comme le taxi ou le train, se prêtent mal à de telles politiques d'étiquetage. De plus, cette solution ne permet pas à l'utilisateur de prendre en charge et de gérer facilement la collecte de ses données. Cette solution permet seulement à l'utilisateur d'être au fait des informations collectées par le véhicule.
2. **La relation professionnel-client et les profils de risque.** Les représentants en investissement faisant affaire au Canada doivent (i) dresser le profil de risque financier de leurs clients investisseurs et (ii) leur offrir des produits de placement qui conviennent à leurs préférences en matière de risque[63]. De manière analogue, les compagnies qui vendent des objets connectés au Canada pourraient être dans l'obligation de cibler les préférences du consommateur (en termes de sécurité et de vie privée) et de lui suggérer d'acheter des objets connectés qui correspondent à ses préférences. Par exemple, un consommateur ayant un profil prudent pourrait se tourner vers les objets connectés ayant de plus hauts standards de sécurité ou collectant peu d'informations personnelles. Ces mesures pourraient améliorer la qualité du consentement, puisque l'utilisateur connaîtrait mieux ses préférences et les risques qu'il encourt selon les différents appareils. Cependant, tout comme l'approche par l'étiquetage, cette solution pourrait être difficile à appliquer à certains objets connectés partagés. De plus, cette solution ne permet pas à l'utilisateur de prendre en charge et de gérer facilement la collecte de ses données. Enfin, cette solution pourrait être coûteuse et difficile à implanter dans les entreprises qui ont de nombreux clients ponctuels (comme une compagnie qui loue des vélos connectés).

61 Agence canadienne d'inspection des aliments 2019; Bureau de la concurrence Canada 2018; Gouvernement du Canada 2019; Ressources naturelles Canada 2019.
62 Par exemple, l'Organisation internationale de normalisation (ISO) développe présentement le standard « Protection des consommateurs : respect de la vie privée assuré dès la conception des biens de consommation et services aux consommateurs » (ISO/PC 317).
63 Chambre de la sécurité financière (s. d.).

3. **Les logiciels médiateurs.** Une autre option serait d'exiger des entreprises développant des objets connectés qu'elles intègrent un « logiciel médiateur » (*middleware*) de gestion des données aux objets. Comme son nom l'indique, ce logiciel ferait la médiation entre deux autres modules[64]. Par exemple, dans le cas des technologies médicales connectées, le logiciel médiateur pourrait gérer la transmission des données entre un stimulateur cardiaque connecté et l'équipe de soignants du patient. Le logiciel médiateur pourrait permettre à l'utilisateur de décider quelles données peuvent être collectées, agrégées et transmises par l'objet à des tiers. Non seulement cette solution est déjà en cours de développement ailleurs[65], mais elle permet à l'utilisateur d'être consulté, informé et de prendre en charge la collecte de ses données. La qualité du consentement serait donc grandement améliorée par une telle mesure. Or, cette solution pourrait avoir peu d'effets sur la charge mentale de certains consommateurs (par exemple, un consommateur d'objets connectés pourrait être appelé à configurer tous les objets connectés qu'il possède ou utilise, ce qui peut être exigeant).

Précisons aussi que l'amélioration de la qualité du consentement est particulièrement importante dans certains secteurs de pointe de l'Internet des objets. Pensons, à titre d'exemple, au marché des objets connectés pour les personnes âgées ou en perte d'autonomie[66].

Des spécialistes des sciences sociales et du développement technologique ont commencé à se pencher sur les promesses de l'Internet des objets pour résoudre ou atténuer des problèmes actuels et potentiels de la vieillesse et de la perte d'autonomie[67]. Ces écrits se concentrent principalement sur les aînés, qui développent avec l'âge des limitations physiques et/ou cognitives à divers degrés. Ces constats pourraient dans plusieurs cas s'appliquer aux non-aînés (par exemple, à toute personne atteinte de maladies dégénératives).

Les objets connectés développés spécifiquement pour les personnes en perte d'autonomie et les personnes âgées peuvent aller des capteurs de pression et rappels de prendre ses médicaments, aux systèmes de surveillance et de détection de chute. Ceux qui sont le plus discutés dans la littérature traitent des objets connectés portatifs (ou *wearables*) et domotiques pour le domicile. Les objets portatifs peuvent être munis de capteurs pour détecter les mouvements et divers indices physiologiques (comme les signes vitaux). L'objectif de ces outils intelligents est principalement d'assurer un suivi des données médicales et un environnement plus sécuritaire et plus confortable aux personnes en perte d'autonomie (Dohr *et al.*, 2010).

Les personnes en perte d'autonomie sont vulnérables. C'est pourquoi il est particulièrement important de faciliter leur consentement libre et éclairé. Comme l'explique Marjolaine Laroche dans son mémoire *L'éthique du* care *: les enjeux de la relation de soin asymétrique* (2018) :

> La relation de soin asymétrique se caractérise par l'écart en termes de vulnérabilité et de pouvoir entre la personne dispensant le soin et la personne recevant le soin. Dans la relation médicale, la compétence côtoie la fragilité humaine. En effet, cette relation se déroule entre personnes inégales tant par leur savoir que par leur capacité de prendre soin d'elles-mêmes. Le savoir et le pouvoir risquent de déboucher sur des abus et des injustices (Laroche 2018, p. 46).

64 À noter qu'il est presque essentiel de développer de tels logiciels médiateurs, ne serait-ce que pour relier différents objets connectés entre eux (Mineraud, Mazhelis, Su et Tarkoma 2016). La question à se poser, dès lors, est : devrions-nous exiger de ces logiciels qu'ils permettent à l'utilisateur de contrôler quelles données il transmet?

65 Pensons au logiciel SecKit (Neisse, Steri, Fovino et Baldini 2015). Voir Mineraud, Mazhelis, Su et Tarkoma (2016) pour un survol d'autres solutions.

66 Sur cette question, voir les travaux de Camarinha-Matos *et al.* (2014), Dobre *et al.* (2016), Dohr *et al.* (2016), Jara *et al.* (2011), Kulkani et Sathe (2014), Laplante et Laplante (2014), Monekosso *et al.* (2014), Pasluosta *et al.* (2015) et Qi *et al.* (2017).

67 Le degré d'autonomie qu'une personne possède peut se mesurer et s'évaluer de diverses manières : les indicateurs retenus peuvent inclure l'orientation (ex. spatiale et temporelle), l'hygiène et l'habillement, l'alimentation, l'élimination des besoins naturels, les déplacements intérieurs et extérieurs et les capacités de communication (Caisse Nationale de l'Assurance Maladie des Travailleurs Salariés 2008).

Aux fins de la présente section, voici ce qu'il faut retenir. Il est beaucoup plus facile de bafouer le droit au consentement libre, éclairé et continu des personnes en perte d'autonomie. Ces personnes sont vulnérables sur les plans physique (capacité moindre à s'exprimer, à bouger, etc.) et épistémique (manque d'expertise, manque d'accès aux informations pertinentes, etc.). Sachant cela, nous devons porter une attention particulière à la mise en place de mécanismes favorisant un consentement de qualité. Plus que quiconque, cette population saurait bénéficier des mesures décrites dans cette section.

Le même genre d'argument vaut pour les personnes mineures ou qui n'atteindront jamais la pleine autonomie.

Recommandation 5
La Commission recommande au gouvernement du Québec de mettre en place des politiques favorisant (i) une compréhension facile et claire des politiques d'utilisation des objets connectés et (ii) la prise en charge, par les utilisateurs, des données qu'ils transmettent à des tierces parties. À titre d'exemple, le gouvernement du Québec pourrait mettre en place de nouvelles règles concernant l'étiquetage, la vente ou la conception des objets connectés.

Recommandation 6
La Commission recommande au gouvernement du Québec de porter une attention particulière à la mise en place de ces politiques pour les objets visant des populations non autonomes ou pouvant être en situation de vulnérabilité. Pensons, par exemple, aux personnes mineures, en perte d'autonomie, ou aux personnes qui n'atteindront jamais la pleine autonomie. Ces mesures viseraient à faciliter un consentement de qualité pour des populations particulièrement exposées à des risques éthiques. Également, la Commission recommande au Secrétariat aux aînés de porter une attention particulière à ces politiques touchant les objets connectés destinés aux personnes âgées, et ce, pour les mêmes raisons. Les objets connectés médicaux pour assister les personnes âgées ou en perte d'autonomie pourraient faire l'objet d'un encadrement plus poussé.

3.4. Comment concevoir la propriété des données recueillies par l'Internet des objets?

Le problème ici consiste à trouver une juste application du principe de propriété (un corollaire du respect de la liberté) à la question des données recueillies. En effet, le propriétaire d'un bien (comme un jeu de données) devrait pouvoir en profiter comme bon lui semble dans le respect des limites prévues par la loi. La question difficile est de savoir qui détient ce droit dans le cas des données collectées par des objets connectés. Il semble que les consommateurs possèdent les données recueillies par leurs objets connectés. D'un autre côté, ce sont des entreprises privées, et non l'utilisateur, qui transforment l'information disponible en données. Il y a donc des raisons de penser que les données devraient appartenir à l'individu, mais d'autres raisons de penser qu'elles devraient appartenir à l'entreprise qui les captent.

Une première piste à suivre pour résoudre cette tension est de traiter ce problème de propriété en deux temps. Dans un premier temps, les consommateurs possèdent les informations privées les concernant, et qui servent à faire des données. Dans un second temps, les compagnies et les États, s'ils sont autorisés à accéder à ces informations privées, peuvent construire des données à partir des informations du consommateur. En d'autres termes, l'information privée est un bien dont jouit l'individu, alors que la construction de données (sur une base consentante) est un bien dont peuvent profiter les entreprises et les États.

Cette manière d'appréhender le problème est moins controversée qu'il n'y paraît. Il s'agit d'aborder le problème comme un cas courant de transformation d'un bien informationnel. Prenons un exemple simple. Des entreprises rédigent des communiqués de presse qui contiennent des informations privées (innovations, investissements, etc.). Ces documents appartiennent à l'entreprise qui les rédige. Or, l'entreprise diffuse ces communiqués et en autorise la réutilisation. Les médias s'en servent ensuite pour élaborer des nouvelles (sous la forme d'articles de journaux, de bulletins télévisés, etc.). Le communiqué de presse, un bien informationnel, se voit donc transformé en un autre bien informationnel par l'entreprise médiatique. Dans le cas des données collectées par les objets connectés, on observe un phénomène similaire : un bien informationnel (l'information privée d'un individu) est transformé en un autre bien informationnel (une donnée) par une entreprise sur une base consentante.

Quoiqu'il en soit, il faut faire une distinction entre *possession* et *usage* des données, et c'est l'usage des données qui pose un problème pour la vie privée, la surveillance et le contrôle des personnes. L'usage et la possession des données sont deux questions distinctes. Des entreprises privées ou des États pourraient ne posséder aucune donnée à propos de leurs utilisateurs, mais néanmoins y avoir accès et pouvoir les utiliser à diverses fins. Pensons, par exemple, aux fiducies de données, populaires dans le monde de la santé[68]. Une fiducie est un mode de gestion d'un objet ou d'une propriété pour une autre personne. Dans ce modèle, les patients possèdent toutes les données qui les concernent, mais les équipes de soignants peuvent y accéder (à certaines conditions) et les utiliser au bénéfice du patient. L'idée centrale du modèle fiduciaire est qu'une personne ou une institution peut accéder à des données ou les gérer sans les posséder. Inversement, une entreprise privée ou un État pourrait posséder les données à propos de ses utilisateurs, mais ne pas pouvoir les utiliser à diverses fins. Par exemple, la loi pourrait autoriser des entreprises à posséder des données, mais en interdire l'analyse, le croisement, la vente ou le transfert.

Il existe donc une différence notable entre la possession et l'usage des données. Les fiducies de données illustrent bien ce point. De plus, qu'un individu soit ou non le propriétaire de ses données, il a un droit de regard sur la création et l'utilisation de celles-ci. Dans ce contexte, les questions entourant la propriété des données recueillies par les objets connectés sont moins centrales qu'il n'y paraît. L'enjeu de propriété est subordonné à d'autres enjeux entourant le consentement et l'usage légitime des données.

Recommandation 7
La Commission souligne la distinction entre les questions de *possession* et d'*usage* des données collectées par les objets connectés. Avec cette distinction en tête, la Commission recommande au gouvernement du Québec de concentrer ses politiques publiques sur les *usages* acceptables des données collectées par des objets connectés.

3.5. Quelles garanties de sécurité numérique devraient être offertes à l'utilisateur?

Dans l'état actuel des choses, aucun environnement connecté ne peut être totalement sécuritaire et il serait vain d'exiger des compagnies ou des institutions publiques qu'elles soient infaillibles sur ce plan. On peut néanmoins s'attendre à ce que certaines mesures de *précaution* soient respectées par les entreprises développant les objets connectés et les acteurs collectant des données.

68 Voir aussi Element AI (s. d.) pour un survol des questions entourant les fiducies de données dans les nouveaux domaines technoscientifiques, comme l'intelligence artificielle.

D'abord, les compagnies impliquées dans le développement d'objets connectés devraient respecter les mesures de protection de la vie privée dans la conception des objets *(privacy by design)*. Les entreprises et des institutions gouvernementales devraient être en mesure de justifier d'éventuelles violations de ces principes, qui sont[69] :

1. **La prévention.** Il faut anticiper les événements qui peuvent compromettre la vie privée des utilisateurs et prévenir ces problèmes plutôt que de les corriger.
2. **La vie privée par défaut.** Les données personnelles doivent être protégées « par défaut ». En d'autres termes, même si les individus ne font rien ou sont peu prévoyants, leurs données devraient être protégées.
3. **La vie privée enchâssée dans l'objet.** Les éléments protégeant la vie privée des utilisateurs sont enchâssés dans la fabrication et l'architecture des objets, plutôt que d'être un ajout ultérieur à leur conception.
4. **Un jeu « à somme positive ».** Tous les intérêts sont pris en compte dans l'élaboration des logiciels et des objets. Il faut éviter les fausses dichotomies, telles que « la sécurité contre la vie privée ».
5. **Une protection couvrant tout le cycle d'utilisation.** Les mesures de protection et de sécurisation des données couvrent tout leur cycle de vie. Elles sont prises pour la collecte, l'entreposage et la destruction des données.
6. **La visibilité et la transparence.** Les pratiques d'affaires et les technologies sont vérifiables, transparentes et opèrent selon les objectifs décrits aux utilisateurs. Une vérification indépendante de ces pratiques est possible.
7. **Respect de la vie privée.** Les intérêts des utilisateurs sont au cœur de l'architecture et du mode de fonctionnement des technologies.

Parmi les pratiques concrètes qui se dégagent des sept principes ci-dessus, on peut penser à l'anonymisation des données. Les données collectées ne devraient pas être aisément associées à des personnes, que ce soit par l'identification des individus dans la base de données (identification directe) ou par la spécificité des données collectées (réidentification par déduction et recoupement). Pour certains objets connectés (comme les voitures personnelles ou les maisons intelligentes), une autre bonne pratique serait de donner la possibilité aux utilisateurs d'utiliser l'objet en mode « déconnecté ». Une partie des données peut alors être collectée et analysée tout en demeurant dans l'objet (*on-device data*)[70]. En plus de donner la liberté aux utilisateurs de transmettre ou non leurs données à des entreprises privées, cette mesure leur permettrait aussi de continuer à utiliser leurs biens en cas de faillite ou de détection d'une brèche de sécurité dans le système connecté de l'objet connecté. En d'autres termes, l'existence d'un mode « déconnecté » est une bonne mesure préventive.

Selon une interprétation stricte du principe de prévention, on pourrait conclure que certaines données trop sensibles ne devraient jamais être collectées par les objets connectés. C'est, après tout, une mesure préventive possible : empêcher la collecte de certaines données à partir des objets connectés est une méthode préventive de protection de la vie privée. Cependant, la Commission n'a pas retenu cette interprétation du principe de prévention.

69 Il existe différentes formulations des principes de *privacy by design*. Nous nous concentrons ici sur les principes (traduits et résumés) que l'on trouve chez Cavoukian (2010). Ils sont brièvement discutés et défendus dans l'avis de la Commission sur les nouvelles technologies de surveillance et de contrôle (2008, pp. 53-4).

70 Des limites de stockage pourraient expliquer pourquoi toutes les données générées par un objet connecté ne peuvent pas être stockées dans l'appareil.

On peut difficilement penser qu'il devrait y avoir des limites strictes et universelles quant à la collecte de données par les objets connectés. Certains citoyens ou consommateurs choisiront librement des appareils qui collectent bon nombre de leurs données si les incitatifs offerts en échange de ces données sont suffisamment attrayants[71]. Par exemple, plusieurs consommateurs consentiront à transmettre les données que leurs appareils collectent si cela améliore leur sécurité, leur donne accès à de nouveaux services gratuits, diminue les primes d'assurance du propriétaire ou lui donne accès à des rabais sur différents produits, et ainsi de suite. En d'autres termes, plusieurs consommateurs n'ont pas de problème à ce que des compagnies (et potentiellement des États) aient accès à leur vie privée *s'ils obtiennent quelque chose en échange*. Dans ce contexte, il n'y a pas nécessairement de conflit insoluble entre les principes d'utilité collective, de respect de la vie privée et de respect de la liberté. Tous les acteurs concernés peuvent y trouver leur compte.

Des enquêtes révèlent aussi que les citoyens ne sont pas préoccupés par la collecte de données *tout court,* mais bien par la collecte de données par certaines compagnies ou institutions. Par exemple, Walter et Abendroth (2018, §3.1) notent que, lorsqu'il est question de collecte et de traitement des données personnelles, les consommateurs font confiance aux services ambulanciers et policiers, mais moins aux entreprises privées, aux assureurs et aux développeurs d'applications pour appareils connectés. Cela tend à soutenir l'idée selon laquelle il ne faut pas forcément imposer des limites sur les données collectées, mais plutôt imposer des limites sur l'*usage* des données par différents acteurs. Par exemple, la collecte de certaines données très sensibles peut être permise si cela permet de sauver des vies, mais pas si cela vise simplement à augmenter les profits des entreprises. C'est l'utilisation des données qui pose problème, et non la collecte.

Recommandation 8
La Commission recommande au gouvernement du Québec d'incorporer les principes de protection de la vie privée dans la conception des objets *(privacy by design)* dans la Loi sur la protection des renseignements personnels. Les institutions étatiques ayant accès aux données collectées à partir des objets connectés et les entreprises développant ces objets devraient être contraintes de respecter ces principes.

Recommandation 9
En accord avec la deuxième recommandation du présent supplément, la Commission recommande aux futurs organismes de certification et aux professionnels impliqués dans le développement d'objets connectés d'établir des normes de sécurité appropriées pour les objets connectés.

Recommandation 10
Les mécanismes décrits dans les recommandations 2, 8 et 9 du présent document sont des solutions à long terme pour encadrer le développement des objets connectés. La Commission reconnaît cependant l'importance d'agir rapidement pour protéger la vie privée des citoyens. À court terme, la Commission recommande aux entreprises privées impliquées dans le développement d'objets connectés d'enchâsser les principes de protection de la vie privée dans la conception des objets connectés *(privacy by design)*.

71 Walter et Abendroth 2018.

3.6. Quelles sont les limites raisonnables entourant le stockage, la concentration, le traitement et la vente des données recueillies par les objets connectés?

En plus du respect des normes de consentement, de *privacy by design,* de proportionnalité et d'acceptabilité sociale discutées dans les sections précédentes, un principe général d'utilité collective doit guider le stockage, la concentration, le traitement ou la vente des données. Spécifiquement, l'utilité collective probable de stocker, de concentrer, de traiter et de vendre ces données doit être supérieure aux conséquences négatives probables touchant la vie privée des utilisateurs.

À des fins de clarté, on peut appliquer ce principe à quelques exemples simples :

1. **Données minimales.** Un manufacturier automobile veut entraîner ses robots de freinage et d'accélération avec des données réelles. Pour entraîner un algorithme d'apprentissage automatique, il importe et décrypte un bloc de données de ses serveurs. Or, l'entreprise devrait éviter de décrypter *toutes* les données sur ses utilisateurs. Pour cette tâche, le robot n'a pas besoin de connaître les noms des utilisateurs, leur date de naissance, leurs données socioéconomiques, leurs préférences musicales, etc.
2. **Données anciennes.** Une entreprise spécialisée dans les maisons intelligentes collecte des données sur les habitudes d'écoute télévisuelle des résidents. La valeur et la qualité de ces données diminuent grandement avec le temps[72]. Donc, l'entreprise ne conserve pas toutes les données qu'elle collecte et supprime les plus anciennes.
3. **Partenaires de confiance.** Une entreprise développant des stimulateurs cardiaques connectés est invitée à vendre ses données à une entreprise étrangère. L'entreprise ne sait pas si ce possible partenaire étranger est respectueux de la vie privée de ses clients ni à quelles fins les données seront utilisées. Par prudence, elle ne vend pas les données de ses clients à cette entreprise.
4. **Dérives sécuritaires.** Un État se demande s'il devrait réglementer quant à l'admissibilité en preuve de certaines données lors de procès. L'État sait que, si les données collectées dans les véhicules connectés ou les assistants vocaux personnels sont admissibles, cela pourrait mener à des dérives en termes de surveillance de la part des corps policiers et des services de renseignement[73]. Pour cette raison, l'État limite (ou balise) l'admissibilité en preuve des données collectées dans les véhicules connectés et les assistants vocaux personnels.
5. **Portes dérobées (*backdoors*).** Un État se demande s'il devrait exiger de certaines entreprises de lui fournir une porte dérobée (*backdoor*) dans des logiciels ou des serveurs. Essentiellement, ces portes servent à accéder aux données présentes sur un logiciel ou un serveur. Or, l'accès à ces portes est potentiellement désastreux. En effet, si la porte existe pour un État, elle existe aussi pour des malfaiteurs, le crime organisé, etc. Donc, accepter les portes dérobées implique un risque de perte de contrôle très grand sur les données recueillies à propos des citoyens[74]. Étant donné ce très grand risque, et étant donné qu'il existe d'autres méthodes pour accéder aux données collectées par les entreprises (comme les procédures déjà existantes devant les tribunaux), l'État n'exige pas l'accès à des portes dérobées dans les logiciels et les serveurs des entreprises.

72 Bucherer et Uckelmann 2011, p. 261.
73 Shahkari et Haugen 2018, p. 512.
74 Experts consultés.

Les acteurs qui collectent et analysent les données collectées doivent aussi faire preuve de transparence. En premier lieu, un environnement transparent permet d'établir une relation de confiance entre, d'une part, les consommateurs et le public, et d'autre part, les parties impliquées dans le développement des objets connectés. Un environnement marqué par la confiance favorise l'utilité collective (les entreprises développant des objets connectés ne trouveront pas d'acheteurs pour leurs produits sans avoir la confiance du public)[75]. En second lieu, un environnement transparent favorise la prise de décision éclairée pour les consommateurs et le public. En d'autres termes, plus les parties impliquées dans le développement des objets connectés sont transparentes, plus elles permettent aux utilisateurs de ces technologies de prendre des décisions éclairées. La transparence favorise donc également le principe de respect de la liberté.

Naturellement, dans certains contextes spéciaux, les entreprises pourraient justifier un certain degré de non-transparence. Par exemple, une entreprise pourrait choisir de ne pas divulguer certaines informations au grand public sur la base du secret industriel. Imaginons qu'une entreprise développant des maisons intelligentes conçoive un système de sécurité breveté basé sur de nouveaux indicateurs, comme les heures de sommeil ou le niveau d'éclairage dans certaines pièces. Si elle révélait publiquement qu'elle collecte des données sur les heures de sommeil des résidents à des fins de sécurité, l'entreprise dévoilerait une information concurrentielle importante concernant son programme de recherche et développement. Si l'on souhaite protéger la position concurrentielle de certaines entreprises, des mécanismes alternatifs de contrôle et de vérification (à l'instar des mécanismes de brevetage ou de contrôle des produits pharmaceutiques) pourraient prendre le relais. Par exemple, plutôt que de se justifier publiquement quant au fait qu'elle capte certaines données, l'entreprise pourrait exposer ses recherches dans le cadre d'audits confidentiels avec les agences gouvernementales responsables d'assurer la sécurité des objets connectés.

Malgré ces remarques, dans les scénarios ordinaires ou courants, une entreprise développant des objets connectés devrait être en mesure d'exposer publiquement ce qu'elle compte faire avec les données collectées auprès des utilisateurs. La non-transparence doit être l'exception plutôt que la règle.

75 *Ibid.*, p. 510; Allhoff et Henschke 2018, p. 62.

Recommandation 11

La Commission réitère l'importance de deux principes :

(i) Les entreprises et le gouvernement du Québec doivent respecter le principe de proportionnalité. Selon ce principe, les moyens mis en œuvre à des fins justifiées (sécurité, profitabilité, etc.) doivent être proportionnels aux fins qui sont poursuivies. Par exemple, mettre en place des moyens de surveillance trop intrusifs sur le plan de la vie privée compte tenu des fins visées et du contexte, tout comme collecter des données personnelles au-delà de ce qui est nécessaire à la finalité déclarée, serait inacceptable.

(ii) Le gouvernement du Québec doit être sensible à l'acceptabilité sociale. La population doit être favorable aux méthodes de surveillance préconisées par l'État, comme le recours aux données collectées par l'Internet des objets. De plus, cet appui populaire doit se baser sur une discussion collective réfléchie. Il importe donc aussi d'éduquer les citoyens quant aux implications de ces technologies sur leurs droits.

Recommandation 12

Lorsqu'il est question de pratiques socialement risquées, comme le stockage, de la concentration ou de la vente de données, la Commission recommande aux entreprises développant des objets connectés de considérer le fait qu'elles doivent faire preuve de prudence. Elles devraient notamment être en mesure de justifier raisonnablement en quoi l'utilité collective probable de stocker, de concentrer, de traiter et de vendre ces données est supérieure aux conséquences négatives probables touchant la vie privée des utilisateurs. Par exemple, une entreprise incapable d'expliquer pourquoi elle conserve toutes les données de ses utilisateurs (ou pourquoi elle collecte certaines données à leur sujet) ne peut justifier raisonnablement une pratique aussi risquée.

Recommandation 13

La Commission recommande au gouvernement du Québec d'imposer des normes de transparence aux entreprises collectant des données à partir des objets connectés. Dans les cas où une entreprise ne peut pas exposer publiquement ses pratiques de collecte, de stockage ou de traitement des données, le gouvernement du Québec devrait prévoir des mécanismes alternatifs de vérification des pratiques de l'entreprise. Il pourrait s'agir, par exemple, d'audits confidentiels avec les agences gouvernementales responsables d'assurer la sécurité des objets connectés.

4. PISTES DE RÉFLEXION FUTURES

Ce document propose une réflexion éthique sur la place de la vie privée dans la conception et le développement des objets connectés. Il supplée un avis étudiant les nouvelles technologies de surveillance, publié en 2008 par la Commission. Dans la précédente section, treize recommandations ont été proposées. Elles s'adressent à différents acteurs, comme le gouvernement du Québec, les entreprises et les ordres professionnels.

En guise de conclusion, nous tenons à souligner des aspects du problème qui auraient pu être explorés davantage dans ce supplément. D'autres recherches seront nécessaires pour cerner les implications éthiques de ces facettes du problème.

D'une part, dans ce supplément, la vie privée a été analysée sous un angle individuel. Nous nous sommes concentrés sur les invasions de la vie privée que peuvent subir des personnes prises séparément. Or, depuis quelques années, on constate un intérêt pour le concept de vie privée de groupe. Comme l'indiquent Taylor, Floridi et van der Sloot :

> À l'ère des données massives, où les analyses sont développées pour s'appliquer à une échelle aussi large que possible, l'individu est souvent relégué au second plan. Les technologies d'analyse des données sont plutôt orientées vers les groupes. [...] Les types d'actions et d'interventions qu'elles facilitent sont destinés à aller au-delà des individus. C'est précisément la valeur des grandes données : elles permettent à l'analyste d'avoir une vision plus large, de tendre vers l'universel. [...] L'analyse des données [...] peut aboutir à des décisions qui présentent des risques réels au niveau agrégé, pour des groupes de personnes (Taylor *et al.* 2017, p. 2, traduction libre).

Le rôle des groupes soulève aussi des questions de responsabilité partagée. Le développement de l'Internet des objets se fait par la collaboration et l'interaction entre plusieurs spécialistes et entreprises. L'intégration de chacun des acteurs dans le développement de cette technologie fait en sorte qu'on peine à distinguer les responsabilités (juridiques et éthiques) de chacun des acteurs impliqués. Pour certains auteurs, ce genre de situations devrait nous amener à réfléchir à la responsabilité sous un angle collectif. Par exemple, Tracy Isaacs écrit :

> Certaines actions sont réalisées par des collectifs, et non par des individus isolés. Parmi ces actions, certaines au moins ont une dimension morale et peuvent être évaluées — et même devraient être évaluées — en termes moraux comme étant bonnes ou mauvaises. Dans cette mesure, elles sont l'objet de la responsabilité morale, et les agents qui les accomplissent peuvent être blâmables ou louables. Dans le cas des actions collectives, ce sont les agents collectifs qui sont blâmables ou louables. Les individus qui contribuent au résultat ne peuvent pas — en réalité — exécuter ou avoir l'intention d'exécuter l'ensemble de l'acte, même s'ils peuvent partager l'objectif collectif et contribuer à sa réalisation (Isaacs 2011, p. 55, traduction libre).

Des analyses futures pourront permettre de mieux comprendre quelles protections sont nécessaires pour bien protéger la vie privée des groupes, et comment bien rendre justice aux questions de responsabilité partagée.

D’autre part, les questions de sécurité des objets connectés ont été laissées de côté dans ce document. Voulant suppléer l’avis de 2008 sur la protection de la vie privée des citoyens, le présent document s’est surtout concentré sur cette question. Or, une part importante (et grandissante) de la littérature sur les objets connectés s’intéresse à la sécurité des utilisateurs de ces objets. Pensons, par exemple, aux systèmes des voitures connectées qui peuvent être piratés et mettre en péril la conduite, aux objets médicaux connectés mal sécurisés qui, une fois piratés, peuvent mettre en danger les patients, et ainsi de suite (Schneier 2018). Des recherches futures sur les politiques de sécurité entourant les objets connectés pourraient être pertinentes.

BIBLIOGRAPHIE

Ackerman, S. et S. Thielman. 2016. « US intelligence chief: we might use the Internet of things to spy on you », *The Guardian,* 9 février

Administrateur général des données. 2017. *La donnée comme infrastructure essentielle. Rapport au premier ministre sur la donnée dans les administrations 2016-2017.* La documentation française

Agence canadienne d’inspection des aliments. 2019. « Exigences en matière d’étiquetage des boissons alcoolisées ». En ligne : http://www.inspection.gc.ca/aliments/exigences-et-documents-d-orientation/etiquetage-normes-d-identite-et-classification/pour-l-industrie/alcool/fra/1392909001375/1392909133296 (page consultée le 19 mars 2019)

Allhoff, F. et A. Henschke. 2018. « The Internet of Things: Foundational ethical issues », *Internet of Things* 1–2: 55-66. DOI: 10.1016/j.iot.2018.08.005

Arendt, H. 1958. *The Human Condition*. Chicago: The University of Chicago Press

Baldini, G., Botterman, M., Neisse, R. et M. Tallacchini. 2018. « Ethical Design in The Internet of Things », *Science Engineering Ethics* 24: 905-925. DOI: 10.1007/s11948-016-9754-5

Benn, S. I. 1971. « Privacy, Freedom, and Respect for Persons », 1-26, dans Ciochon, R. L. (dir.), *Privacy and Personality,* New York: Atherton Press

Benyekhlef, K. et Déziel, P-L. 2018. *Le droit à la vie privée au Canada et au Québec*. Montréal : Éditions Yvon Blais

Berkman Centre. 2016. *« Don’t panic : making progress on the «going dark» debate »,* Cambridge: Berkman Centre for Internet and Society at Harvard

Bloustein, E. J. 1964. « Privacy as an aspect of human dignity: an answer to Dean Prosser », *New York University Law Review* 39: 962-1007

Boucher, F. 2018. « Données massives et droit à la vie privée : enjeux éthiques ». Document produit pour la Commission de l’éthique en science et en technologie

Bucherer, E. et D. Uckelmann. 2011. « Business Models for the Internet of Things »: 253-77. Dans *Architecting the Internet of Things,* édité par D. Uckelmann, M. Harrison et F. Michahelles, Berlin et Heildelberg: Springer-Verlag

Bureau de la concurrence Canada. 2018. « Étiquetage des textiles ». En ligne : https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/h_02940.html (page consultée le 19 mars 2019)

Caisse Nationale de l’Assurance Maladie des Travailleurs Salariés (CNAMTS). 2008. « Le modèle ‘AGGIR’. Guide d’utilisation », Paris : Gouvernement de la France

Camarinha-Matos, L.M. *et al.* 2014. « Care services provision in ambient assisted living », *IRBM* 35 (6): 286-298

Canto-Sperber, M. et R. Ogien. 2006. *La philosophie morale,* Paris : Presses universitaires de France (collection « Que sais-je? »)

Cavoukian, A. 2010. « Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. », *Identity in the Information Society* 3 (2): 247–251. DOI: 10.1007/s12394-010-0062-y

Chambre de la sécurité financière. s. d. « Profil d’investisseur ». En ligne : https://www.chambresf.com/fr/info-deonto/relation-client/connaissance-du-client/profil-dinvestisseur/ (page consultée le 16 avril 2019)

Cohen, J. E. 2000. « Examined Lives: Informational Privacy and the Subject as Object », *Georgetown Law Faculty Publications and Other Works,* 810: 1373-1437

Commissariat à la protection de la vie privée du Canada. 2019. *Réforme des lois sur la vie privée. Pour faire respecter les droits et rétablir la confiance envers le gouvernement et l’économie numérique.* Gatineau : Commissariat à la protection de la vie privée du Canada

Commission de l'éthique en science et en technologie. 2003. *Pour une gestion éthique des OGM.* Sainte-Foy : Commission de l'éthique en science et en technologie

Commission de l'éthique en science et en technologie. 2008. *Viser un juste équilibre : un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité.* Québec : Commission de l'éthique en science et en technologie

Commission de l'éthique en science et en technologie. 2016. *Enjeux éthiques liés au trading haute fréquence.* Québec : Commission de l'éthique en science et en technologie

Commission de l'éthique en science et en technologie. 2017. *La ville intelligente au service du bien commun.* Québec : Commission de l'éthique en science et en technologie

DeCew, J. 2018. « Privacy », *The Stanford Encyclopedia of Philosophy,* édité par Edward N. Zalta

Dietsch, P. 2008. « L'interprétation du principe de la propriété de soi au sein du libertarisme de gauche », *Dialogue* 47 (1): 65-80

Dobre, Ciprian et al. 2016. *Ambient assisted living and enhanced living environments.* Oxford: Butterworth-Heinemann

Doctorow, C. 2015. « Technology should be used to create social mobility, not to spy on citizens », *The Guardian,* 10 mars

Dohr, A., *et al.* 2010. « The Internet of Things for Ambient Assisted Living », 804-809, dans *2010 Seventh International Conference on Information Technology: New Generations,* Las Vegas

Element AI, s. d. « Fiducies de Données. Un nouvel outil pour la gouvernance des données », En ligne : https://hello.elementai.com/rs/024-OAQ-547/images/Fiducies_de_Donnees_FR_201914.pdf (page consultée le 14 novembre 2019)

Estlund, D. 2014. « Utopophobia », *Philosophy & Public Affairs* 42 (2): 113–134

Fried, C. 1968. « Privacy: A moral analysis », *Yale Law Journal* 77 (3): 475-493

Fowler, G. A. 2019. « What does your car know about you? We hacked a Chevy to find out », *The Washington Post,* 19 décembre

Gaus, G. 2016. *The Tyranny of the Ideal: Justice in a Diverse Society,* Princeton: Princeton University Press

Gouvernement du Canada. 2019. « Tableau de la valeur nutritive ». En ligne : https://www.canada.ca/fr/sante-canada/services/comprendre-etiquetage-aliments/tableau-valeur-nutritive.html (page consultée le 19 mars 2019)

Hardin, G. 1968. « The Tragedy of the Commons », *Science* 162 (3859): 1243-1248

Hern, A. 2015. « Samsung rejects concern over 'Orwellian' privacy policy », *The Guardian,* 9 février

Hern, A. 2017. « «Am I at risk of being hacked?» What you need to know about the 'Vault 7' documents », *The Guardian,* 8 mars

Hittinger, E., et Jaramillo, P. (2019). « Internet of Things: Energy boon or bane? », *Science* 364 (6438): 326-328

Jara, A. J., Zamora, M. A., et Skarmeta, A. F. G. 2011. « An internet of things–based personal device for diabetes therapy management in ambient assisted living (AAL) », *Personal and Ubiquitous Computing* 15 (4): 431-440

Isaacs, T. 2011. *Moral Responsibility in Collective Contexts.* Oxford: Oxford University Press

Kurnicki, K. et Salamon, K. 2012. « Sociological and philosophical insight into privacy in postmodern cities », 75-87, dans Carucci, Margherita (dir.), *Revealing Privacy: Debating the Understandings of Privacy,* New York: Peter Lang

Landry, Normand et Anne-Sophie Letellier (éd.). 2016. *L'éducation aux médias à l'ère numérique,* Montréal : Presses de l'Université de Montréal

Laplante A. P. et Laplante, N. 2016. « The Internet of Thins in Healthcare: Potential Applications and Challenges », *IEEE Computer Society:* 2-4

Laroche, M. 2018. L'*éthique du* care *: les enjeux de la relation de soin asymétrique.* Mémoire, Université de Sherbrooke. En ligne : http://hdl.handle.net/11143/14478 (page consultée le 7 octobre 2019)

Lever, A. 2013. *A Democratic Conception of Privacy.* Bloomington: AuthorHouse

Ligue des droits et libertés. 2016. *Remettre les droits humains au centre de nos politiques de sécurité.* Mémoire présenté au Comité parlementaire sur la sécurité publique et nationale. Montréal : Ligue des droits et libertés

Lipsey, R. G. et K. Lancaster. 1956. « The General Theory of Second Best », *The Review of Economic Studies* 24 (1): 11–32

Luger, E., Moran, S., & Rodden, T. 2013. « Consent for all: revealing the hidden complexity of terms and conditions » dans *Proceedings of the SIGCHI conference on Human factors in computing systems:* 2687-2696

McArdle, E. 2016. « The new age of surveillance », *Harvard Law Today,* 10 mai

McCarthy, S. 2015. « 'Anti-petroleum' movement a growing security threat to Canada, RCMP say », *The Globe and Mail,* 17 février

Mill, J. S. 2008 (1871). *L'utilitarisme* (traduction de P. Folliot), Chicoutimi : Les Classiques des sciences sociales. DOI : 10.1522/000202188

Mindle, G. B. 1989. « Privacy, and Autonomy », *The Journal of Politics* 51 (3): 575-598

Mineraud, J., Mazhelis, O., Su, X. et S. Tarkoma. 2016. « A gap analysis of Internet-of-Things platforms », *Computer Communications* 89-90 : 5-16. DOI : 10.1016/j.comcom.2016.03.015

Monekosso, D., Florez-Revuelta, F. et Remagnino, P. 2015. « Ambient Assisted Living », *IEEE Intelligent Systems* 30 (4): 2-6

Nagel, T. 1998. « Concealment and Exposure », *Philosophy & Public Affairs* 27 (1): 3-30

Neisse, R., Steri, G., Fovino, I. N. et G. Baldini. 2015. « SecKit: A Model-based Security Toolkit for the Internet of Things », *Computers & Security* 54: 60-76. DOI: 10.1016/j.cose.2015.06.002

Nissenbaum, Helen. 2009. *Privacy In Context: Technology, Policy, and the Integrity of Social Life,* Stanford University Press

Nozick, R. 1974. *Anarchy, State, and Utopia,* New York: Basic Books

Okin, S. M. 1989. *Justice, gender, family,* New York: Basic Books

O'Neill, O. 2004. « Autonomie : Le Roi est Nu », *Raison publique 2.* En ligne : http://www.raison-publique.fr/article171.html (page consultée le 16 avril 2019)

Open Internet of Things Assembly. 2012. En ligne : https://www.postscapes.com/open-Internet-of-things-assembly/ (page consultée le 16 avril 2019)

Organisation internationale de normalisation, « ISO/PC 317. Protection des consommateurs : respect de la vie privée assuré dès la conception des biens de consommation et services aux consommateurs ». En ligne : https://www.iso.org/fr/committee/6935430.html (page consultée le 16 avril 2019)

Ostrom, E. 1990. *Governing the Commons,* Cambridge: Cambridge University Press

Paperman, P. 2015. « L'éthique du *care* et les voix différentes de l'enquête », *Recherches féministes* 28 (1) : 29-44

Pasluosta, C. *et al.* 2015. « An Emerging Era in the Management of Parkinson's Disease: Wearable Technologies and the Internet of Things », *IEEE Journal of Biomedical and Health Informatics* 19 (6): 1873-1881

Petrou, M. 2017. « Surveillance in Canada: who are the watchers? », *OpenCanada,* 6 juillet

Porup, J.M. 2016. « The Internet of things is a surveillance nightmare », *The Daily Dot,* 20 mars

Posner, R. A. 1978. « An Economic Theory of Privacy », *Regulation:* 19-26

Powles, J. 2015. « Internet of things: the greatest mass surveillance infrastructure ever? », *The Guardian,* 15 juillet

Qi, J. *et al.* 2017. « Advanced internet of things for personalised healthcare systems: A survey », *Pervasive and Mobile Computing* 41: 132-149

Rachel, J. 1975. « Why Privacy Is Important », *Philosophy & Public Affairs* 4 (4): 323-333

Ferradini, B. 2019. « Trans Mountain a mis des militants antipipeline sous surveillance », Radio-Canada, 25 novembre. En ligne : https://ici.radio-canada.ca/nouvelle/1404556/trans-mountain-surveillance-militants-pipeline-autochtones (page consultée le 28 novembre 2019)

Räikkä, J. 2008. « Is Privacy Relative? », *Journal of Social Philosophy* 39 (4): 534-546

Rawls, J. 1993. *Libéralisme politique*. Paris : Presses Universitaires de France

Rawls, J. 1997. *Théorie de la justice*. Paris : Seuil

Ressources naturelles Canada. 2019. « Appareils de cuisson ». En ligne : https://www.nrcan.gc.ca/energy/products/categories/appliances/cooking/13987 (page consultée le 19 mars 2019)

Reiman, J. H. 1995. « Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Information Technology of the Future », *Santa Clara High Technology Law Journal* 11 (1): 27-44

Reiman, J. H. 1976. « Privacy, Intimacy, and Personhood », *Philosophy & Public Affairs* 6 (1): 26-44

Roman, R., Najera, P. et J. Lopez. 2011. « Securing the Internet of Things », *Computer* 44 (9): 51-58. DOI: 10.1109/MC.2011.291

Schneier, B. 2018. *Click Here to Kill Everybody: Security and Survival in A Hyper-Connected World.* WW Norton & Company.

Shahraki, A. et Ø. Haugen. 2018. « Social ethics in Internet of Things: An outline and review », *IEEE Industrial Cyber-Physical Systems*. DOI:10.1109/icphys.2018.8390757

Sicari, S., Rizzardi, A., Grieco, L.A. et A. Coen-Porisini. 2015. « Security, privacy and trust in Internet of Things: The road ahead », *Computer Networks* 76: 146-164. DOI: 10.1016/j.comnet.2014.11.008

Singer, P. 2011. *Practical Ethics* (2nd edition), Cambridge: Cambridge University Press

Sloot, B. v. d., Floridi, L. et Taylor, L. (dir.). 2017. *Group privacy.* New York, Springer International Publishing

Stemplowska, Z., et A. Swift. 2012. « Ideal and Nonideal Theory »: 373-90. Dans *The Oxford Handbook of Political Philosophy,* édité par David Estlund, Oxford: Oxford University Press

Taylor, L., Floridi, L. et B. van der Sloot. 2017. *Group Privacy. New Challenges of Data Technologies*. Springer

The Economist. 2017. « The World's Most Valuable Ressource Is no Longer Oil but Data », 6 mai

Thomson, J. J. 1975. « The Right to Privacy », *Philosophy and Public Affairs* 4 (4): 295-314

Timm, T. 2016. « The government just admitted it will use smart home devices for spying », *The Guardian,* 9 février

Tremblay, M. 2011. *Rapport 10 – Les infrastructures essentielles : un défi pour la sécurité des États, Analyse des impacts de la mondialisation sur la sécurité*. Québec : Laboratoire d'étude sur les politiques publiques et la mondialisation.

Waldron, J. 2004. « Property and Ownership », *The Stanford Encyclopedia of Philosophy,* édité par Edward N. Zalta

Walter, J. et B. Abendroth. 2017. « Losing a Private Sphere? A Glance on the User Perspective on Privacy in Connected Cars »: 237-47. Dans *Advanced Microsystems for Automotive Applications,* édité par C. Zachäus, B. Müller, et G. Meyer, Cham: Springer

Warren, S. D. et Brandeis, L. D. 1890. « The Right to Privacy », *Harvard Law Review* 4 (5): 193-220

Wattles, J. et D. O'Sullivan. 2019. « Facebook's Mark Zuckerberg calls for more regulation of the Internet », *CNN Business,* 30 mars

Weber, R. H. 2010. « Internet of Things – New security and privacy challenges », *Computer Law & Security Review* 26 (1): 23-30. DOI: 10.1016/j.clsr.2009.11.008

Westin, A. F. 1970. *Privacy and freedom*. New York: Atheneum

Whitmore, A., Agarwal, A. et L. D. Xu. 2015. « The Internet of Things—A survey of topics and trends », *Information Systems Frontiers* 17 (2): 261-274

Yadron, D., Ackerman, S. et S. Thielman. 2016. « Inside the FBI's encryption battle with Apple », *The Guardian,* 18 février

L'Internet des objets désigne l'ensemble des objets physiques (ex. appareils, capteurs, supports de stockage) mis en réseau et communiquant entre eux via Internet. Parmi les objets connectés, on compte des appareils portables (ex. téléphones intelligents, tablettes, ordinateurs), des vêtements et accessoires (ex. lunettes, montres, moniteurs médicaux), des appareils électroniques (ex. téléviseurs intelligents), des jouets pour enfants, des moniteurs pour bébé ou animaux de compagnie, des appareils ménagers (ex. réfrigérateurs), des systèmes pour le domicile (ex. thermostats, éclairage, sécurité, caméras, serrures), des voitures, etc. Ces objets ainsi que les données qu'ils collectent et les réseaux par lesquels ils transmettent et reçoivent de l'information sont possédés ou gérés par des acteurs variés (consommateurs, entreprises, pouvoirs publics), à des fins diverses. On estime qu'il y aura jusqu'à 30 milliards d'objets connectés en circulation à la fin de 2020.

L'arrivée des objets connectés sur le marché soulève plusieurs enjeux éthiques. Ces objets améliorent la qualité de vie des citoyens et la rentabilité des entreprises. Or, ils peuvent compromettre le droit à la vie privée des citoyens. Les objets connectés peuvent aussi affecter la sécurité physique, financière ou informationnelle des personnes.

Dans ce document, la CEST propose une réflexion éthique sur la place de la vie privée dans la conception et le développement des objets connectés, en supplément de son avis portant sur les nouvelles technologies de surveillance, publié en 2008. Le supplément propose treize recommandations. Elles s'adressent à différents acteurs, comme le gouvernement du Québec, les entreprises et les ordres professionnels.

Ce document et les autres publications de la Commission sont disponibles à l'adresse suivante :
www.ethique.gouv.qc.ca

La mission de la Commission de l'éthique en science et en technologie consiste, d'une part, à informer, à sensibiliser, à recevoir des opinions, à susciter la réflexion et à organiser les débats sur les enjeux éthiques du développement de la science et de la technologie. Elle consiste, d'autre part, à proposer des orientations susceptibles de guider les acteurs concernés dans leur prise de décision.

Commission de l'éthique en science et en technologie
Québec