L'Internet des objets, la vie privée et la surveillance

Balises éthiques et recommandations

COMMISSION DE L'ÉTHIQUE
EN SCIENCE ET EN TECHNOLOGIE

Québec

L’Internet des objets, la vie privée et la surveillance

Balises éthiques et recommandations

Commission de l'éthique
en science et en technologie
888, rue Saint-Jean, bureau 555
Québec (Québec) G1R 5H6
www.ethique.gouv.qc.ca

RÉDACTION DE L'AVIS

Secrétariat de réunion, recherche et rédaction
Marc-Kevin Daoust, conseiller en éthique

Direction
Sylvain Pelletier, secrétaire général

SOUTIEN TECHNIQUE

Révision linguistique
Liette Lemay, rév. a.

Graphisme, mise en page et accessibilité
Accessibilité Québec

Photo de page couverture
iStock

Avis adopté à la 97e séance
de la Commission de l'éthique en science
et en technologie le 17 avril 2020.

Dépôt légal : Octobre 2020
Bibliothèque et Archives nationales du Québec

ISBN : 978-2-550-87710-3 (version PDF)

Pour faciliter la lecture du texte, le genre masculin
est utilisé sans aucune intention discriminatoire.

COMITÉ DE TRAVAIL

PRÉSIDENT DE LA COMMISSION

M. Jocelyn Maclure
Professeur titulaire
Faculté de philosophie, Université Laval

PRÉSIDENT DU COMITÉ

M. Éric Simard
Président-directeur général
Idunn Technologies inc.
Membre de la CEST

RECHERCHE ET RÉDACTION

M. Marc-Kevin Daoust
Conseiller en éthique

MEMBRES EXTERNES

Mme Allison Marchildon
Professeure agrégée
Département de philosophie et d'éthique appliquée, Université de Sherbrooke

Mme Anne-Sophie Letellier
Candidate au doctorat
Faculté de communication, Université du Québec à Montréal
Directrice des communications
Crypto-Québec

M. Karim Benyekhlef
Professeur titulaire
Faculté de droit, Université de Montréal

Commission de l'éthique en science et en technologie
Québec

Québec, le 30 octobre 2020

Monsieur Pierre Fitzgibbon
Ministre de l'Économie et de l'Innovation
710, place D'Youville, 6e étage
Québec (Québec) G1R 4Y4

Monsieur le Ministre,

C'est avec plaisir que je vous transmets par la présente notre dernier supplément d'avis intitulé *L'Internet des objets, la vie privée et la surveillance*.

En espérant le tout à votre entière satisfaction, je vous prie d'accepter, Monsieur le Ministre, l'expression de ma haute considération.

Le président de la Commission,

Jocelyn Maclure

888, rue Saint-Jean, 5e étage, bureau 555
Québec (Québec) G1R 5H6
Téléphone : 418 691-5989
Télécopieur : 418 646-0920
www.ethique.gouv.qc.ca

TABLE DES MATIÈRES

SOMMAIRE DÉCISIONNEL

Le présent document constitue un supplément à un avis sur les nouvelles technologies de surveillance et de contrôle, publié en 2008 par la Commission de l'éthique en science et en technologie.

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. Des balises éthiques sont donc proposées pour encadrer le développement et l'usage de cette technologie. La Commission a formulé treize recommandations. Voici une synthèse des principales recommandations soutenues dans ce document.

La Commission recommande au gouvernement du Québec :

1. de se coordonner avec ses principaux partenaires commerciaux pour adopter des lois et des standards communs encadrant la collecte de données par l'Internet des objets (§3.1);
2. d'étudier la possibilité de créer une certification des objets connectés (§3.1);
3. d'instaurer des protections minimales par défaut des données collectées par les objets connectés (§3.2);
4. de favoriser l'approfondissement des connaissances touchant les méthodes de protection de la vie privée pour les objets connectés (§3.2);
5. 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 (§3.3);
6. de porter une attention particulière à ces politiques pour les personnes mineures, âgées, vulnérables, en perte d'autonomie, ou qui n'atteindront pas la pleine autonomie (§3.3);
7. 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 (§3.5);
8. d'imposer des normes de transparence aux entreprises collectant des données à partir des objets connectés (§3.6).

La Commission recommande aux entreprises développant des objets connectés :

1. d'enchâsser les principes de protection de la vie privée dans la conception des objets connectés *(privacy by design)* (§3.5);
2. d'être en mesure de justifier publiquement des pratiques socialement risquées, comme la collecte, le stockage ou la vente de données personnelles (§3.6).

1 INTRODUCTION

1.1 Résumé des recommandations de 2008 de la Commission touchant les nouvelles technologies de surveillance et de contrôle

L'avis intitulé *Viser un juste équilibre : Un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité,* publié par la Commission en 2008, étudie trois technologies de surveillance à l'aune de la sécurité publique (p. ex., le maintien de l'ordre, la protection contre le crime et les menaces internes, etc.) et nationale (p. ex., la lutte contre le terrorisme, la protection des infrastructures essentielles, etc.). Il s'agit :

- des **systèmes biométriques**, qui permettent d'identifier une personne ou de vérifier l'admissibilité d'une personne « à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'œil, contour de la main…), de traces (ADN, sang, odeurs) ou d'éléments comportementaux (signature, démarche)[1] »;
- de la **vidéosurveillance**, qui consiste en la surveillance à distance de lieux publics ou privés, à l'aide de caméras, qui transmettent les images saisies à un équipement de contrôle qui les reproduit sur un écran[2];
- de l'**identification par radiofréquence (IRF)**, qui consiste à transmettre des informations par ondes radio à partir de puces électroniques, et qui se manifeste souvent par l'insertion de puces contenant des renseignements personnels ou d'autres informations (la nationalité, le sexe, la date de naissance, etc.) dans les documents d'identité et les cartes d'accès[3].

L'avis de 2008 se voulait une réponse à un constat social préoccupant. L'exigence sécuritaire défendue par les États occidentaux post-11 Septembre est souvent à l'origine de restrictions illégitimes du droit individuel à la vie privée. Cependant, ce constat en apparence simple comprend son lot de complications. Par exemple, la Commission reconnaît la difficulté de définir tant ce qu'est la sécurité (et, de façon complémentaire, le sentiment d'insécurité) que la vie privée[4]. De plus, l'avis ne s'inquiète pas seulement des actions d'un seul grand acteur de surveillance (comme l'État), mais de plusieurs petits acteurs privés ou publics. C'est pourquoi il faut aussi prendre en compte les acteurs non étatiques, comme les compagnies privées et les familles[5].

L'avis de 2008 présente les cadres juridiques québécois, canadien et international entourant la protection de la vie privée. Au Québec, la Loi sur la protection des renseignements personnels dans le secteur privé définit un renseignement personnel comme étant « tout renseignement qui concerne une personne physique et permet de l'identifier[6] ». Au Canada, la Loi sur la protection des renseignements personnels offre une définition complémentaire des renseignements personnels. Ils y sont définis comme les « renseignements […] concernant un individu identifiable[7] ». La loi donne ensuite des exemples de tels renseignements, allant de l'âge à l'origine ethnique, en passant par les opinions ou idées véhiculées par la personne.

---

1 Commission de l'éthique en science et en technologie 2008, p. xx.
2 *Ibid.*, p. xxi.
3 *Ibid.*
4 *Ibid.*, p. xix.
5 *Ibid.*, p. xx.
6 L.R.Q., chap. P-39.1, 1993, c. 17, a. 2.
7 L.R.C., 1985, chap. P-21, a. 3.

Au Québec, l'article 5 de la Charte des droits et libertés de la personne et les articles 35 à 41 du Code civil garantissent à toute personne le droit au respect de sa vie privée. La législation québécoise précise des obligations qui doivent s'appliquer à la collecte, à l'utilisation, à la conservation et à la communication de renseignements personnels. Ces obligations sont notamment précisées dans la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., chapitre A-2.1), la Loi sur la sécurité privée (L.R.Q., chapitre S-3.5), ainsi que la Loi sur la protection des renseignements personnels dans le secteur privé (L.R.Q., chapitre P-39.1) et la Loi concernant le cadre juridique des technologies de l'information (L.R.Q., chapitre C-1.1). Au niveau fédéral, l'article 8 de la Charte canadienne des droits et libertés et la partie 6 du Code criminel inscrivent le respect de la vie privée comme un droit fondamental. La législation fédérale comporte également un ensemble de textes juridiques qui encadrent de façon générale la collecte, l'utilisation, la conservation et la communication de renseignements personnels, dont la Loi sur la protection des renseignements personnels (L.R.C., 1985, chapitre P-21) et la Loi sur la protection des renseignements personnels et les documents électroniques (L.C., 2000, chapitre 5). L'avis de 2008 précise aussi comment la protection de la vie privée et des renseignements personnels se traduit à l'échelle internationale. Comme les lois québécoises et canadiennes protégeant la vie privée ont peu changé entre 2008 et 2020, nous référons le lecteur à l'avis de 2008 pour plus de détails sur celles-ci (voir, en particulier, les pages 18 à 21)[8].

L'avis fait état de plusieurs valeurs devant guider les recommandations de la Commission. On y souligne des valeurs comme l'autonomie, la sécurité, la liberté, la vie privée, la transparence, la justice et l'égalité[9].

Les principales conclusions de l'avis peuvent être regroupées en six catégories, soit :

- **Pertinence, efficacité et fiabilité.** Les moyens de surveillance et de contrôle les moins intrusifs doivent être privilégiés. Il faut que les résultats obtenus par ces technologies correspondent aux « visées d'origine ». Il faut aussi que les nouvelles technologies de surveillance et de contrôle ne soulèvent pas plus de problèmes qu'elles n'en règlent[10].
- **Proportionnalité.** 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, est inacceptable[11].
- **Acceptabilité sociale.** La population doit être favorable aux méthodes de surveillance préconisées par l'État. Il ne semble pas y avoir de volonté populaire d'interdire toutes les nouvelles technologies de surveillance et de contrôle. Dans certains cas, on observe même un intérêt pour ces technologies. On peut toutefois se demander si l'opinion publique est bien informée de ce développement technologique. Il vaudrait mieux recueillir des opinions éclairées à ce sujet, mais aussi éduquer les citoyens quant aux implications de ces technologies sur leurs droits[12].
- **Consentement.** La Commission estime que, si le déploiement des nouvelles technologies de surveillance et de contrôle se fait de manière transparente et en accord avec les valeurs fondamentales des sociétés démocratiques, chaque individu n'a pas nécessairement à consentir au déploiement de ces technologies. Cependant, l'absence de consentement individuel libre, éclairé et continu soulève des enjeux éthiques. C'est pourquoi la Commission insiste aussi sur la nécessité de mettre en place des moyens permettant aux citoyens de faire valoir leurs doléances face aux usages des technologies de surveillance. Elle estime de plus que les citoyens devraient être mieux informés sur une foule de points, allant des dispositions juridiques entourant le déploiement des technologies de surveillance jusqu'aux lieux et aux documents mis sous surveillance[13].
- **Respect des finalités.** Si des technologies de surveillance ne sont justifiées que pour l'atteinte de certains buts précis, on ne doit pas les utiliser à d'autres fins. Par exemple, il est inquiétant que des normes, des procédés, des pratiques, des moyens de surveillance et de contrôle mis en place dans la foulée d'attentats terroristes soient progressivement intégrés à la lutte à la petite délinquance, puis récupérés par le secteur commercial. Compte tenu de la facilité avec laquelle les nouvelles technologies de surveillance et de contrôle trouvent des applications et donc les finalités qui peuvent être très différentes, il convient de rester vigilant à cet égard[14].
- **Protection des renseignements personnels.** L'acquisition de renseignements personnels peut compromettre le droit à la vie privée des personnes. Mais la collecte de ces renseignements peut aussi, dans certaines circonstances, contribuer à la sécurité des sociétés. Comment concilier (ou équilibrer) ces deux objectifs? Sur cet enjeu, l'avis demeure exploratoire (aucune réponse précise n'est proposée). Il met plutôt en lumière une foule de questions complexes touchant l'équilibre entre vie privée et sécurité. L'avis propose toutefois une démarche pour résoudre cette question : les gouvernements provincial et fédéral devraient mener des consultations publiques pour déterminer, collectivement, le juste équilibre entre protection des renseignements personnels et sécurité publique et nationale[15].

Le but du présent document est de poursuivre la réflexion sur le rapport entre sécurité et droit à la vie privée dans le contexte du développement rapide de l'Internet des objets.

1.2 Qu'est-ce que l'Internet des objets?

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[16]. 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 (Hittinger et Jaramillo 2019).

8 Le cadre juridique québécois entourant la protection de la vie privée pourrait changer prochainement, avec l'arrivée du projet de loi 64 visant à moderniser les dispositions législatives en matière de protection des renseignements personnels. Cette loi introduit de nouvelles notions, comme le renseignement personnel sensible ou le renseignement anonymisé.
9 *Ibid.*
10 *Ibid.*, p. xxi.
11 *Ibid.*
12 *Ibid.*, p. xxii.
13 *Ibid.*, p. xxiii.
14 *Ibid.*
15 *Ibid.*, pp. xxiv-xxvi.
16 La transmission des données passe par des réseaux filaires, cellulaires, satellite, Wi-Fi, Bluetooth, etc.

1.3 Pourquoi l'arrivée de l'Internet des objets nécessite-t-elle d'actualiser les travaux menés en 2008

Dans la littérature sur les risques éthiques entourant l'Internet des objets, on remarque des similarités importantes avec les enjeux étudiés dans l'avis de 2008 sur les nouvelles technologies de surveillance et de contrôle. Pensons notamment à l'équilibre entre, d'une part, le confort et le bien-être recherchés par les consommateurs à l'achat d'objets connectés et, d'autre part, le respect de leur vie privée et de leur autonomie, notamment en raison d'un contexte où les conditions d'un consentement libre, éclairé et continu sont difficilement réunies. Des enjeux sont aussi soulevés en ce qui concerne l'équilibre entre la sécurité civile et nationale et le respect de la vie privée et, plus généralement, des droits et libertés fondamentaux des individus.

Bien que les enjeux entourant l'Internet des objets soient semblables à ceux entourant les nouvelles technologies de surveillance et de contrôle, les analyses menées en 2008 ne s'appliquent pas intégralement à ce développement technologique. Trois différences importantes ont motivé la rédaction d'un supplément d'avis consacré spécifiquement à l'Internet des objets. Premièrement, l'Internet des objets exacerbe certaines menaces aux droits fondamentaux des citoyens. Les experts s'entendent pour dire que la législation actuelle serait insuffisante pour protéger les citoyens canadiens des risques liés à l'Internet des objets[17]. De plus, de nombreux experts et observateurs s'inquiètent que l'Internet des objets devienne l'outil de surveillance de masse par excellence[18]. Grâce aux nouvelles technologies, nous entrerions dans « l'âge d'or de la surveillance[19] ». Ces craintes semblent fondées. En 2016, le directeur du renseignement national américain, James Clapper, reconnaissait lui-même le potentiel de l'Internet des objets pour les agences de surveillance :

> Dans l'avenir, les services de renseignement pourraient avoir recours à l'Internet des objets pour l'identification, la surveillance, la localisation des personnes et le ciblage à des fins de recrutement, ou pour accéder à des réseaux ou à l'identité des utilisateurs[20].

Deuxièmement, l'avis de 2008 étudiant les nouvelles technologies de surveillance et de contrôle s'est concentré sur les données biométriques, la vidéosurveillance et l'identification par radiofréquence. Ces modes de surveillance sont surtout efficaces dans l'espace public (dans les rues, les parcs, les commerces, et ainsi de suite). Pour souligner ce point, l'avis insiste par moments sur l'intimité dont bénéficient (et devraient bénéficier) les citoyens dans leur domicile[21]. Par exemple, il est rare que les appareils de vidéosurveillance déployés par les États occidentaux captent des images dans les domiciles des personnes. L'arrivée de l'Internet des objets accentue les possibles intrusions dans la vie privée des individus, puisque les objets connectés collectent des données à propos des citoyens, quel que soit leur emplacement (incluant, notamment, leur domicile).

17 Voir notamment Trosow, Taylor et Hanam (2016). D'autres sources sont citées plus loin.
18 McArdle 2016; Porup 2016; Berkman Centre 2016; Doctorow 2015; Powles 2015; Timm 2016.
19 McArdle 2016.
20 Ackerman et Theilman 2016, traduction libre.
21 Voir notamment les pages xxv, 15 et 52 de l'avis de 2008. Le document précise aussi que les moyens de surveillance préconisés par les États ne doivent pas être utilisés pour capter des données dans des lieux privés, comme les domiciles (p. 33).

Troisièmement, l'implication des acteurs privés est centrale au développement de l'Internet des objets. Avec l'Internet des objets, ce sont avant tout des entreprises privées qui collectent des données à propos des citoyens (et qui peuvent les transmettre à des tierces parties, comme des États). Ce n'était pas le cas avec les trois technologies étudiées dans l'avis de 2008. À titre d'exemples, les puces d'identification par radiofréquence insérées dans les cartes d'identité, les données biométriques collectées aux frontières et les données captées par vidéosurveillance dans les lieux publics sont généralement gérées par l'État. À tout le moins, les États ne sont pas tenus d'avoir recours aux services de firmes privées pour collecter des données à partir de ces technologies. Le constat est très différent en ce qui a trait à l'Internet des objets. Les données collectées dans des téléphones portables, des réfrigérateurs connectés ou des voitures connectées sont d'abord accessibles à des entreprises privées, et non aux États. C'est donc en collaborant avec le secteur privé que des États peuvent tirer des informations captées et enregistrées par ces appareils.

Ces différences affectent l'analyse des risques éthiques entourant l'Internet des objets. C'est pourquoi la Commission a choisi de produire un supplément d'avis portant précisément sur l'Internet des objets.

1.4 Plan du supplément

Le chapitre 2 offre une description plus approfondie de l'Internet des objets et des enjeux s'y rattachant. Différents cas de figure sont décrits de façon à ce que ces enjeux soient bien compris. Le chapitre 3 propose une mise à jour de certaines conclusions tirées dans cet avis. Il développe aussi un cadre normatif pour guider les fabricants d'objets connectés et les acteurs qui collectent des données à partir de ces objets. Le dernier chapitre clarifie les limites de l'analyse proposée et propose des pistes de réflexion futures.

2. L'INTERNET DES OBJETS : CAS DE FIGURE ET PROBLÈMES À RÉSOUDRE

2.1 Qu'est-ce que l'Internet des objets?

2.1.1 Vie privée et agrégation de données personnelles

Cette section vise à clarifier les enjeux éthiques *spécifiques* entourant l'Internet des objets. En d'autres termes, quels sont les problèmes éthiques soulevés spécifiquement par ces développements technologiques?

Du point de vue éthique, ce qui distingue essentiellement l'Internet des objets est que cette technologie facilite énormément la collecte d'informations à propos de personnes (ou de groupes sociaux). Ces informations peuvent fournir une description directe de l'utilisateur (comme dans des images ou des enregistrements sonores). On parle alors de « données ». Ces informations peuvent aussi décrire d'autres données captées (comme des informations à propos de l'heure à laquelle une image a été captée, ou des informations touchant la géolocalisation d'une image). On parle alors de « métadonnées ». Enfin, certaines données sont inférées. Elles sont obtenues par des recoupements et des déductions effectués à partir des données et des métadonnées. Afin de simplifier l'analyse, nous référerons à la notion de « données » d'une manière large, en incluant les métadonnées et les données inférées sous ce concept.

Les données (et les métadonnées) collectées par les objets connectés sont accumulées, transmises et potentiellement agrégées. Des zones autrefois privées peuvent désormais être connues et analysées par une foule d'acteurs. Par exemple, en l'absence d'encadrement éthique ou juridique, les activités au sein des foyers peuvent, par l'accumulation de données, être accessibles à des compagnies ou à des États[22]. La concentration des données obtenues par l'Internet des objets compromet le droit à la vie privée des utilisateurs, facilite grandement la surveillance de masse et peut avoir des conséquences néfastes sur les consommateurs et les citoyens.

Le fait que des objets collectent des données n'est pas nouveau. Pensons, à titre d'illustration, aux voitures personnelles. Dès la fin des années 1980, les ordinateurs de bord et les systèmes de diagnostic embarqués des véhicules traditionnels ont été utilisés pour collecter des données sur l'autonomie du véhicule, la durée des trajets ou les problèmes du groupe motopropulseur. Or, contrairement aux véhicules connectés, ces données sont contenues dans la base de données du véhicule, ce qui complique grandement la tâche des compagnies qui souhaitent se les approprier[23]. Si le véhicule est connecté à Internet, ces données peuvent être *transmises* directement aux fabricants.

De plus, le croisement entre différents types de données pose aussi problème. Reprenons, à titre d'exemple, le cas des véhicules personnels. On pourrait imaginer qu'un véhicule collecte seulement des données sur le nombre de passagers à bord lors de différents trajets, ce qui soulève peu de questions éthiques. Or, un problème se pose lorsque différentes données sont *compilées* et *agrégées,* comme on peut le voir dans le tableau suivant :

22 Walter et Abendroth 2017.
23 Par exemple, les données peuvent être collectées manuellement au moment de l'entretien du véhicule chez le concessionnaire.

Tableau 1
Comparaison entre deux jeux de données d'un utilisateur de véhicule connecté[24]

Jour(s)	Régularités observées, un type de données	Régularités observées, plusieurs types de données compilées
Lundi au jeudi	• 1 occupant (le propriétaire).	• 1 occupant (le propriétaire); • Aller-retour entre le domicile et le stationnement d'une banque; • Utilise généralement le véhicule à 9 h (aller), et à 17 h (retour).
Vendredi	• 1 à 2 occupants (le propriétaire et une autre personne).	• 1 à 2 occupants (le propriétaire à l'aller, et une autre personne s'ajoute au retour); • Aller-retour entre le domicile et le stationnement d'un bar; • La deuxième occupante est toujours une femme, mais jamais la même (déduction par recoupement avec les données vocales); • Utilise généralement le véhicule à 22 h (aller) et à 2 h (retour);

Ce qui est frappant dans le Tableau 1 est que l'on puisse deviner des aspects profondément intimes de la vie du propriétaire en croisant quatre types de données simples (le nombre d'occupants, le trajet, le sexe des occupants et les heures d'utilisation du véhicule). La collecte d'un seul type de données, comme le nombre d'occupants du véhicule, donne un portrait très limité du propriétaire et semble inoffensive. Prises séparément, on pourrait dire la même chose des autres données recueillies (trajet, sexe des occupants et heures d'utilisation). Or, en compilant différentes données, on peut deviner le type d'emploi, l'orientation sexuelle, les valeurs, le mode de vie du propriétaire du véhicule, et ainsi de suite. Un utilisateur de véhicule connecté n'a pas forcément envie de partager ces informations avec le fabricant du véhicule, ni de les savoir enregistrées dans une base de données à la sécurité inconnue[25].

Il importe tout de même de noter que la vie privée des individus n'est pas inéluctablement compromise par l'arrivée des objets connectés. En théorie, ce développement technologique pourrait même offrir plus d'intimité à certains individus. En effet, les objets connectés pourraient permettre l'abandon (ou la réforme) d'opérations effectuées par des êtres humains jugées gênantes ou intrusives. Prenons l'exemple des soins médicaux. L'Internet des objets permet de faire un suivi moins intrusif de l'état de santé des patients. Comme le notent Shahraki et Haugen :

> L'Internet des objets peut aider les sociétés à fournir des services moins chers et plus facilement. Il y a quelques années, les aînés qui vivaient chez eux devaient recevoir la visite d'infirmiers ou d'infirmières pour effectuer des tests réguliers. Aujourd'hui, l'Internet des objets permet d'avoir des maisons intelligentes, permettant des vérifications sans intervention humaine et moins coûteuses. L'Internet des objets peut être moins intrusif que les interventions humaines. Pensons aux personnes âgées souffrant d'incontinence. Les capteurs connectés peuvent être placés dans leurs couches, de sorte qu'il n'est pas nécessaire d'effectuer constamment des vérifications. Cela permet non seulement de gagner du temps mais aussi de préserver la dignité des patients. (Shahraki et Haugen 2018, 511, traduction libre)

24 Ce scénario est inspiré d'Allhoff et Henschke 2018, pp. 58-9.

25 Évidemment, il manque plusieurs éléments contextuels dans cette mise en situation. Par exemple, l'intention et l'utilisation derrière la collecte de ces données sont inconnues. Le but de cette mise en situation est simplement d'illustrer comment le croisement entre différents types de données peut être intrusif.

2.1.2. Mais qu'est-ce que la vie privée, exactement?

L'Internet des objets pourrait compromettre le droit à la vie privée des personnes. Mais que signifie le droit à la vie privée, exactement? L'avis de 2008 sur les nouvelles technologies de surveillance et de contrôle évite de répondre à cette question particulièrement complexe. Dans le cadre de ce supplément, nous souhaitons clarifier le sens de cette notion et la nécessité (ou non) d'établir et de défendre un cadre théorique particulier entourant la notion de vie privée.

Outre le champ de la philosophie, qui a tenté de cerner la nature et les implications de la vie privée, plusieurs domaines se sont penchés sur la question, notamment la psychologie, la sociologie, la science politique et le droit. Ces champs théoriques se concentrent sur l'examen de facteurs contextuels, socioculturels et technologiques pouvant grandement influencer notre compréhension du concept. Plusieurs auteurs ont parlé de la vie privée en termes de *valeur,* mais également en termes d'*intérêt,* d'*exigence,* d'*utilité,* tout comme de *menace* vis-à-vis celle-ci. Les qualificatifs qui viennent décrire la nature de la vie privée sont souvent ceux de *solitude,* d'*anonymat,* de secret, d'*intimité,* ou encore de *réserve*. L'idée d'une violation de notre vie privée peut renvoyer, quant à elle, à des concepts comme l'*embarras,* la *honte* et même la *culpabilité*.

Il existe au moins cinq grandes interprétations de ce qu'est la vie privée et des raisons motivant sa protection. Voici un résumé de chacune de ces interprétations :

1. Selon une **approche libérale**, la vie privée rend possible ce que nous avons appelé les « valeurs libérales », telles que la liberté, l'égalité, l'autonomie et l'individualisme, ou en fait partie. Certains auteurs incluent également la dignité dans ces valeurs libérales, mais souvent comme découlant elle-même de la possibilité d'être libre et autonome (Mindle, 1989). La vie privée, dans le cas présent, nous permet d'avoir un espace sans interférence provenant de la société ou de l'État, où l'on peut être libre de choisir diverses occupations et rôles sociaux, liés par exemple à la famille ou à notre emploi (Westin, 1967). De façon similaire, la vie privée peut faire partie intégrante de la dignité humaine (Bloustein, 1964). Sans possibilité d'entretenir une intériorité, il serait difficile, voire impossible de se constituer comme sujet authentique, en étant constamment transparents à autrui dans nos pensées et nos sentiments (Cohen, 2000). Si nous étions constamment placés sous le regard et la surveillance des autres, nous perdrions le sentiment de nous appartenir et pourrions même devenir des moyens pour des acteurs plus puissants d'atteindre leurs fins (Reiman, 1995).
2. Selon l'approche des **relations personnelles**, sans vie privée, il serait impossible d'entretenir des relations personnelles et intimes variées et significatives, qui sont fondamentales pour assurer l'épanouissement personnel (Fried, 1968; Rachels, 1975; Reiman, 1976). Dans la même veine, la vie privée agit comme protection mutuelle entre les individus à travers leurs relations sociales (Nagel, 1998). Notre conscience de nous-même et des autres peut être à la fois considérée comme une ressource indispensable pour notre réalité privée, mais aussi comme un fardeau, par le regard et le jugement d'autrui. Cette perception des autres a souvent un effet inhibiteur et même souhaitable chez chacun, puisqu'il serait improbable de pouvoir maintenir des relations avec d'autres s'ils savaient à tout moment, dans les moindres détails et en toute honnêteté ce que l'on pensait ou ce que l'on ressentait à propos d'eux et sur divers objets. La vie privée nous permet un certain contrôle sur notre façon de nous montrer à autrui, en choisissant de leur communiquer certaines informations ou non.
3. Selon l'approche du **droit à la propriété privée**, la vie privée découle du droit de propriété des personnes. Dans *The Right to Privacy,* Judith Jarvis Thomson défend cette conception de la vie privée. Elle donne l'exemple d'un homme qui ne voudrait pas que d'autres personnes puissent avoir accès à une photo intime qu'il conserve chez lui. Si quelqu'un tentait effectivement de regarder l'image ou de se l'approprier, c'est son droit à la propriété privée (par l'accès à son domicile et la possession de sa photo) qui serait bafoué.

4. Selon l'approche de la **non-nuisance**, la vie privée détient une valeur instrumentale, puisqu'elle constitue un outil pour contrer divers torts. Dans *Privacy, Freedom, and Respect for Persons* (1971), Stanley I. Benn explique que l'information que l'on possède sur des individus pourrait nous donner un certain contrôle sur leurs actions, par exemple en les faisant chanter. Des individus mal intentionnés ou des gouvernements trop contrôlants peuvent assurément utiliser des informations de nature « privée », que l'on ne voudrait pas révéler à tous, pour nous dominer. Selon Reinman, la vie privée nous met moins à risque de subir des pertes de liberté parce qu'ainsi nous sommes moins vulnérables face à ces entités qui voudraient avoir le contrôle de nos vies (Reinman, 1995). Ce n'est donc pas la valeur du respect pour la vie privée des individus qui est valorisée en elle-même, mais l'instrument qu'elle représente pour contrer les torts possibles.
5. Enfin, pour de nombreuses **approches féministes** comme celle de Susan Moller Okin, la distinction entre les sphères privées et publiques doit être remise en cause. Selon Okin, les questions publiques et politiques ne peuvent pas être séparées complètement des questions privées et personnelles. Autrement, on laisserait des zones « privées », comme le domicile, libres de relations de domination, sans possibilité pour l'État d'intervenir au nom du respect de la vie privée familiale (Okin, 1989). La vie privée ne doit donc pas être utilisée comme prétexte pour couvrir les possibilités de domination, de dégradation ou se sévices, particulièrement envers les femmes et les enfants dans le cadre de relations de couple et familiales (DeCew, 2002). Toutefois, les femmes peuvent avoir un intérêt très fort pour la vie privée en matière de choix reproductifs. Ces critiques féministes ont tout de même démontré les limites de la sphère privée, en mettant de l'avant le respect du droit de la personne.

Ces brèves remarques sur l'existence de théories distinctes entourant la vie privée et sa justification montrent qu'il s'agit d'une question complexe et difficile à résoudre[26]. Plutôt que de retenir et de défendre une de ces approches, la Commission fait le pari que l'on peut mettre ces débats entre parenthèses et fonctionner selon une approche du *consensus par recoupement*.

La notion de consensus par recoupement a été formulée par John Rawls dans ses ouvrages intitulés *Théorie de la justice* (1997) et *Libéralisme politique* (1995). On observe un consensus par recoupement lorsque des normes sociales sont admises par n'importe quelle personne raisonnable, bien que chaque personne puisse justifier ces normes d'une manière différente. En d'autres termes, il s'agit de consensus pouvant être justifiés de plusieurs manières différentes, voire incompatibles. Par exemple, le principe de non-nuisance a été au cœur de différentes religions et théories éthiques, bien qu'il existe une foule de justifications incompatibles entre elles en faveur de ce principe.

De façon similaire, certaines informations vont sans conteste appartenir au domaine de la vie privée, et certaines actions vont de toute évidence enfreindre le droit à la vie privée, et ce, peu importe la théorie de la vie privée que l'on privilégie. Prenons un exemple simple. Une entreprise privée enregistre vos conversations personnelles sans votre consentement. Les enregistrements sont analysés par des êtres humains. Ces conversations permettent de vous identifier et d'en apprendre sur vos secrets, vos désirs intimes et vos préférences. N'importe quelle théorie de la vie privée mentionnée ci-dessus y verra un problème éthique. L'approche des relations personnelles y verra un obstacle aux relations personnelles variées et intimes, l'approche libérale reprochera à l'entreprise d'enfreindre les libertés fondamentales de ses clients, et ainsi de suite. Même les approches féministes, qui nous invitent au scepticisme quant à la distinction entre sphère privée et sphère publique, pourraient admettre qu'une telle action pose un sérieux problème éthique.

26 Ce résumé n'est pas exhaustif. Il existe d'autres perspectives importantes sur la vie privée, telles que la théorie de la vie privée comme intégrité contextuelle (Nissenbaum 2009).

Ainsi, nous n'avons pas besoin de trancher les débats substantiels entourant la notion de vie privée et sa justification. Certaines situations claires illustrent des infractions au droit à la vie privée, quelle que soit la justification en faveur du droit à la vie privée. Dans le cadre de cet avis, on peut s'en tenir à ces situations claires et laisser aux théoriciens le soin d'analyser les cas limites (c.-à-d. les cas où il pourrait y avoir des divergences d'avis raisonnables entourant le droit à la vie privée). Cela ne signifie pas que l'étude de ces cas est impertinente. Mais la difficulté entourant leur résolution n'est pas un obstacle à la démarche en cours.

2.2 Différents cas de figure et leurs enjeux propres

Les enjeux entourant l'Internet des objets varient selon le type et la quantité de données collectées par les objets. Dans cette section, trois cas de figure sont discutés ainsi que les enjeux s'y rattachant. Ces cas de figure seront repris tout au long du document pour illustrer les arguments et les conclusions de la Commission.

Il y a d'abord les **objets collectant des données sensibles de différents types**. Les données sensibles peuvent être sommairement définies comme des informations personnelles devant être traitées avec une vigilance particulière, telles que la date de naissance, l'orientation sexuelle, l'état de santé, l'origine ethnique, l'adresse, le revenu, et ainsi de suite. Plusieurs objets connectés collectent de nombreuses informations sensibles, par exemple :

> **Voiture connectée.** Votre nouvelle voiture est connectée à Internet par satellite. Elle transmet des données au fabricant. Celles-ci peuvent inclure votre géolocalisation, l'historique de votre GPS, votre profil de conduite, vos réactions dans des situations potentiellement dangereuses, vos conversations personnelles avec les autres passagers, vos préférences musicales, les données captées par les caméras de recul, le nombre de passagers à bord, et ainsi de suite.

Naturellement, étant donné qu'une grande quantité de données sensibles sont collectées, les objets de ce type sont ceux qui comportent les risques éthiques les plus importants et les plus clairs. Par exemple, ces données sensibles pourraient être utilisées d'une manière inacceptable par le fabricant. Sans cadre éthique et juridique adéquat, ce dernier pourrait les transmettre à un tiers, ou les compiler pour dresser un portrait invasif de l'utilisateur.

La question se complique dans d'autres cas de figure. Prenons le cas d'**objets connectés collectant des données sensibles d'un seul type**, par exemple :

> **Stimulateur cardiaque.** À la suite d'une maladie coronarienne, on vous implante une pile cardiaque pour réguler la pulsation de votre cœur. Votre stimulateur est connecté à Internet et transmet des informations à votre dossier médical. Ainsi, votre équipe soignante peut analyser vos données et déterminer si votre état de santé progresse ou non.

Une équipe de soignants ayant accès aux données d'un stimulateur cardiaque obtient une moins grande quantité de données sensibles qu'un fabricant de voitures connectées. Malgré un accès plus limité aux données sensibles de l'utilisateur, des risques éthiques importants demeurent associés à ce type d'objet. Par exemple, l'équipe de soignants pourrait *recouper* ces données avec d'autres données collectées par d'autres objets connectés et faire des déductions plus fines à propos de la vie privée du patient. Les données du stimulateur cardiaque pourraient être recoupées avec d'autres données, tirées par exemple d'un vêtement connecté, d'un bracelet d'alerte pour les chutes, du dossier médical du patient, et ainsi de suite. Donc, bien que l'appareil collecte moins de données, la question de l'utilisation de ces données pose tout de même problème.

En fait, n'importe quel objet connecté peut potentiellement contribuer à miner la vie privée de son utilisateur. Prenons un **objet connecté collectant un seul type de données non sensibles**, par exemple :

> **Cafetière connectée.** Votre nouvelle cafetière est connectée à Internet. Elle est coordonnée avec l'alarme de votre montre connectée et s'active quelques minutes après votre réveil. Ainsi, votre café est toujours prêt au bon moment.

Les données collectées par une cafetière connectée semblent inoffensives. Dans la grande majorité des cas, la consommation quotidienne de café d'une personne n'est pas une donnée sensible nécessitant des protections importantes. Mais un problème se pose tout de même lorsque des recoupements sont faits entre les données « inoffensives » compilées par différents appareils. Comme le mentionnent Allhoff et Henschke :

> Par exemple, supposons qu'une machine à café connectée est activée deux fois le vendredi matin, alors qu'elle ne démarre qu'une seule fois les autres jours de la semaine. Supposons que la douche intelligente de l'utilisateur soit également plus active qu'à l'habitude le vendredi matin. Notre utilisateur a-t-il rencontré quelqu'un dans un bar la veille au soir? Que se passe-t-il si cela se produit tous les vendredis — est-ce que cela en dévoile davantage sur la vie personnelle ou les pratiques de l'utilisateur? Des informations apparemment inoffensives, comme le moment où une machine à café est activée, peuvent s'avérer hautement révélatrices lorsqu'elles sont intégrées et agrégées à d'autres informations. (Allhoff et Henschke 2018, p. 59, traduction libre)

Dans le cas décrit ci-dessus, le partage des responsabilités éthiques se complique grandement. Une compagnie collectant seulement des données sur le nombre et le type de cafés d'un utilisateur peut se déresponsabiliser sur la base du fait que, prises séparément, les données qu'elle collecte sont peu invasives. Il en va de même pour une entreprise collectant des données sur le temps passé sous la douche, une autre collectant des données sur les heures auxquelles les lumières ont été activées, etc. Mais lorsqu'elles sont mises en commun, ces données sont potentiellement invasives et entrent en conflit avec le droit à la vie privée. Des actions individuelles en apparence acceptables peuvent avoir des effets graves lorsque mises ensemble.

Dans ce contexte, il est aussi difficile d'attribuer des torts et des responsabilités clairs quant à l'invasion de la vie privée. Chaque collecte de données explique pourquoi les utilisateurs peuvent subir des torts, bien que chaque collecte prise séparément ne soit pas particulièrement invasive. Conformément à ce qui précède, chaque entreprise responsable de la collecte de certaines données y est pour quelque chose, bien que chaque entreprise prise séparément ne soit pas particulièrement blâmable.

En somme, les objets connectés qui collectent une ou de nombreuses données sensibles posent un risque éthique clair. Mais les autres objets connectés posent aussi des risques éthiques d'une nature différente, puisque des données en apparence inoffensives peuvent être recoupées entre elles. Une fois recoupées, ces différentes données deviennent souvent sensibles, et y accéder compromet la vie privée des utilisateurs.

2.3 L'application des recommandations de 2008 à l'Internet des objets

Dans cette section, nous passons en revue la démarche d'évaluation éthique et les différentes recommandations tirées de l'avis de 2008. Cela nous permettra de voir quels aspects de l'avis original doivent être revus.

2.3.1 Les valeurs et principes en jeu

Dans ses travaux, la Commission met d'abord l'accent sur le soutien à la prise de décision. Pour y arriver, elle adopte une démarche d'évaluation éthique fondée sur les valeurs et les principes éthiques. Définis de manière générale, les valeurs et principes éthiques se rapportent à des conceptions de ce qui devrait être. Ils servent à évaluer, à déterminer l'acceptabilité ou le caractère désirable des actions, des situations ou des événements. Ainsi, ils orientent et justifient certaines actions. Lorsqu'une personne doit prendre des décisions quant aux actions à entreprendre par rapport à une situation, plusieurs valeurs et principes peuvent guider son choix dans différentes directions. Il s'agit alors de déterminer lesquels devront être priorisés et quels moyens seront les plus à même de les matérialiser[27].

Nous visons d'abord à *établir clairement les valeurs et principes en jeu* dans le développement de l'Internet des objets. Le repérage de ces valeurs et principes se fait grâce à une revue de la littérature. Ces clarifications nous permettent ensuite de *réfléchir* aux valeurs et principes devant être priorisés ainsi qu'aux meilleurs moyens de matérialiser cette hiérarchisation, puis de formuler des recommandations d'actions particulières.

Déjà, dans la section précédente, plusieurs valeurs et principes centraux ont émergé des controverses entourant le développement de l'Internet des objets. Dans cette section, nous les relevons de façon plus claire et précise.

Le respect de l'autonomie

Le respect de l'autonomie des personnes est un principe central en éthique. Selon ce principe, il faut, lorsque les circonstances s'y prêtent, permettre aux individus de prendre des décisions éclairées et libres sur des questions qui les concernent. Le fait d'obtenir le consentement d'autrui, ou de ne pas interférer avec les décisions d'autrui, sont des moyens de respecter l'autonomie des personnes. En éthique, ce principe est couramment associé au déontologisme[28].

Un corollaire du respect de l'autonomie est le principe de propriété. Selon ce principe, les individus sont en droit de profiter (par exemple, utiliser, partager, prêter, vendre, détruire, etc.) de leurs propres biens comme bon leur semble, dans le respect de la loi et des droits d'autrui[29]. Dans le cas de l'Internet des objets, les principaux biens en jeu sont les données collectées à propos des utilisateurs ou des groupes sociaux.

Le principe d'utilité collective

Une valeur éthique fondamentale pour juger de la qualité d'un système, d'une pratique ou d'une mesure réglementaire est la mise en balance des conséquences que génèrent ceux-ci. Il s'agit de la capacité, à partir d'une quantité finie de ressources, de produire un maximum d'utilité collective, c'est-à-dire le plus de bénéfices nets totaux pour le plus grand nombre d'individus. Ce principe est couramment associé à l'éthique utilitariste[30]. Par exemple, dans le cas de l'Internet des objets, le fait que certains objets connectés (mais pas tous) offrent plus de fonctionnalités, soient plus rapides, plus sécuritaires ou plus susceptibles de s'adapter aux préférences des utilisateurs, augmente la somme de bénéfices nets totaux pour le plus grand nombre d'individus. Par voie de comparaison, les failles de sécurité ou le manque de confiance dans cette industrie pourraient réduire l'utilité collective.

27 Commission de l'éthique en science et en technologie 2016, p. 42.
28 Canto-Sperber et Ogien 2006, chap. 1; O'Neill 2004.
29 Dietsch 2007; Nozick 1974.
30 Mill [2008] 1871, chap. 2; Singer 2011.

Le respect de la vie privée

Un principe éthique important dans le débat sur l'Internet des objets est le respect de la vie privée. Toutes choses étant égales, toute personne a droit à l'intimité dans sa sphère privée. Ce droit à l'intimité passe par certaines protections spécifiques. Par exemple, la non-divulgation des informations personnelles sur cette personne, la non-diffusion des images de cette personne, et ainsi de suite, sans son consentement libre, éclairé et continu[31].

À titre de rappel, il est difficile de cerner exactement ce qui fait partie de la sphère privée des personnes. Par exemple, certains considèrent que la sphère privée est simplement ce qui n'est pas inclus dans la sphère publique. Mais ces approches ne sont pas particulièrement informatives, puisque nous ne savons pas exactement ce qui relève de la sphère publique[32]. Or, comme nous l'avons mentionné dans la section 2.1.2., nous n'avons pas besoin d'une théorie complète et systématique de la vie privée aux fins du présent supplément. Nous pouvons supposer que plusieurs informations sont couvertes par le droit à la vie privée sans aborder des questions plus fondamentales entourant la nature de la sphère privée et les normes gouvernant le respect de cette sphère.

La transparence

Selon la valeur de transparence, le déploiement des technologies de surveillance et de contrôle doit se faire non pas dans une zone d'ombre, mais plutôt en partenariat avec des acteurs du milieu et des citoyens bien informés des principaux enjeux. La transparence « est une valeur démocratique essentielle à la gouvernance publique; elle témoigne d'une approche non paternaliste qui invite à une responsabilisation des divers acteurs sociaux[33] ».

La responsabilité

Selon la valeur de responsabilité, les personnes et les institutions doivent répondre de leurs actions. Les agents responsables réfléchissent aux conséquences de leurs actions et les prennent en compte dans leurs décisions. La responsabilité concerne parfois des individus. Par exemple, on entend souvent que les consommateurs doivent réfléchir aux conséquences d'une transmission de leurs informations personnelles à des entreprises par le biais d'objets connectés, car ils sont responsables de leur vie privée. Mais la responsabilité concerne aussi des institutions ou des entreprises. Par exemple, les entreprises doivent analyser et prendre en compte les impacts sociaux de la collecte de données personnelles.

Le principe de non-discrimination

La démarche d'évaluation de la Commission fait également appel à l'importance de la non-discrimination, notamment au regard du traitement des renseignements personnels. Le recours à des techniques comme le profilage ou le ciblage de certaines catégories de personnes en vue d'améliorer l'efficacité de la surveillance peut accroître les risques de discrimination et de stigmatisation. Des mécanismes institutionnels et des politiques doivent favoriser un traitement juste des citoyens sous surveillance. Cela diminue les risques qu'ils subissent des préjudices pouvant être difficiles à réparer.

31 DeCew 2018. La protection de l'intimité est aussi souvent associée à la protection des données sensibles. Voir Commission de l'éthique en science et en technologie (2017, p. 71) pour une définition des données sensibles.
32 *Ibid.*
33 Commission de l'éthique en science et en technologie 2003.

Le principe de faisabilité (ou d'effectivité)

Si la prise de décision éthique vise à réaliser ou à promouvoir certains idéaux, elle doit être sensible aux contraintes économiques, sociales, physiques ou autres auxquelles font face les acteurs. Sans quoi, les solutions proposées seront purement théoriques et inapplicables dans les circonstances. C'est l'idée derrière le principe de faisabilité (ou d'effectivité). Selon ce principe, les solutions proposées doivent être faisables ou potentiellement effectives, et donc tenir compte d'un certain nombre de contraintes[34].

Par exemple, une solution à certains des problèmes décrits dans le présent document serait l'abandon de l'économie de marché. Or, cette solution risque fortement de ne pas être effective ou faisable dans l'état actuel du monde. Donc, en vertu du principe de faisabilité, cette solution ne sera pas retenue ici.

2.3.2 Les recommandations inchangées

Certaines des recommandations mises en place en 2008 s'appliquent parfaitement à l'Internet des objets, et il n'est donc pas nécessaire de se pencher sur ces recommandations en détail. Trois recommandations issues de l'avis de 2008 ne changent pas avec l'arrivée de l'Internet des objets. La première concerne la pertinence, l'efficacité et la fiabilité :

- **Pertinence, efficacité et fiabilité.** Les moyens de surveillance et de contrôle les moins intrusifs doivent être privilégiés. Il faut aussi que les nouvelles technologies de surveillance et de contrôle ne soulèvent pas plus de problèmes qu'elles n'en règlent[35].

La surveillance via l'Internet des objets s'avère facilement intrusive et compromet grandement la vie privée des citoyens. Étant donné ce qui précède, la surveillance par l'Internet des objets ne peut être qu'une solution de dernier recours, à envisager dans des situations exceptionnelles où d'autres modes de surveillance ne répondent pas aux objectifs visés. Il va aussi de soi que ce mode de surveillance ne doit pas générer plus de problèmes qu'il n'en règle.

La deuxième recommandation concerne la proportionnalité entre la fin et les moyens :

- **Proportionnalité.** 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.

Cette recommandation ne dépend pas réellement de la technologie de surveillance étudiée. Tout comme l'identification par radiofréquence, la vidéosurveillance ou les systèmes biométriques, le recours à l'Internet des objets à des fins de surveillance doit respecter le principe de proportionnalité.

La troisième recommandation concerne l'acceptabilité sociale :

- **Acceptabilité sociale.** La population doit être favorable aux méthodes de surveillance préconisées par l'État. Il ne semble pas y avoir de volonté populaire d'interdire toutes les nouvelles technologies de surveillance et de contrôle. Dans certains cas, on observe même un intérêt pour ces technologies. On peut toutefois se demander si l'opinion publique est bien informée de ce développement technologique. Il vaudrait mieux recueillir des opinions éclairées à ce sujet, mais aussi éduquer les citoyens quant aux implications de ces technologies sur leurs droits[36].

34 Estlund 2014; Gaus 2016, chap. 1; Stemplowska et Swift 2016. Suivant Lipsey et Lancaster (1956), nous savons aussi qu'il peut être contre-productif de simplement imiter (ou approximer) les normes idéales dans des conditions non idéales.
35 Commission de l'éthique en science et en technologie 2008, p. xxi.
36 *Ibid.*, p. xxii.

Mentionnons d'abord que l'acceptabilité sociale est surtout un critère important dans les cas où les citoyens sont raisonnables et informés. Dans les cas où la population n'a pas accès aux informations pertinentes, ou ne se montre pas sensible aux raisons en présence, l'acceptabilité sociale est un facteur éthique moins important. Mais tout comme la recommandation précédente, l'acceptabilité sociale ne dépend pas de la technologie de surveillance étudiée. Elle s'applique donc parfaitement à l'Internet des objets. En particulier, une discussion publique éclairée, menée par des experts et des citoyens informés, est toujours appréciable[37]. Elle est importante lorsqu'il est question des droits des citoyens, comme le droit à la vie privée.

2.3.3 Les recommandations inapplicables

L'une des recommandations mises en place en 2008 ne s'applique pas à l'Internet des objets. Il s'agit du respect des finalités :

- **Respect des finalités.** Si des technologies de surveillance ne sont justifiées que pour l'atteinte de certains buts bien précis, on ne doit pas les utiliser à d'autres fins. Par exemple, il est inquiétant que des normes, des procédés, des pratiques, des moyens de surveillance et de contrôle mis en place dans la foulée d'attentats terroristes soient progressivement intégrés à la lutte à la petite délinquance, puis récupérés par le secteur commercial. Compte tenu de la facilité avec laquelle les nouvelles technologies de surveillance et de contrôle trouvent des applications et donc les finalités qui peuvent être très différentes, il convient de rester vigilant à cet égard[38].

Cette recommandation ne s'applique pas à l'Internet des objets. Elle concerne les technologies dont la finalité première et avérée est la surveillance des citoyens. Or, contrairement à la vidéosurveillance, aux systèmes biométriques et à l'identification par radiofréquence, l'Internet des objets n'a pas pour finalité première la surveillance des citoyens à des fins de sécurité et de contrôle. Ce n'est pas une technologie de surveillance; c'est une technologie développée à d'autres fins, mais qui permet *par accident* de mettre en place de nouvelles activités de surveillance.

La grande majorité des objets connectés en circulation (téléphones portables, voitures connectées, maisons intelligentes, vêtements connectés, etc.) ont d'abord deux grands objectifs : améliorer la qualité de vie des consommateurs (ou leur offrir de nouveaux services personnalisés) et permettre aux entreprises développant ces technologies d'augmenter leur profitabilité. La surveillance des citoyens par l'Internet des objets est une finalité *secondaire* ou *extrinsèque*.

2.3.4 Les recommandations à revoir et les nouvelles questions à résoudre

Enfin, deux recommandations issues de l'avis de 2008 sont à revoir, et de nouveaux problèmes devront être résolus. Commençons par les deux recommandations à revoir :

- **Consentement.** La Commission estime que, si le déploiement des nouvelles technologies de surveillance et de contrôle se fait de manière transparente et en accord avec les valeurs fondamentales des sociétés démocratiques, chaque individu n'a pas nécessairement à consentir au déploiement de ces technologies. Cependant, l'absence de consentement individuel libre, éclairé et continu soulève des enjeux éthiques. C'est pourquoi la Commission insiste aussi sur la nécessité de mettre en place des moyens permettant aux citoyens de faire valoir leurs doléances quant aux usages des technologies de surveillance. Elle estime de plus que les citoyens devraient être mieux informés sur une foule de points, qui vont des dispositions juridiques entourant le déploiement des technologies de surveillance jusqu'aux lieux et aux documents mis sous surveillance[39].

37 Naturellement, l'éducation aux nouvelles technologies de surveillance devrait être revue pour inclure l'Internet des objets. Voir Landry et Letellier (2016) sur la littératie numérique et les compétences à l'usage des nouvelles technologies, dont les objets connectés font partie.
38 *Ibid.*, p. xxiii.
39 *Ibid.*

Cette recommandation est directement liée au fonctionnement de la vidéosurveillance, des systèmes biométriques et de l'identification par radiofréquence. Contrairement à ces technologies, l'Internet des objets collecte des données revenant d'abord à des compagnies privées. Ces dernières pourraient ensuite les partager avec des corps policiers ou des services de renseignements. Les citoyens pourraient donc exiger le consentement libre, éclairé et continu quant à la collecte de leurs renseignements personnels par ces objets, *ne serait-ce que pour empêcher des compagnies privées d'avoir accès à ces renseignements*. Ainsi, les recommandations de l'avis de 2008 entourant le consentement doivent être adaptées à l'Internet des objets.

Notons aussi brièvement que l'avis de 2008 ne précise pas le type de consentement sur lequel il se penche. Il existe plusieurs interprétations de cette notion, selon le contexte. Par exemple, le consentement peut être explicite (c.-à-d. manifeste par des indications ou des actions claires) ou implicite, spécifique (c.-à-d. concerne seulement une fin bien précisée) ou « unilatéral » (« *blanket consent* »). La Loi sur la protection des renseignements personnels dans le secteur privé précise que le consentement à la collecte ou à l'utilisation des renseignements personnels d'une personne doit être « manifeste, libre, éclairé et être donné à des fins spécifiques[39] ». En d'autres termes, les transactions entre citoyens et acteurs privés sont régies par une exigence de consentement *explicite* (car le consentement doit être manifeste) et *spécifique*. Dans le présent supplément, c'est ce type de consentement qui nous intéresse, puisque, comme on vient de le mentionner, l'Internet des objets collecte des données revenant d'abord à des compagnies privées[40].

La seconde recommandation à revoir concerne la protection des renseignements personnels :

- **Protection des renseignements personnels.** L'acquisition de renseignements personnels peut compromettre le droit à la vie privée des personnes. Mais la collecte de ces renseignements peut aussi, dans certaines circonstances, contribuer à la sécurité des sociétés. Comment concilier (ou équilibrer) ces deux objectifs? Sur cet enjeu, l'avis demeure exploratoire (aucune réponse spécifique n'est proposée). Il met plutôt en lumière une foule de questions complexes touchant l'équilibre entre vie privée et sécurité. L'avis propose toutefois une démarche pour résoudre cette question : les gouvernements provincial et fédéral devraient mener des consultations publiques pour déterminer, collectivement, le juste équilibre en matière de protection des renseignements personnels et de sécurité publique et nationale.

D'une part, plusieurs experts ont tenu à rappeler que l'idée même d'un « compromis » ou d'un « équilibre » entre sécurité et vie privée est à revoir. Lorsqu'on collecte des renseignements, on s'expose à des fuites d'information pouvant compromettre la sécurité des personnes ou des institutions[41]. Puisqu'elles limitent ou encadrent la collecte de renseignements personnels, les mesures de protection de la vie privée renforcent la sécurité des personnes et des sociétés. Il faut donc éviter de mettre ces principes en opposition et reconnaître qu'ils vont généralement de pair. D'autre part, comme on peut le voir dans le paragraphe ci-dessus, la Commission a joué de prudence et a fait peu de recommandations spécifiques quant aux compromis entre vie privée et sécurité. Dans ce supplément, on tentera d'établir de nouveaux compromis acceptables entre protection de la vie privée et sécurité.

En plus de ces deux recommandations qu'il faudra revoir, la Commission se doit d'étudier le problème posé par le rôle central des acteurs privés dans la collecte de données par l'Internet des objets. Afin d'accéder aux données personnelles de citoyens collectées par l'Internet des objets, l'État doit collaborer avec des entreprises privées (car ce sont elles qui collectent ces données). Les risques éthiques ne découlent donc pas seulement des actions de l'État, mais aussi de celles des entreprises privées. Par exemple, les États pourraient avoir plus facilement accès aux données des citoyens en fonction des pratiques d'anonymisation et de chiffrement (parfois appelé « encryptage ») des données préconisées par l'industrie.

40 La question du type de consentement approprié pourrait se compliquer si les objets connectés et les données qu'ils collectent étaient la propriété de l'État. Pensons, à titre d'illustration, aux bornes de reconnaissance faciale utilisées dans certains casinos (ou d'autres établissements appartenant à des sociétés publiques). Or, dans ce cas de figure, les enjeux éthiques associés à l'Internet des objets seraient très semblables à ceux soulevés par la vidéosurveillance, un cas de figure déjà bien étudié dans l'avis de 2008.
41 Experts consultés.

Il s'agit d'abord de savoir si les États devraient intervenir pour encadrer le développement de l'Internet des objets. D'un côté, laisser l'industrie à elle-même ne semble pas une solution viable. Dans un contexte de laisser-faire, les entreprises sont peu incitées à investir dans la sécurisation de leurs technologies. La sécurité des appareils connectés est globale ou « holiste », c'est-à-dire qu'elle dépend de la sécurité de *toutes* les technologies reliées entre elles. Par exemple, une voiture connectée conçue à partir des plus hauts standards de sécurité est à risque si, par exemple, la connexion à Internet du véhicule n'est pas sécuritaire, un autre appareil connecté à la voiture (comme un téléphone, une tablette, etc.) est mal sécurisé, et ainsi de suite[42]. Dans ce contexte, les entreprises peuvent se renvoyer la balle et plaider que, tant qu'il n'y aura pas un environnement *global* sécuritaire pour développer l'Internet des objets, aucune d'elle n'a le fardeau individuel de mettre en branle les plus hauts standards de sécurité. On se retrouve alors dans un problème d'action collective classique : étant témoin de l'inaction des autres acteurs, chaque acteur n'a pas intérêt à agir[43]. C'est d'ailleurs pourquoi plusieurs compagnies importantes impliquées dans le développement de l'Internet des objets réclament une politique globale forçant toutes les entreprises à adopter certaines pratiques sécuritaires[44].

Naturellement, il semble donc que c'est aux États d'agir. En effet, ces derniers peuvent mettre en place des politiques qui s'appliquent à toutes les compagnies développant des objets connectés. Or, les États sont eux aussi aux prises avec un problème d'(in)action collective. Dans un contexte où les consommateurs peuvent acheter ou utiliser des objets connectés dans différents pays, les États hésitent à faire cavalier seul dans la lutte pour des objets connectés sécuritaires. Pourquoi le Québec ou le Canada mettraient-ils en place des politiques substantielles de sécurité des objets connectés si les États-Unis ou le Mexique refusent de mettre en branle des politiques similaires? Et si, au contraire, il faut attendre que tous les États adoptent une réglementation internationale, ne risque-t-on pas d'attendre longtemps[45]? Ainsi, la première question qui se pose est :

Question 1 Doit-on prioriser le laisser-faire, la législation nationale ou la législation internationale entourant l'Internet des objets?

Un autre enjeu de taille entourant l'Internet des objets concerne les responsabilités des différents acteurs impliqués. Par exemple, doit-on responsabiliser les consommateurs, les entreprises, les institutions étatiques ou tout à la fois ces trois acteurs?

Les consommateurs doivent assumer leur juste part de responsabilités dans la divulgation de données sensibles. Certains individus font visiblement preuve de négligence lorsqu'il est question de protéger leur vie privée (par exemple, en divulguant publiquement leurs informations sensibles sans que cela soit nécessaire).

Cependant, il est de plus en plus reconnu qu'en matière de cybersécurité et de protection de la vie privée, les consommateurs n'ont que peu ou pas de leviers pour se protéger. Par exemple, l'étendue de la collecte et du traitement de l'information est souvent cachée, soit indirectement par des politiques d'utilisation des données longues et arides que personne ne lit (qualité du consentement), ou directement lorsque la collecte est passive et invisible[46].

42 Neisse, Steri, Fovino et Baldini 2010; Roman, Najera et Lopez 2011; Sicari, Rizzardi, Grieco et Coen-Porisini 2015; Weber 2010.
43 Voir notamment Hardin 1968 et Ostrom 1990 sur les problèmes d'action collective.
44 Wattles et O'Sullivan 2019.
45 Voir Weber (2010) sur la possibilité d'une législation internationale.
46 Voir, par exemple, l'enquête menée par Fowler (2019).

Les pratiques en cours laissent peu de place à la négociation par les consommateurs des conditions acceptables d'utilisation des objets connectés. Par exemple, une personne en désaccord avec la politique de respect de la vie privée d'une grande compagnie technologique (Google, Microsoft, Apple, Facebook, etc.) peut difficilement contacter la compagnie pour négocier, de gré à gré, un contrat plus adapté à ses préférences. Si le problème se pose pour les objets et services « gratuits », il est encore plus marqué pour les objets ou services que le consommateur paie et pour lesquels il peut s'attendre à pouvoir exiger certaines conditions.

De plus, bon nombre d'entreprises se concentrent sur l'obtention du consentement *libre* et *éclairé*, mais ignorent la question du consentement *continu*. Par exemple, plusieurs entreprises ne s'assurent pas du maintien du consentement de l'utilisateur tout au long du cycle d'utilisation du produit connecté (elles tiennent plutôt pour acquis que, sauf indication contraire, le consentement obtenu en début d'utilisation est toujours maintenu). Or, la continuité est l'un des trois aspects centraux de la qualité du consentement.

En somme, le partage des responsabilités entre les consommateurs et les entreprises n'est pas simple. Ce problème est accentué par l'agrégation et le croisement de données. Comme souligné dans la section 2.1, la mise en commun de différentes données peut dresser un portrait beaucoup trop invasif des utilisateurs. Cela peut se produire même si les données en question ne semblent pas invasives. Une compagnie collectant des données de géolocalisation peut donc se déresponsabiliser sur la base du fait que, prises séparément, les données qu'elle collecte sont peu invasives. Il en va de même pour une entreprise collectant des données vocales, une autre collectant des données sur les préférences de consommation des utilisateurs, et ainsi de suite. Mais lorsqu'elles sont mises en commun et accessibles, ces données sont nettement invasives.

Dans ce contexte, il est difficile d'attribuer des torts et des responsabilités spécifiques quant à l'invasion de la vie privée. Chaque collecte de données y est pour quelque chose, bien que chaque collecte prise séparément ne soit pas particulièrement invasive. Conformément à ce qui précède, chaque entreprise responsable de la collecte de certaines données y est pour quelque chose, bien que chaque entreprise prise séparément ne soit pas particulièrement blâmable.

En regard de ces brèves remarques, deux questions importantes entourant le partage des responsabilités entre consommateurs et entreprises seront étudiées :

Question 2 Qui assume les responsabilités éthiques associées à l'Internet des objets?

Question 3 Comment améliorer la qualité du consentement dans l'utilisation de l'Internet des objets?

En amont de la question qui vise à savoir ce qu'il convient de faire des données recueillies en émerge une autre, pour savoir qui possède ces données. C'est pourquoi il faut aussi se pencher sur la question suivante :

Question 4 Comment concevoir la propriété des données recueillies par l'Internet des objets?

Naturellement, cette question fait intervenir des aspects juridiques entourant les notions de propriété privée, de données et de renseignements personnels (voir, à ce sujet, les remarques dans l'introduction sur les cadres juridiques québécois et canadien et la protection de la vie privée).

Cette question fait aussi intervenir des enjeux éthiques. À première vue, il semble que les consommateurs et les utilisateurs possèdent les données recueillies par leurs objets connectés. C'est ce qui a motivé les deux premiers points de la « charte des droits » de l'Internet des objets proposée par la *Open Internet of Things Assembly* (2012). Ces points sont : « les citoyens possèdent les données qu'ils (ou que leurs objets) créent » et « les citoyens possèdent les données que d'autres personnes créent à propos d'eux » (traduction libre).

La question est toutefois plus compliquée qu'il n'y paraît. Le passage des informations aux données est un travail complexe. Les données encodent des informations, ce qui nécessite un protocole de capture et un support physique de stockage. Très souvent, les compagnies possèdent ces protocoles et les supports physiques où sont stockées les données. Ce sont donc les compagnies, et non les utilisateurs, qui transforment l'information disponible en données. Donc, l'information initiale permettant la création de données semble appartenir au citoyen, mais c'est l'entreprise qui en détient le protocole de capture et de stockage. Ces facteurs compliquent la question relative à la possession des données recueillies par les objets connectés.

Enfin, le fait que des entreprises ou des États puissent posséder des données sur des personnes ne les autorise pas à posséder n'importe quelles données, ni à en faire ce que bon leur semble. Par voie de comparaison, des personnes peuvent posséder des voitures sans pour autant avoir l'autorisation de conduire à la vitesse qui leur plaît. Entrent en scène les contraintes sur la collecte et l'usage des données.

Des questions éthiques se posent quant aux limites légitimes entourant la collecte, le stockage, le traitement et la vente (ou le transfert) des données. Ces questions se posent tant du point de vue des États (qui mettent en place des mécanismes de surveillance à diverses fins) que de celui des entreprises (qui veulent rentabiliser les données recueillies).

Pour les entreprises privées, être en mesure de collecter, de conserver, de vendre ou de transférer librement les données est très profitable. Plusieurs entreprises prédisent déjà que l'accès aux données sera le « nouveau pétrole » du 21e siècle, c'est-à-dire la ressource incontournable au développement de toutes les industries, et irremplaçable[47]. Toutes choses étant égales, les données augmentent les chances d'une entreprise de bien cibler ses clients et leurs besoins, de bien communiquer avec eux, d'anticiper les tendances du marché, et ainsi de suite. Plus les entreprises disposeront de données sur un client ou sur le comportement des consommateurs, plus elles seront en mesure d'augmenter leurs profits. Il est donc dans l'intérêt des entreprises de collecter, de conserver ou de vendre librement des données. Mais cet intérêt commercial n'est pas forcément compatible avec d'autres principes, comme le respect de la vie privée des consommateurs[48]. Il faut donc trouver une manière raisonnable de concilier l'intérêt marchand des entreprises à la protection et au respect de la vie privée des consommateurs.

47 *The Economist* 2017.

48 Allhoff et Henschke 2018, §2-3; Neisse, Steri, Fovino et Baldini 2015; Roman, Najera et Lopez 2011; Sicari, Rizzardi, Grieco et Coen-Porisini 2015; Weber 2010.

Les enjeux sont différents en ce qui concerne les États[49]. Comme mentionné précédemment, des experts et des observateurs s'inquiètent du fait que l'Internet des objets soit l'outil de surveillance de masse par excellence[50]. Ces craintes sont amplifiées dans le cas des technologies collectant plusieurs données distinctes. Contrairement à une faille de sécurité ou de la surveillance à partir d'un seul objet connecté collectant peu de données sensibles (comme une cafetière connectée), une faille de sécurité dans un véhicule connecté risque de donner accès à une foule d'informations sensibles sur les utilisateurs.

Alors que les agences justifient l'espionnage domestique sur la base de la sécurité civile et nationale, l'une des craintes des experts est que la surveillance serve aussi à repérer et à contrecarrer des activités légitimes d'activisme et d'opposition politique[51]. Dans sa critique de la loi C-51, la Ligue des droits et libertés exprimait ses inquiétudes face à un tel risque :

> Parmi les atteintes à la sécurité visées par la loi il y a « entraver le fonctionnement d'infrastructures essentielles ». Ainsi, malgré les assurances du gouvernement, des groupes autochtones, environnementaux et citoyens se portant à la défense du bien commun qui posent des gestes de résistance aux pipelines pourraient faire les frais de ces nouveaux pouvoirs[52].

Notons enfin qu'il peut y avoir des enjeux de surveillance et de contrôle pour d'autres acteurs (c.-à-d. des acteurs qui ne sont ni des entreprises ni des États). Pensons aux objets connectés développés dans le monde médical. Ces objets sont parfois utilisés pour informer ou alerter les proches. Les bracelets de détection de chutes en sont un bon exemple. Si leur usage est mal encadré, ou si les données collectées par ces objets sont mal gérées, les familles et les proches des patients pourraient empiéter sur le droit de ceux-ci à la vie privée.

Bref, un problème éthique important concerne les principes généraux entourant l'utilisation des données générées par les objets connectés. Deux questions ont été retenues à cet égard :

Question 5 Quelles garanties de sécurité numérique devraient être offertes à l'utilisateur?

Question 6 Quelles sont les limites raisonnables entourant le stockage, la concentration, le traitement et la vente des données recueillies par l'Internet des objets?

Le prochain chapitre tente de répondre à ces différentes questions et formule des recommandations à l'attention de différents acteurs.

49 Il peut cependant y avoir une juxtaposition des intérêts d'entreprise et des intérêts étatiques. Il suffit de penser aux sociétés d'État à vocation commerciale. Prenons un exemple simple, soit le repérage des « personnes d'intérêt » par la société Trans Mountain. On apprenait récemment que cette entreprise repère les activistes publiant des messages d'opposition aux pipelines sur les réseaux sociaux, et en particulier de militants autochtones (Ferradini 2019). Dans une telle situation, le problème n'est pas simplement qu'une entreprise tente d'en savoir plus sur ses opposants. De telles collectes de renseignements prennent une tout autre signification, puisque l'entreprise appartient à l'État.

50 Berkman Centre 2016; Doctorow 2015; McArdle 2016; Porup 2016; Powles 2015; Timm 2016.

51 Ligue des droits et libertés 2016; Petrou 2017.

52 Ligue des droits et libertés 2016. Notons que sous le gouvernement de S. Harper, la Gendarmerie royale du Canada avait effectivement étiqueté le mouvement anti-pétrole comme une menace à la sécurité nationale. Paul Champ, un avocat et défenseur des libertés civiles, avait alors exprimé des craintes : « En ce qui a trait au projet de loi C-51, moi et d'autres groupes avons de réelles préoccupations. Nous estimons que le projet de loi permettra de cibler non seulement des terroristes qui sont impliqués dans des activités criminelles, mais aussi des individus qui protestent contre les politiques publiques canadiennes. » (McCarthy 2015, traduction libre).

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