



Les risques et enjeux éthiques des véhicules connectés

Rapport d'analyse

**Les risques
et enjeux éthiques
des véhicules connectés**
Rapport d'analyse

Commission de l'éthique en science et en technologie

888, rue Saint-Jean, bureau 555

Québec (Québec) G1R 5H6

www.ethique.gouv.qc.ca

Coordination

Nicolas Bernier, secrétaire général

Recherche et rédaction

Erika Olivaux Marmignon, conseillère étudiante en éthique des sciences et des technologies

Philippe Verreault-Julien, conseiller en éthique des sciences et des technologies

David Hughes, conseiller en éthique des sciences et des technologies

Kathia Légaré, conseillère en éthique des sciences et des technologies

Élise Bastille-Lavigne, conseillère en éthique des sciences et des technologies

SOUTIEN TECHNIQUE

Révision linguistique

Corinne Sarian

Graphisme, mise en page et accessibilité

Pige communication

Photo de page couverture

Shutterstock

Rapport d'analyse adopté à la 116^e séance de la
Commission de l'éthique en science et en technologie le 29 mai 2026.

© Gouvernement du Québec

Dépôt légal : Août 2026

Bibliothèque et Archives nationales du Québec

ISBN : 978-2-5 55-04433-3 (version PDF)

ISBN : 978-2-555-04432-6

Comment citer ce document :

« Commission de l'éthique en science et en technologie (CEST). 2026.
Les risques et enjeux éthiques des véhicules connectés. »

Table des matières

Introduction	1
--------------	---

CHAPITRE 1

Contexte	3
----------	---

1.1 Les véhicules connectés	5
1.2 Les données récoltées	7
1.2.1 Données de géolocalisation	7
1.2.2 Données de conduite et d'utilisation	8
1.2.3 Données de capteurs	8
1.2.4 Données du compte client	8
1.2.5 Données du système d'infodivertissement	9
1.2.6 Données de l'interface véhicule/téléphone	9
1.3 Les acteurs	9
1.3.1 Rencontre de plusieurs industries	9
1.3.2 Organismes régulateurs	10
1.3.3 Autres acteurs	11
1.4 Les dispositions réglementaires et législatives	12
1.4.1 Législation	12
1.4.2 Règlements, normes et lignes directrices	14

CHAPITRE 2

Analyse éthique : valeurs et principes	15
--	----

2.1 La protection de la vie privée	16
2.2 L'autodétermination informationnelle	17
2.3 L'autodétermination collective	17
2.4 La souveraineté numérique et la souveraineté des données	19
2.5 Le bien commun	19
2.6 La protection de l'environnement	19
2.7 La responsabilité	20

CHAPITRE 3

Analyse éthique : cartographie des enjeux 21

3.1	Les risques d'accroissement de la surveillance et d'érosion de la vie privée	22
3.2	La vie privée en famille et les violences intrafamiliales	23
3.3	La surveillance au travail	25
3.4	Le piratage et le vol des données personnelles	25
3.5	Les enjeux liés à l'autopartage et à la location de courte durée	27
3.6	Le droit d'usage et la réparabilité	28
3.7	Les enjeux liés à la personnalisation des assurances en fonction des habitudes de conduite	28
3.8	Les effets environnementaux grandissants des voitures et des technologies numériques	29
3.9	L'accès aux données par les services de police	31
3.10	La sécurité nationale	33
3.11	Les enjeux entourant les flottes gouvernementales	34
3.12	La valorisation des données d'utilité publique	35

CHAPITRE 4

Enjeux liés à l'encadrement et à son application 37

4.1	Une industrie difficile à réguler	38
4.2	Les limites du consentement	39
4.3	Les défis d'implantation de l'approche minimaliste en matière de collecte, conservation et destruction des renseignements personnels	40
4.4	L'efficacité limitée des mécanismes en place	41

Conclusion 43

Notes et références 44

Membres du comité d'expertes et d'experts 54

Commission de l'éthique en science et en technologie 55

Introduction

Longtemps symboles de liberté et de vie privée, les véhicules sont maintenant des « ordinateurs sur roues »¹ : ils recueillent et transmettent une quantité importante de données de natures variées sur les véhicules et leurs occupants. Ces données sont ensuite traitées et transmises pour diverses fins, de la prédiction de bris mécanique à la navigation satellite, en passant par la création de profils marketing.

Un rapport de la firme McKinsey estime qu'en 2030, 90 % des véhicules vendus à l'échelle mondiale seront connectés, comparativement à 50 % en 2024². Il s'agit, selon plusieurs analyses, d'un marché en pleine expansion³. Les voitures offrent maintenant de nombreuses fonctionnalités qui requièrent de la connectivité, telles que la navigation ou encore l'intégration d'un ensemble d'applications mobiles à l'écosystème du véhicule.

La fondation Mozilla, dans un rapport publié à l'automne 2023, a qualifié les automobiles comme étant la « pire » catégorie de produits qu'elle n'ait jamais évaluée en ce qui concerne la vie privée⁴. Ce rapport révèle que les constructeurs automobiles procèdent à une collecte massive de renseignements personnels et de données qu'ils partagent ensuite de manière opaque avec une variété de tierces parties. Au printemps 2024, une série de reportages du *New York Times* dévoilait plusieurs faits troublants concernant la connectivité des véhicules. On y apprenait que General Motors/OnStar recueillait des données sans le consentement des propriétaires de véhicules. Ces données étaient ensuite vendues à des firmes d'analyse de risques (p. ex. Verisk ou LexisNexis), qui elles-mêmes vendaient ces analyses à des assureurs. Des propriétaires de véhicules ont ainsi vu leurs primes exploser soudainement. Ces hausses étaient dues à la transmission non transparente de leurs données, sans qu'ils en aient eu conscience. Dans la foulée de ce scandale, un recours collectif a été intenté contre General Motors/OnStar et LexisNexis⁵. L'État du Texas a également intenté une poursuite contre General Motors/OnStar⁶. General Motors/OnStar s'est vu interdire par la

Federal Trade Commission de vendre ou de partager certaines données pendant cinq ans et a accepté en mai 2026 un règlement d'un montant de 12,5 millions de dollars américains⁷. Des reportages ont aussi mis en lumière que les données de géolocalisation permettaient à des conjoints violents de suivre les déplacements de leur partenaire⁸ ou encore que des applications mobiles pouvaient recueillir des données et les transmettre à de nombreux tiers, pas seulement à des assureurs⁹.

Au Canada, un rapport produit par la BC Freedom of Information and Privacy Association rapportait en 2015 que les constructeurs automobiles échouaient généralement à se conformer aux exigences légales en matière de vie privée¹⁰. Au Québec, l'Union des consommateurs a publié en 2025 un rapport sur les voitures connectées qui concluait, entre autres, que l'encadrement légal en vigueur au Canada est inadéquat pour gérer les risques en matière de vie privée et protéger adéquatement les consommateurs et les consommatrices. Cela dit, les enjeux éthiques liés à la connectivité des véhicules ont généralement reçu moins d'attention au Québec et au Canada qu'aux États-Unis.

Selon un sondage, 60 % des Canadiennes et Canadiens conduisant des véhicules connectés s'inquiètent de la confidentialité des données¹¹. La connectivité commence également à alarmer les décideurs publics. Différentes agences de protection de la vie privée aux États-Unis ou en Europe commencent à mener des enquêtes ou reçoivent des demandes à cet effet¹². Des acteurs européens se questionnent à savoir si les lois actuelles sont suffisantes¹³.

L'**objectif principal** de ce rapport d'analyse est de fournir aux décideurs publics, aux personnes élues et aux membres de l'administration publique une cartographie des enjeux et risques éthiques soulevés par les voitures connectées.

Un **objectif secondaire** est d'identifier des enjeux et perspectives de travaux futurs sur les véhicules connectés, l'Internet des objets, la vie privée ou encore la surveillance. L'analyse proposée pourra ainsi servir de base pour rédiger des **recommandations** dans le cadre de travaux ultérieurs.



Chapitre 1

Contexte

Source convoitée de profits, les données occupent une place grandissante dans l'économie mondiale. Les véhicules connectés communiquent et reçoivent de l'information à l'aide de diverses technologies sans fil. Les constructeurs ont un intérêt pécuniaire à continuer de développer ces fonctionnalités et à convaincre les consommateurs de leurs avantages, principalement liés au confort et à la sécurité.

Véhicules connectés ou véhicules automatisés ?

Il faut distinguer les véhicules connectés des véhicules automatisés. Les véhicules automatisés peuvent effectuer certaines actions sans intervention de la personne qui conduit. Ils nécessitent une quantité importante de données pour fonctionner adéquatement, et sont donc toujours des véhicules connectés. Ils doivent

notamment recevoir et traiter de l'information sur leur environnement (détecter les obstacles pour les éviter, etc.). Le contraire n'est pas vrai : de nombreux véhicules connectés ne sont pas ou sont peu automatisés. Le tableau ci-après présente les échelles de connectivité des véhicules¹⁴.

Échelle de connectivité des véhicules proposée par Privacy4Cars¹⁵

Niveau	Type de connectivité	Description
0	<i>Aucune connectivité</i>	Le véhicule ne peut se connecter ni à Internet ni à d'autres appareils. Il n'a pas de connexion Bluetooth.
1	<i>Connectivité locale uniquement</i>	Le véhicule peut se connecter à d'autres appareils (par exemple par Bluetooth ou USB), mais ne peut exploiter la connectivité des appareils pour offrir des services connectés à bord du véhicule.
2	<i>Connectivité indirecte</i>	Le véhicule n'a pas de connectivité native qui lui est propre (par exemple une connexion télématique par le biais d'une SIM intégrée), mais peut se connecter à d'autres appareils (par exemple par Bluetooth ou USB) et exploiter la connectivité de ces appareils pour offrir des services connectés de la marque du constructeur, par le biais du système d'infodivertissement.
3	<i>Connectivité directe, locale uniquement, services connectés du constructeur exclusivement</i>	Le véhicule a sa propre connectivité native (par exemple, une connexion télématique par le biais d'une SIM intégrée) qui sert à offrir des services connectés de la marque du constructeur, à l'intérieur du véhicule uniquement.

Niveau	Type de connectivité	Description
4	<i>Connectivité directe, locale et à l'extérieur du véhicule, y compris sur les différents appareils personnels des utilisatrices et utilisateurs</i>	Le véhicule a sa propre connectivité native qui sert à offrir une large gamme de services connectés pouvant être utilisés depuis l'intérieur du véhicule ou ailleurs (via les appareils personnels associés avec les véhicules).
5	<i>Connectivité directe, le véhicule sert de plateforme communiquant avec plusieurs services tiers, localement comme à l'extérieur du véhicule, y compris avec d'autres véhicules et infrastructures (V2X)</i>	Le véhicule a sa propre connectivité native (par exemple une connexion télématique par le biais d'une SIM intégrée) qui sert à offrir une large gamme de services connectés pouvant être utilisés depuis l'intérieur du véhicule ou ailleurs (via les appareils personnels associés avec les véhicules), et qui peut interagir avec les infrastructures et l'environnement ou les véhicules connectés de façon similaire.

L'automatisation des véhicules et leur arrivée sur le marché posent de nombreux défis, qui ne font toutefois pas l'objet de ce document de réflexion qui se concentre sur les enjeux éthiques liés à la **connectivité** des véhicules.

Les véhicules récents sont également parfois qualifiés de véhicules définis par logiciel, ou *software defined vehicles (SDV)*¹⁶. En effet, les systèmes logiciels jouent dorénavant un rôle central – plus que le matériel – dans les

fonctionnalités des automobiles. Une des principales conséquences de cette transformation des véhicules est que leurs fonctionnalités peuvent désormais être améliorées, modifiées, ajoutées ou retirées à l'aide de mises à jour à distance. Les réparations, elles aussi, sont plus susceptibles de nécessiter une intervention sur la dimension logicielle. Les véhicules définis par logiciel dépendent donc de la connectivité.

1.1 Les véhicules connectés

Les véhicules connectés sont constitués de technologies multiples qui servent des fonctionnalités variées. On peut diviser la connectivité des véhicules en deux branches : la télématique d'une part, et l'infodivertissement de l'autre.

Les systèmes **télématiques** reposent sur les données relatives aux systèmes du véhicule, produites par une multitude de capteurs. Ces données sont utilisées pour faciliter l'entretien du véhicule (prédiction de bris, diagnostic et alerte lorsqu'un rendez-vous est requis), et permettre l'automatisation de certaines fonctions. La télématique permet de suivre en temps réel la localisation et l'activité du véhicule. En cas de

freinage très brutal ou d'impact, un message d'alerte peut être envoyé automatiquement aux services d'urgence. Les données de conduite ont une utilité pour les assureurs, puisqu'elles permettent d'évaluer les habitudes et comportements de la personne qui conduit. Enfin, les systèmes télématiques permettent également de contrôler certaines fonctions à distance (climatisation et chauffage, verrouillage, etc.) par une application mobile, par exemple.

Les véhicules sont désormais dotés de systèmes d'**infodivertissement** : aide avancée à la navigation et à la planification des déplacements (notamment avec des trajets permettant d'éviter la congestion routière, la recherche d'hôtels ou

de restaurants sur l'itinéraire, etc.), services de *streaming* de musique, radio, mais aussi films et jeux (ces derniers n'étant accessibles que lorsque le véhicule est à l'arrêt). Ces systèmes peuvent utiliser les données télématiques; ils peuvent aussi être connectés à l'appareil mobile des utilisatrices et utilisateurs, par exemple afin que ces derniers aient accès à leurs calendriers, listes de contact, courriels, messages et appels, depuis l'écran embarqué.

Connectés comment ?

Les véhicules connectés emploient différentes technologies de communication sans fil pour répondre à différents besoins; parmi celles-ci, on compte la technologie cellulaire de cinquième génération (5G), la communication dédiée à courte distance (CDDC), le Wi-Fi, la technologie Bluetooth ou des satellites.

L'accès à Internet peut passer par l'appareil mobile de la personne qui conduit, même si les véhicules ont de plus en plus leur propre connectivité (par le réseau cellulaire ou, depuis récemment, par satellite) et peuvent servir de point d'accès mobile (Wi-Fi).

Connectés à quoi ?

Les véhicules connectés peuvent communiquer avec les appareils mobiles de la personne au volant ou des passagers, mais aussi avec d'autres véhicules dans les alentours et les infrastructures de transport environnantes (comme les feux de circulation). Ces différents types de communication sont dénotés de la façon suivante : V2V (véhicule à véhicule), V2I (Véhicule à infrastructure), V2X (Véhicule à tout, c'est-à-dire l'ensemble de l'environnement de la connectivité).

Où sont stockées les données ?

Une grande quantité de données sortent du véhicule et sont conservées sur des serveurs infonuagiques. Cela n'empêche pas que certaines données peuvent être stockées localement, c'est-à-dire dans le véhicule.

Les services connectés sont-ils payants ?

Certaines fonctionnalités connectées sont entièrement gratuites, tandis que plusieurs constructeurs proposent un abonnement payant. L'achat d'un véhicule neuf s'accompagne

généralement d'un abonnement gratuit pour une durée limitée qui peut varier entre une et cinq années.

Comment la voiture et le téléphone sont-ils connectés ?

La communication entre les appareils intelligents et les voitures connectées est bidirectionnelle. Il n'est pas strictement obligatoire de posséder un téléphone intelligent pour utiliser sa voiture connectée, mais les deux sont désormais intégrés de différentes façons.

D'une part, les constructeurs automobiles proposent des applications mobiles liées à leurs services connectés. Ces applications permettent, entre autres, d'utiliser les fonctions de contrôle à distance (climatisation, verrouillage), de suivre la localisation du véhicule (par exemple, une notification peut être envoyée sur un téléphone si le véhicule sort d'un certain périmètre ou s'il est utilisé par un conducteur ou une conductrice secondaire) et de recevoir les informations sur l'entretien du véhicule.

D'autre part, le traditionnel autoradio des voitures a été remplacé par des écrans multimédias aux fonctionnalités multiples. Ces systèmes d'infodivertissement peuvent être utilisés de façon autonome ou en étant intégrés avec les appareils cellulaires.

Grâce à une connexion filaire, Wi-Fi ou Bluetooth, la personne au volant peut accéder à sa musique, à son calendrier, à ses contacts, passer et recevoir des appels, etc., à partir de l'écran embarqué du véhicule. De plus, ces systèmes intègrent de plus en plus des systèmes d'intelligence artificielle (IA), notamment des agents conversationnels comme Gemini AI qui permettent de vérifier les itinéraires, de répondre aux questions de la personne qui conduit, etc.

Les véhicules connectés s'intègrent dans l'Internet des objets, c'est-à-dire « l'ensemble des objets physiques (ex. appareils, capteurs, supports de stockage) mis en réseau et communiquant entre eux via Internet » ou d'autres réseaux¹⁷. De nos jours, de plus en plus d'objets sont ainsi connectés, des téléviseurs aux bouilloires en passant par les montres et les machines à laver. En 2025, un journaliste

informatique a analysé le code de la prochaine version de Gemini et a constaté qu'une fonctionnalité prochaine pourrait permettre aux utilisatrices et utilisateurs d'accéder à Google Home depuis leur véhicule, faisant de ce dernier

un centre de contrôle pour l'ensemble des appareils connectés de leur domicile¹⁸. Des constructeurs automobiles sont également en train de développer des fonctionnalités similaires¹⁹.

1.2 Les données récoltées

Dans l'écosystème des véhicules connectés, des données très nombreuses et variées sont récoltées et stockées. Cette section offre un panorama des différents types de données concernées. Comme indiqué précédemment, on peut diviser ces types de données en deux grandes catégories : les données des systèmes télématiques (données de conduite et d'utilisation, données de géolocalisation, données de capteurs), et celles des systèmes d'infodivertissement.

Les voitures connectées sont une source de mégadonnées, ou données massives (*big data*), au même titre que les interactions sur les médias sociaux, entre autres. Celles-ci se distinguent en premier lieu par leur taille (volume), par la rapidité de leur collecte (vélocité), leur variété (audio ; image ; numérique, etc.), et par leur valeur²⁰. Le *Grand dictionnaire terminologique* de l'Office québécois de la langue française propose une définition simple et éclairante des mégadonnées : « ensemble d'une très grande quantité de données, structurées ou non, dont le traitement et l'analyse exigent l'utilisation de technologies avancées ». Elles sont donc étroitement liées aux développements technologiques qui déterminent les modalités d'extraction, de transmission et de traitement, c'est-à-dire la quantité et la variété de données qui peuvent être produites, recueillies et analysées ainsi que leur qualité (type et précision). Les mégadonnées permettent de produire des connaissances sur le comportement des personnes et sur leur environnement, qui permettent en retour de faire des prédictions et de prendre des décisions, notamment sur la configuration des systèmes²¹.

Ainsi, les données récoltées par les véhicules connectés (voir les sections 1.2.1 à 1.2.6) sont susceptibles d'être anonymisées, agrégées, et intégrées aux ensembles de mégadonnées pour ensuite être échangées sur les marchés. Elles

peuvent servir diverses finalités (en ce qui concerne les renseignements personnels, ces fins doivent selon la législation québécoise être « sérieuses et légitimes »). La grande valeur commerciale des données repose sur le partage et l'utilisation de ces mégadonnées.

1.2.1 Données de géolocalisation

Les données de géolocalisation sont une pièce centrale de la connectivité des véhicules. Comme leur nom l'indique, elles permettent de situer les véhicules en temps réel, grâce aux données géographiques (latitude, longitude, altitude) et aux données de mouvement (vitesse, direction). Souvent associées à la date et l'heure, elles permettent aussi de faire l'historique de localisation. Elles peuvent être récoltées par des capteurs GPS intégrés au véhicule, ou par triangulation avec les tours cellulaires lorsque ce dernier est connecté au réseau cellulaire.

Ces données ont plusieurs utilités : assistance à la navigation, incluant des suggestions d'itinéraires, mais aussi de commerces à proximité comme des restaurants, envoi de secours en cas d'accident, repérage du véhicule en cas de vol, gestion de flotte, surveillance du véhicule par son propriétaire (notamment lorsqu'il est utilisé par d'autres conducteurs ou conductrices).

Par ailleurs, les données de géolocalisation comptent parmi les données les plus préoccupantes en matière d'impact sur la vie privée. La Commission sur l'accès à l'information considère qu'elles ne peuvent être anonymisées²². En effet, ces données, lorsqu'elles sont analysées, sont extrêmement révélatrices : elles peuvent donner lieu à des inférences précises sur les caractéristiques d'une personne et sur son mode de vie. Par exemple, les déplacements entre le domicile

et le lieu de travail peuvent permettre d'identifier une personne ; à partir de là, il est facile de connaître les autres lieux que celle-ci fréquente.

1.2.2 Données de conduite et d'utilisation

Les véhicules connectés peuvent collecter des données d'utilisation et de conduite. Les données d'utilisation concernent l'état du véhicule ou de son environnement, ainsi que le statut des fonctionnalités : verrouillage et déverrouillage du véhicule, réglage de climatisation et chauffage, ouverture des portes et des vitres, etc.²³ Quant aux données sur la conduite, elles peuvent comprendre la vitesse du véhicule, le port de la ceinture, les données d'accélération et de freinage²⁴.

Les données de conduite peuvent être particulièrement utiles en ce qui a trait aux assurances (voir la section 3.7). Le conducteur ou la conductrice peut se voir attribuer un score de conduite qui prend en compte sa façon de conduire (freinage et accélération brusques ou doux, heures de conduite, etc.) : les personnes jugées à risque peuvent voir leurs primes d'assurance augmenter, tandis que celles jugées plus prudentes peuvent être récompensées par des tarifs plus avantageux.

D'apparence anodine, les données du véhicule peuvent constituer des renseignements personnels ou permettre d'inférer d'autres données sur les conductrices ou conducteurs et leurs habitudes. Par exemple, le comportement de conduite est propre à chaque personne et rend ainsi possible son identification²⁵.

1.2.3 Données de capteurs

Les véhicules connectés sont pourvus de nombreux capteurs, incluant des caméras, externes et internes, qui récoltent des données sur le véhicule, la personne au volant, les passagers et passagères et l'environnement.

Certains capteurs ne sont pas nouveaux et étaient déjà présents dans les véhicules non connectés, comme ceux qui fournissaient l'information sur le tableau de bord (niveau d'essence, etc.). Toutefois, alors que ces

capteurs étaient dans les véhicules traditionnels uniquement connectés à l'ordinateur de bord, et accessibles uniquement avec un accès physique au véhicule, ils sont maintenant accessibles à distance. De nouveaux capteurs sont ajoutés (p. ex. capteurs de pression des pneus Bluetooth) pour générer plus d'informations sur l'état du véhicule. Ces données, qui peuvent être consultées à distance par les techniciens et techniciennes, servent à la prévention de bris, au diagnostic et à la réparation à distance, à l'analyse, etc.

Les caméras et capteurs internes servent par exemple à détecter des signes de fatigue ou d'inattention chez la personne qui conduit, ou à vérifier que cette dernière ainsi que les autres personnes occupant le véhicule portent leur ceinture de sécurité.

Les caméras externes servent aux fonctions d'aide à la conduite (stationnement, trafic) ou de sécurité — comme c'est le cas du mode Sentinelle de Tesla, dont les caméras peuvent capter des images même lorsque le véhicule est éteint. Les images récoltées incluent des photos de passants et passantes.

Les images récoltées par les caméras sont disponibles pour les utilisatrices et utilisateurs et leur appartiennent : ils sont donc en mesure de les utiliser à des fins diverses et variées, plus ou moins légitimes.

1.2.4 Données du compte client

Certaines données d'identification doivent être transmises par le client ou la cliente au moment de l'achat d'un véhicule connecté ou lors de la souscription aux services connectés. Il peut s'agir des informations bancaires, des renseignements figurant sur le permis de conduire, des coordonnées complètes, etc.

Le fait de communiquer ces données très sensibles pour l'achat d'un véhicule n'est pas nouveau. De plus, ces données ne sont pas collectées par les deux systèmes mentionnés précédemment, et ne sont donc pas issues de la connectivité. Elles font toutefois partie prenante de l'écosystème de la connectivité, puisqu'elles sont désormais liées à un compte client, et sont parfois accessibles depuis le véhicule ou depuis

une application. Les serveurs dans lesquels elles sont conservées peuvent également faire l'objet de cyberattaques (voir la section 3.4).

1.2.5 Données du système d'infodivertissement

Les véhicules connectés recueillent les données d'usage des services connectés, par exemple : les données de recherche ; l'utilisation des écrans multimédias ; les entrées du calendrier et du carnet d'adresses ; les préférences et favoris des applications (musique, navigation), ainsi que les adresses enregistrées.

1.2.6 Données de l'interface véhicule/téléphone

En plus des données du véhicule, les constructeurs peuvent également récolter des données de toutes sortes à partir du téléphone des utilisatrices et utilisateurs. Cela peut se faire au moyen de l'interface entre le téléphone et le véhicule, ou encore, directement par le téléphone, par le biais d'une application, par exemple (certaines fonctionnalités connectées n'étant disponibles que si l'application est ouverte sur le téléphone). Par ailleurs, les systèmes d'infodivertissement sont souvent compatibles avec des applications mobiles tierces, telles qu'Android Auto ou Apple CarPlay,

avec lesquelles l'utilisateur peut contrôler d'autres applications de son téléphone à partir de l'écran du véhicule.

L'intégration des univers connectés des véhicules et des appareils mobiles donne lieu à de nombreuses possibilités de collecte de données. Les applications, par exemple, en plus de collecter l'information d'utilisation (texte saisi, clics, défilements, etc.), recueillent parfois les données stockées sur le téléphone et celles d'autres applications. Au-delà du téléphone, les véhicules offrent de plus en plus de fonctionnalités en lien avec l'Internet des objets (appareils mobiles, mais aussi électroménagers, télévisions, etc.). L'intégration d'agents conversationnels et d'assistants IA (comme Gemini) dans les systèmes comme Android Auto accentue cette tendance : les différents appareils pourraient être contrôlés depuis le véhicule. Dans le futur proche, des agents IA pourraient avoir accès aux données du véhicule pour prendre certaines décisions en lien avec l'utilisation du véhicule, mais qui ne relèvent pas de la conduite automatisée.

Le téléphone est ainsi devenu un portail d'entrée pour avoir accès à différents aspects de la vie des personnes : l'interface téléphone/véhicule rend possible la collecte de ces données par les acteurs de l'industrie automobile, en premier lieu les constructeurs et leurs partenaires. De même, les données concernant les véhicules et leurs utilisatrices et utilisateurs sont recueillies par les acteurs des technologies numériques, au-delà de l'industrie automobile.

1.3 Les acteurs

1.3.1 Rencontre de plusieurs industries

L'intégration des technologies connectées dans les véhicules a complètement transformé le paysage de l'industrie automobile. En effet, alors que les innovations relevaient auparavant principalement de la mécanique, la concurrence se joue désormais en grande partie sur les technologies de l'informatique et du numérique. Les constructeurs automobiles ont dû développer de nouvelles expertises et tisser

de nombreux partenariats pour développer des technologies de plus en plus sophistiquées. En raison de la grande diversité des expertises requises pour la conception et la production des voitures modernes, des acteurs extrêmement nombreux participent à ce processus. Les géants des technologies numériques se sont démarqués par leur expertise déjà existante dans le domaine des technologies numériques et sont ainsi devenus des acteurs importants du secteur automobile.

L'IA prend également une place grandissante dans ce secteur. L'automatisation des voitures repose en effet sur l'analyse des données et la prise de décision algorithmique. En plus de la conduite automatisée, les divers capteurs des véhicules (voir la section 1.2.3) récoltent une énorme quantité de données, qui peuvent s'avérer très rentables pour les constructeurs automobiles. Encore faut-il pouvoir les exploiter, ce qui nécessite des moyens technologiques et matériels importants. Enfin, les systèmes d'infodivertissement reposent eux aussi de plus en plus sur des systèmes d'IA pour offrir des fonctionnalités toujours plus poussées aux utilisatrices et utilisateurs.

Au cœur de l'industrie se trouvent les **constructeurs automobiles** : les plus connus sont **nord-américains** (notamment General Motors, Tesla, Ford), **européens** (notamment Volkswagen, Mercedes, Stellantis, Volvo) et **asiatiques** (notamment Subaru, Toyota, Honda, Kia, Hyundai, Nissan, Mitsubishi, Mazda).

Les constructeurs ne produisent pas eux-mêmes toutes les composantes des véhicules : ils ont recours à des **fournisseurs de composantes matérielles** (hardware) et de **logiciels** (software). Assurer la connectivité des véhicules nécessite les services des **entreprises de télécommunications**.

Les données produites par les véhicules doivent ensuite être conservées : les constructeurs doivent donc faire affaire avec des **fournisseurs de services infonuagiques** (cloud).

Aux principales catégories d'acteurs de l'industrie mentionnés ici s'ajoutent **divers fournisseurs de service, tiers, et partenaires**. Par exemple, les services connectés incluent souvent des services d'assistance en temps réel, qui sont fournis par des centres d'appels.

1.3.2 Organismes régulateurs

L'industrie et le marché de l'automobile sont régulés par divers organismes publics qui veillent à s'assurer du respect des lois et de la protection des consommateurs et de leurs renseignements personnels.

Transports Canada est l'organisme fédéral responsable d'élaborer et de superviser les politiques et les programmes du secteur des transports au Canada. C'est lui qui dicte les règles sur les véhicules autorisés à circuler sur les routes.

Le **ministère des Transports et de la Mobilité durable du Québec** est responsable de proposer au gouvernement provincial des politiques relatives aux services, aux réseaux et aux systèmes de transport, notamment la conception et l'entretien du réseau routier.

La **Société de l'assurance automobile du Québec** a pour mandat de protéger les usagers et usagers des routes, notamment en mettant en place les règles de sécurité routière, et en assurant ces personnes pour les dommages corporels causés par les accidents de la route.

Du côté de la protection des renseignements personnels, on trouve au niveau fédéral le **Commissariat à la protection de la vie privée du Canada**, organisme responsable de protéger le droit à la vie privée et de veiller au respect des lois applicables (voir la section 1.4).

Au Québec, la **Commission d'accès à l'information (CAI)** joue un rôle analogue, comme le précise la *Loi sur la protection des renseignements personnels dans le secteur privé* (LPRPSP). Comme le Commissariat à la protection de la vie privée du Canada, elle a le mandat de recevoir des plaintes, faire des vérifications et imposer des sanctions en cas de non-respect des lois en matière de protection de la vie privée. Les deux organismes émettent aussi des recommandations, lignes directrices et avis (voir la section 1.4).

L'**Autorité des marchés financiers**, au Québec, régule différents secteurs d'activités financières, notamment celui des assurances. Or, les véhicules automatisés et connectés soulèvent de nouveaux enjeux (sécurité, responsabilité), mais aussi de nouvelles possibilités pour les assureurs (voir la section 3.7).

Le **Conseil canadien des administrateurs en transport motorisé** regroupe des représentants des différents gouvernements du Canada (provinciaux, territoriaux et fédéral). Cet organisme est responsable de la sécurité

routière et de l'administration, de la réglementation et du contrôle du transport par véhicule automobile.

Innovation, Sciences et Développement économique Canada est un organisme fédéral chargé d'encadrer et de promouvoir l'innovation pour favoriser le développement économique. Dans l'industrie automobile, son rôle est de « fixe[r] et fai[re] respecter les normes techniques et les exigences de délivrance de permis relatifs aux technologies sans fil intégrées aux véhicules et à l'infrastructure routière. Ces normes et exigences en matière de permis sont établies de manière à réduire au minimum le brouillage nuisible des services de radiocommunication et à s'assurer que les Canadiens ne sont pas surexposés aux champs de radiofréquences des technologies sans fil²⁶ ».

1.3.3 Autres acteurs

Le secteur des véhicules connectés concerne également d'autres acteurs d'importance variable.

Les constructeurs automobiles sont représentés par des **associations industrielles** comme le CMAC (Constructeurs mondiaux d'automobiles du Canada).

Les **consortiums industriels**, comme le Car Connectivity Consortium, participent au développement des technologies connectées dans le domaine de l'automobile, ainsi qu'à l'élaboration de normes de cybersécurité, de standardisation et de compatibilité.

Les **concessionnaires** jouent un rôle d'intermédiaire entre les constructeurs automobiles et les consommateurs, que ce soit au moment de la vente et de l'acceptation des conditions d'utilisation, ou encore pour les réparations et l'entretien du véhicule.

Les **administrations territoriales** – notamment les **municipalités** – font partie de l'écosystème de la connectivité des véhicules. En effet, la connexion V2I consiste à faire communiquer les véhicules avec leur environnement (feux de signalisation, etc.). Cette connectivité est en lien avec le concept de ville intelligente. La mise en place, l'entretien, la gestion et la sécurité de ces

infrastructures connectées nécessitent l'implication des administrations municipales, et peuvent engendrer des coûts pour elles²⁷.

Les **assureurs automobiles** font partie des utilisatrices et utilisateurs potentiels des données collectées. Les données de conduite leur permettent en effet d'évaluer le niveau de risque des conducteurs ou conductrices et d'ajuster l'offre de franchise en fonction de celui-ci. Les données télématiques peuvent également être utiles aux assureurs pour déterminer les circonstances et les causes d'un accident et, le cas échéant, pour déterminer la responsabilité²⁸.

Pour tirer profit des données, il faut les traiter et les analyser – ainsi, les **sociétés d'analyse de données (data analytics)** jouent désormais un rôle important dans l'industrie automobile.

Les **courtiers de données** sont des acteurs centraux dans la nouvelle économie du marché des données. Ces entreprises récoltent données et renseignements personnels à partir de diverses sources et voient à les assembler, puis à les revendre à des compagnies qui peuvent s'en servir à des fins commerciales, le tout dans le respect des lois. Cette industrie est caractérisée par sa grande opacité : il est en effet difficile de savoir précisément qui sont les courtiers de données et quelles sont leurs pratiques.

Les **gestionnaires de flotte**, c'est-à-dire les organisations publiques ou privées qui disposent d'un grand nombre de véhicules à diverses fins (livraison, transport, services), constituent une catégorie importante de la clientèle des vendeurs de véhicules connectés. En effet, la connectivité permet aux gestionnaires de flotte d'avoir accès à de nombreuses informations sur un ensemble de véhicules, sans accès physique à ces derniers, ce qui facilite grandement la gestion et le suivi des trajets (optimisation) et de l'entretien (diagnostic et réparation).

Les **entreprises de location et d'autopartage** de véhicules proposent des voitures connectées à leurs clients. Les fonctionnalités de clé virtuelle et de déverrouillage à distance (par une application) sont particulièrement utiles pour l'autopartage. La connectivité permet aussi de faire un suivi rigoureux et à distance du kilométrage effectué à des fins de facturation.

Enfin, comme pour les autres gestionnaires de flotte, le suivi de l'entretien des véhicules est facilité par ces nouvelles technologies.

On ne saurait oublier les **consommateurs individuels**, c'est-à-dire la population du Québec et du Canada dans toute sa diversité. Selon la Société de l'assurance automobile du Québec, on comptait en 2021 environ 5,7 millions de titulaires d'un permis de conduire dans la province, et 7 millions de véhicules²⁹, pour une population d'environ 8,7 millions de personnes³⁰. Tant les propriétaires automobiles que les autres conducteurs et utilisateurs sont de potentiels

bénéficiaires des avancées technologiques dans le domaine des voitures connectées, mais ils sont aussi au cœur des enjeux éthiques soulevés par la collecte et l'utilisation des données dans ce contexte.

Finalement, les **organismes de la société civile et les groupes militants** peuvent jouer un rôle lorsqu'ils se prononcent sur des enjeux et portent des revendications afférentes aux voitures connectées — qu'il s'agisse de questions environnementales, de protection de la vie privée ou des droits des consommateurs.

1.4 Les dispositions réglementaires et législatives

1.4.1 Législation

Les véhicules connectés sont des technologies complexes à la croisée de plusieurs secteurs industriels, qui sont eux-mêmes intégrés à des marchés internationaux. Les textes de loi et les règlements qui régulent leur production, leur vente et leur utilisation sont donc nombreux.

Considérant que ce rapport porte principalement sur la connectivité des véhicules, et non sur leur automatisation, la Commission énumère ici les principaux textes applicables en matière de protection de la **vie privée** d'une part et de **protection et vente de véhicules** de l'autre. Les lois encadrant l'usage de l'IA sont laissées de côté, car elles s'appliquent plutôt aux enjeux d'automatisation.

Aussi, les questions entourant le **partage des compétences** ajoutent de la complexité au sujet. En effet, plusieurs aspects du marché des véhicules connectés relèvent de la compétence de différents paliers gouvernementaux.

Au Québec

P-39.1 – Loi sur la protection des renseignements personnels dans le secteur privé (LPRPSP)

Modernisée en 2021 par la Loi 25, la LPRPSP est le cadre législatif qui établit « [...] des règles particulières à l'égard des renseignements

personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise [...] »³¹.

La LPRPSP précise dans quelles circonstances et dans quelles conditions les renseignements personnels peuvent être recueillis; elle encadre leur usage et leur conservation et attribue également aux entreprises certaines obligations de gouvernance et de gestion du risque en matière de vie privée. Elle confère à la CAI de nombreux pouvoirs d'application et de surveillance de la loi ainsi que de sanctions administratives, pécuniaires et pénales.

A-2.1 – Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

Cette loi encadre la gestion de l'information et la protection des renseignements personnels par les organismes publics. Elle contient des dispositions similaires à la LPRPSP.

C-1.1 – Loi concernant le cadre juridique des technologies de l'information (LCCJTI)

Cette loi précise les obligations des acteurs qui collectent des renseignements personnels par le biais de technologies numériques. Elle encadre notamment l'usage de systèmes biométriques et exige qu'une personne qui utilise des données biométriques pour vérifier ou confirmer une identité fasse une déclaration préalable à la

Commission et respecte certaines règles, dont l'obtention du consentement explicite des personnes concernées. La même exigence s'applique à la création d'une banque de données biométriques.

(Ccq-1991) – Code civil du Québec

Le troisième chapitre du *Code civil du Québec* contient des articles qui affirment que toute personne a droit au respect de sa vie privée (art. 35 à 41). Les atteintes à cette dernière sont notamment le fait d'« intercepter ou utiliser volontairement une communication privée », de « capter ou utiliser son image ou sa voix lorsqu'elle se trouve dans des lieux privés » et de « surveiller sa vie privée par quelque moyen que ce soit »³².

(C-12) La Charte des droits et libertés de la personne

La Charte affirme elle aussi que « toute personne a droit au respect de sa vie privée » (art. 5)³³.

A-25 – Loi sur l'assurance automobile

Cette loi encadre les pratiques d'assurance automobile (indemnités, etc.). Elle confère à l'Autorité des marchés financiers son autorité. Elle constitue également le Groupement des assureurs automobiles, qui réunit les assureurs agréés.

Au Canada

Loi sur la protection des renseignements personnels et les documents électroniques (L.C. 2000, ch. 5)

Cette loi s'applique aux organisations du secteur privé qui recueillent, utilisent ou communiquent des renseignements personnels dans le cadre de leurs activités à but lucratif. Elle prévoit que lorsqu'une organisation est assujettie à une loi provinciale jugée similaire – comme c'est le cas de la LPRPSP au Québec –, elle est alors exonérée de se conformer à la loi canadienne. Toutefois, contrairement à la LPRPSP, elle ne comprend pas de **principe d'équivalence** pour l'interterritorialité – principe selon lequel les données transférées à l'extérieur d'un pays doivent bénéficier d'un niveau de protection jugé équivalent à celui prévu par le droit canadien.

Loi sur la protection des renseignements personnels (L.R.C. (1985), ch. P-21)

Cette loi s'applique au secteur public fédéral et aux institutions gouvernementales (p. ex. Transports Canada).

Loi sur la sécurité automobile (L.C. 1993, ch. 16)

Cette loi régit la fabrication et l'importation des véhicules et équipements automobiles au Canada.

Loi sur les transports au Canada (L.C. 1996, ch. 10) et la Loi sur les transports routiers (L.R.C. (1985), ch. 29 (3^e suppl.))

Ces lois encadrent le transport routier au Canada.

À l'international

L'industrie automobile est intégrée dans une économie internationale. Si ce sont les lois fédérales et provinciales qui s'appliquent sur le territoire canadien, les constructeurs automobiles et autres acteurs de l'industrie doivent bien souvent se conformer à des cadres légaux et réglementaires d'autres juridictions.

Les entreprises qui réalisent des activités sur le territoire de l'**Union européenne** ou qui traitent des données personnelles des ressortissants de celle-ci doivent se conformer au **Règlement général sur la protection des données (RGPD)**, entré en vigueur en 2018. La Loi 25 contient plusieurs dispositions analogues à celles du RGPD, notamment le **principe d'équivalence** en cas de transfert des données hors territoire.

Aux **États-Unis**, il n'y a pas de loi fédérale concernant la protection de la vie privée : les entreprises doivent se conformer à différentes lois et réglementations selon l'État où elles exercent leurs activités. C'est l'État de la **Californie** qui encadre le plus strictement la protection de la vie privée, avec notamment la **loi californienne sur la protection de la vie privée des consommateurs** (*California Consumer Privacy Act*). Par ailleurs, de nombreuses lois d'États aux États-Unis ont trait aux **véhicules automatisés**; elles portent généralement sur l'automatisation plutôt que sur la protection de la vie privée³⁴.

Finalement, il faut noter que des **accords commerciaux** encadrent le commerce des véhicules et facilitent le transfert de données, notamment entre le Canada et les États-Unis.

1.4.2 Règlements, normes et lignes directrices

Les acteurs de l'industrie automobile doivent se conformer à différentes lignes directrices, règlements et normes, notamment :

- Le **Règlement sur la sécurité des véhicules automobiles (C.R.C., ch. 1038)** qui définit les exigences et les normes techniques auxquelles les véhicules doivent satisfaire pour être importés ou fabriqués et vendus au-delà des frontières provinciales.
- Les **Normes de sécurité des véhicules automobiles du Canada**, produites par Transports Canada.
- Le **Cadre de sécurité du Canada pour les véhicules connectés et automatisés 2.0**, produit par Transports Canada.
- On compte également des **normes industrielles ISO** (par exemple, la norme ISO/SAE 21434 :2021 Véhicules routiers — Ingénierie de la cybersécurité).
- En matière de cybersécurité, l'ONU fournit les normes **No. 155 – Cyber security and cyber security management system** ainsi que **No. 156 – Software update and software update management system**.
- L'Union européenne fournit des lignes directrices spécifiques sur la protection de la vie privée dans le cadre des véhicules connectés : **Lignes directrices 01/2020 sur le traitement des données à caractère personnel dans le contexte des véhicules connectés et des applications liées à la mobilité**.



Chapitre 2

Analyse éthique : valeurs et principes

Cette section présente les principales valeurs et principes éthiques sur lesquels la Commission s'est appuyée pour produire l'analyse éthique des enjeux soulevés par les véhicules connectés. Ces valeurs et principes sont interreliés et une analyse éthique doit les intégrer de façon holistique.

2.1 La protection de la vie privée

On considère généralement la vie privée comme un **droit fondamental**, comme en atteste son inscription dans la Charte des droits et libertés (voir la section 1.4.1).

Chacun a le **droit au respect de sa vie privée**, c'est-à-dire le droit de garder certains aspects de sa vie à l'abri du regard et de la connaissance ou de l'ingérence d'autres personnes³⁵. Pour certains penseurs, la vie privée a une **valeur intrinsèque** : elle est essentielle à une vie digne, au même titre que la liberté, par exemple. Pour d'autres, la vie privée a plutôt une **valeur instrumentale** : elle permet la jouissance d'autres droits ou biens, comme l'autonomie, la liberté, la sécurité, les relations sociales, ou même la démocratie.

Les conceptions classiques font reposer la **vie privée** sur la distinction entre sphère publique et sphère privée. Ce qu'une personne peut choisir de garder pour elle, c'est ce qui relève de la *sphère privée* ; au contraire, certaines informations relèvent de la *sphère publique* et peuvent être diffusées et circuler dans la société, sans causer un préjudice à la personne. Toutefois, les développements technologiques des dernières décennies ont montré une limite de la dichotomie public/privé³⁶. En effet, certains usages de données produites dans un contexte public semblent soulever des enjeux de vie privée : pensons aux images filmées dans la rue par des véhicules connectés.

Face à ces nouveaux enjeux, il importe donc de se tourner vers des conceptions de la vie privée plus souples, qui ne reposent pas principalement sur la dichotomie public/privé, mais qui portent attention au **contexte** dans lequel les informations sont créées et circulent. Il faut aussi considérer les **attentes raisonnables** des personnes dans différents contextes, attentes qui découlent des normes légales et sociétales³⁷. Le droit canadien utilise d'ailleurs le critère

d'attente raisonnable pour déterminer s'il y a une atteinte à la vie privée des citoyennes et citoyens. La jurisprudence, et en particulier de nombreux jugements de la Cour Suprême du Canada, précise ce qui constitue ou non une attente raisonnable en matière de vie privée.

Les normes en matière de vie privée varient selon les contextes, les époques et les cultures et peuvent aussi faire l'objet de transformation, notamment avec le développement de nouvelles technologies. Par exemple, l'utilisation d'un véhicule personnel a longtemps été un contexte très privé : les personnes en appréciaient le caractère privé, quasiment intime. La connectivité vient modifier cet état de fait, puisqu'une quantité importante de données sur l'utilisation d'un véhicule est maintenant produite et mise en circulation. Quoiqu'il puisse y avoir des avantages à ce changement, on peut toutefois identifier un **risque d'atteinte à la vie privée** puisque les normes de flux de l'information sont perturbées. Il importe de réévaluer ces normes en cas de décalage entre les attentes des individus et la circulation réelle de l'information.

Les développements technologiques appellent également une souplesse dans la définition des **renseignements personnels**. Les tribunaux canadiens font preuve d'une telle approche en considérant comme renseignement personnel tout renseignement « concernant un individu identifiable lorsqu'il y a de fortes possibilités que l'individu puisse être identifié par l'utilisation de ces renseignements, seuls ou en combinaison avec d'autres sources accessibles »³⁸.

Le droit à la **vie privée** concerne donc les **informations** à propos d'une personne (comprises au sens large) et la façon dont elles peuvent être **créées, collectées et partagées**. Plusieurs mesures peuvent contribuer à protéger la vie privée des individus.

2.2 L'autodétermination informationnelle

L'**autodétermination informationnelle** consiste à mettre de l'avant l'**autonomie** des personnes en matière de vie privée. Dans une société libérale, on devrait viser à ce que chacun soit le plus autonome possible, dans la limite du respect d'autrui. La vie privée est un des champs d'application de cette autonomie.

Selon le principe d'**autodétermination informationnelle**, chacun devrait pouvoir contrôler autant que possible l'accès aux données qui le concernent. Ce principe motive la logique du **consentement** à la collecte et au partage des données, ainsi que la reconnaissance du **droit d'accès**.

DANS LE DROIT QUÉBÉCOIS

- Le consentement** Toute entreprise doit s'assurer d'obtenir le consentement d'une personne avant de recueillir et d'utiliser ses renseignements personnels. Pour être valide, la demande de consentement doit être **compréhensible et présentée de manière distincte** et le consentement doit être **manifeste, libre, éclairé, spécifique, temporaire, et granulaire**³⁹.
- Le droit d'accès** Chaque personne dispose également du droit fondamental d'obtenir la communication des renseignements personnels que détient une organisation publique ou privée à son sujet. Ce droit inclut la possibilité de demander la **rectification** des données inexactes, incomplètes ou équivoques. L'accès doit être offert dans un format compréhensible, quels que soient le support et l'interface utilisés pour la collecte, et dans des délais raisonnables.

2.3 L'autodétermination collective

Le principe d'autodétermination peut être appliqué à une échelle **collective** plutôt qu'individuelle. Ainsi, l'**autodétermination collective** correspond à la capacité des collectivités et des institutions publiques de prendre des décisions sur les enjeux collectifs, et de les implanter en pratique. Il s'agit d'un principe **démocratique**, puisqu'il vise à garantir l'expression et le respect de la volonté collective des citoyennes et citoyens. L'autodétermination collective peut être abordée selon deux approches : une approche par réglementation et une approche démocratique.

Approche par réglementation

Une façon de réaliser l'autodétermination collective consiste à s'en remettre aux institutions législatives pour protéger la vie privée de la population. Ces institutions, représentant la population, **légifèrent** et balisent la collecte, l'usage et le partage des données par les entreprises.

L'approche par réglementation dans le cas de l'autodétermination collective diffère de celle de l'autodétermination informationnelle en cela qu'elle considère que certaines pratiques ne sont pas acceptables, et ce, indépendamment

du consentement des personnes. Par exemple, selon le droit québécois, les entreprises ne doivent récolter des renseignements personnels que s'ils sont nécessaires à la poursuite de fins légitimes, et ne peuvent vendre les renseignements personnels, quand bien même les personnes concernées y consentiraient. En effet, la commercialisation des renseignements personnels est considérée comme incompatible

avec la reconnaissance de la dignité des personnes : le consentement ne saurait donc légitimer l'illégitime.

Le cadre législatif en vigueur au Québec protège la vie privée des personnes en promouvant une approche **minimaliste** en matière de collecte de renseignements personnels. Cette approche minimaliste repose notamment sur les principes de **nécessité** et de **proportionnalité** des fins et des moyens.

DANS LE DROIT QUÉBÉCOIS

Principe de nécessité

Les entreprises ne peuvent collecter que des renseignements personnels qui sont **nécessaires** pour la poursuite des fins visées, lesquelles doivent être **importantes** et **réelles**.

Principe de proportionnalité

Les **risques** associés à la collecte des renseignements personnels doivent être **proportionnels** à l'importance des fins visées.

Légiférer sur la protection de la vie privée permet **d'homogénéiser** les pratiques des entreprises, de rendre **ces dernières imputables** (voir la section 2.7), et donne l'occasion à l'État de se doter de **moyens** de faire respecter la vie privée des personnes.

Approche démocratique

Selon le principe **d'autodétermination collective**, les normes de protection de la vie privée doivent refléter les valeurs et les préférences de la communauté. Mais comment bien identifier ces dernières? Une piste de réponse consiste à intégrer des pratiques de **démocratie participative**, à mener des **consultations publiques**, ou toute autre mesure de participation citoyenne⁴⁰.

Cette approche permet de dépasser une perspective purement réglementaire en montrant que la protection de la vie privée soulève de vraies questions pour une société démocratique. Faut-il réaffirmer les normes de vie privée s'appliquant aux véhicules

traditionnels, ou bien est-il préférable d'adopter des normes contextuelles plus ouvertes, permettant un plus grand partage des données? **Quelles devraient être les normes encadrant les flux de l'information dans le contexte des véhicules connectés?** Il s'agit là de questions éthiques qui devraient faire l'objet de **délibérations collectives**⁴¹.

Cette approche fait face aux défis classiques de la démocratie participative : il faut adéquatement identifier les **acteurs** participant aux délibérations (les entreprises doivent-elles en faire partie?), s'assurer que la population est adéquatement **représentée** dans sa diversité, que les procédures permettent une participation **équitable**, et que les participants sont adéquatement **renseignés** sur les enjeux sur lesquels ils sont appelés à se prononcer.

2.4 La souveraineté numérique et la souveraineté des données

La souveraineté réfère au pouvoir d'un État d'exercer une autorité exclusive sur son territoire. Dans une société démocratique, la souveraineté est une forme d'autodétermination collective, puisque l'État représente sa population.

Le principe de souveraineté s'applique aux technologies numériques : on parle alors de **souveraineté numérique**. Lorsque l'État fait affaire avec des compagnies étrangères (p. ex. les GAFAM⁴²) pour le fonctionnement des institutions publiques, il risque de se placer dans une situation de dépendance à leur égard, ce qui menace sa souveraineté.

Des enjeux de souveraineté numérique peuvent également émerger dans le secteur privé. Le caractère international de l'industrie automobile nuit à la capacité de l'État à faire appliquer ses lois et à réguler les pratiques des acteurs de cette industrie. C'est particulièrement le cas lorsque les entreprises collectent des données qui sont ensuite transférées et traitées à l'extérieur du territoire. Si ces données sont sensibles, ou qu'elles incluent des renseignements personnels sur les citoyennes et citoyens, cela peut également accroître le risque d'atteinte à la *sécurité nationale*, notamment le risque d'espionnage. C'est particulièrement le cas dans un contexte de relations internationales tendues et conflictuelles.

2.5 Le bien commun

Le bien commun est un principe phare qui doit guider l'action des institutions publiques. Bien qu'il existe plusieurs définitions de cette notion, nous l'approchons sous l'angle de la maximisation des bénéfices collectifs. Ainsi, respecter et poursuivre le bien commun, c'est s'assurer que les décisions génèrent non seulement une plus grande quantité de bénéfices que d'inconvénients pour l'ensemble de la collectivité, mais tentent également de maximiser ces bénéfices. Par exemple, toutes choses égales par ailleurs, il est conforme au bien commun d'améliorer la **sécurité** routière. En revanche, les failles de sécurité, qui risquent d'occasionner des fuites importantes de données sensibles, compromettent le bien commun.

Une façon d'évaluer si l'utilisation d'une technologie est conforme à la poursuite du bien commun pourrait être d'analyser les biens qu'elle apporte (**bienfaisance**) et s'assurer que les **inconvénients**, s'il y en a, sont minimes (**non-malfaisance**). Un tel calcul devrait reposer sur des **données probantes**. Il devrait également respecter un principe d'**équité** : il ne serait pas acceptable que tous les bénéfices ne reviennent qu'à une partie de la population, et que la majorité des inconvénients soient subis par un autre groupe.

Enfin, dans une société pluraliste, les conceptions du bien commun sont évolutives et peuvent varier selon les individus et les groupes ou être sujettes à délibération.

2.6 La protection de l'environnement

La protection de l'environnement demande de prendre des mesures en vue d'éliminer ou de restreindre significativement les conséquences des activités humaines sur l'environnement naturel, et de s'abstenir de poser des actions nuisant à celui-ci. Les véhicules connectés se trouvent à la jonction de deux industries polluantes, tant à la production qu'à l'usage :

celles de l'automobile et du numérique. Conformément aux principes de **bien commun**, de **bienfaisance** et de **non-malfaisance**, il est important de garder en tête le **coût environnemental de ces technologies et de leurs usages**. Certaines fonctionnalités pourraient être bénéfiques, par exemple si elles fluidifient le trafic routier ou permettent

d'adopter des itinéraires qui nécessitent moins de carburant. Il faut faire preuve de **prudence** et de **rigueur**, s'appuyer sur des **données scientifiques**, et considérer l'impact environnemental total d'une technologie, avant de conclure qu'elle est bénéfique pour

l'environnement. Pris ensemble, ces impératifs de prudence, de rigueur, auxquels on peut ajouter également la **modération** et le **discernement**, renvoient à l'impératif de la **sobriété numérique**⁴³.

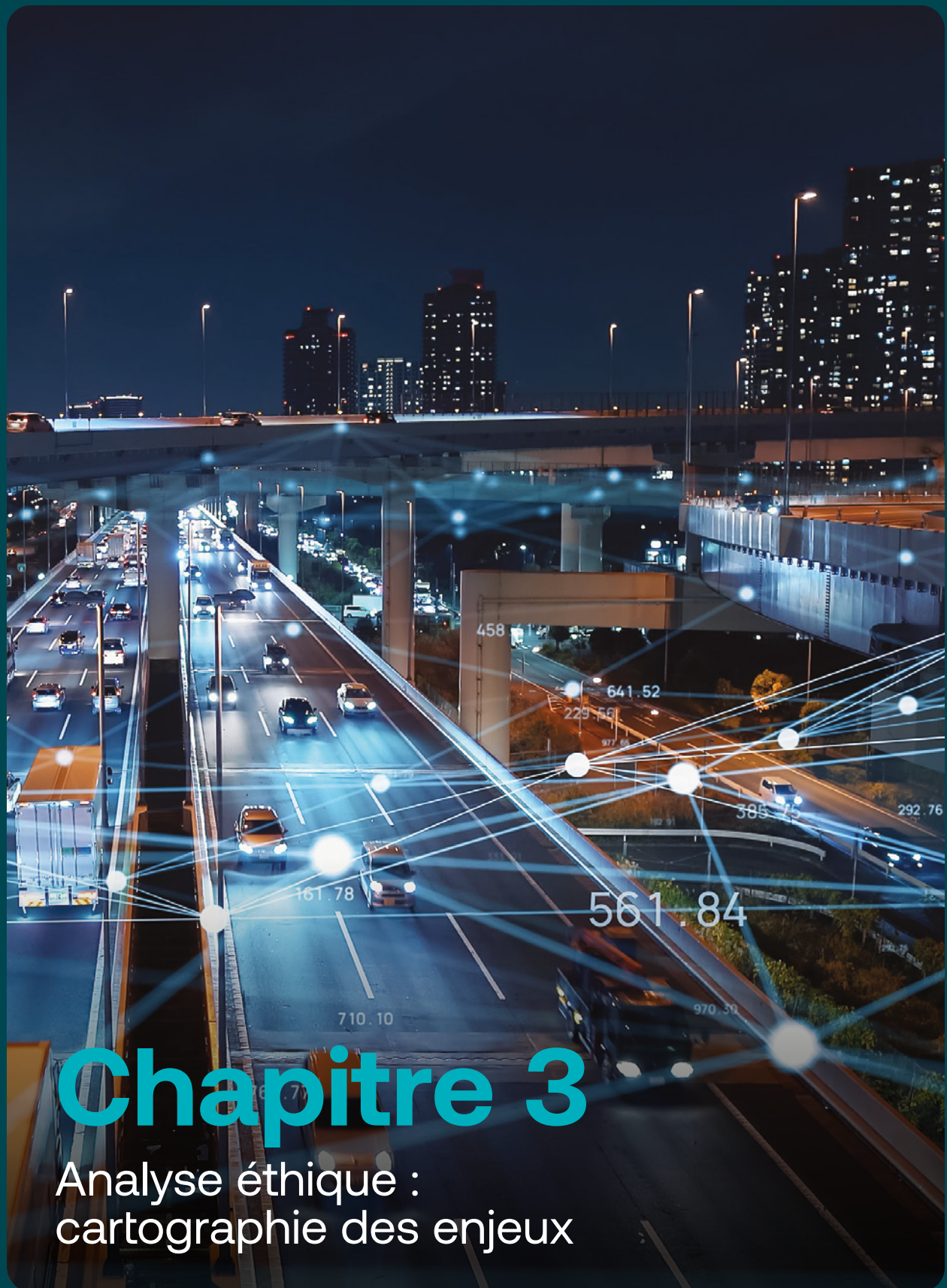
2.7 La responsabilité

La **responsabilité** est l'obligation morale pour une personne, pour une institution ou pour une communauté de répondre de ses actes. Elle peut être comprise dans un sens **rétrospectif** (nous pouvons être tenus responsables d'un acte passé) ou dans un sens **prospectif** (nous avons des devoirs moraux impliqués par une charge ou une position). Sur le plan juridique, la responsabilité se traduit généralement par un principe **d'imputabilité**, qui implique que l'on puisse être jugé et éventuellement sanctionné pour les actes dont nous sommes tenus responsables. Les acteurs doivent mettre en place des pratiques de **reddition de comptes** et faire preuve de **transparence** dans leurs actions et décisions afin de mériter et de conserver la **confiance** du public.

Les acteurs privés doivent respecter les obligations qui leur sont imposées par l'ensemble des dispositions législatives et réglementaires.

Toutefois, dans une industrie aussi complexe que celle de l'automobile, il n'est pas toujours facile de déterminer quel(s) acteur(s) sont ou devraient être responsables. Par exemple, si un tiers fournisseur utilise ou partage à mauvais escient les données personnelles des utilisatrices et utilisateurs qui ont été récoltées par le constructeur automobile, dans quelle mesure ce dernier doit-il être tenu responsable ?

Les différents acteurs publics et gouvernementaux (décideurs, législateurs, administrateurs) sont responsables de mettre en place des lois, règlements, mesures et politiques qui correspondent aux attentes et aux besoins de la société et qui favorisent la poursuite du bien commun et le respect des valeurs démocratiques.



Chapitre 3

Analyse éthique :
cartographie des enjeux

Cette section présente les principaux enjeux éthiques identifiés par la Commission. Ces différents enjeux comportent bien sûr une dimension éthique, mais également juridique, économique, politique, etc. Nous nous concentrons principalement sur l'analyse éthique, sur la façon dont les valeurs et principes énoncés dans la section 2 sont mis en jeu, et sur les risques posés pour les individus ou la collectivité.

3.1 Les risques d'accroissement de la surveillance et d'érosion de la vie privée

Les développements technologiques rapides de l'Internet des objets, notamment des voitures connectées, viennent bousculer les normes et les pratiques sociétales en matière de vie privée. Il y a quelques décennies seulement, il aurait été jugé plus problématique qu'aujourd'hui d'être filmé dans sa cour par la voiture de son voisin, ou que l'historique de tous nos déplacements soit accessible au gouvernement ou à des acteurs privés. Pourtant, ces possibilités techniques font désormais partie intégrante de nos vies. Cette érosion de la vie privée conduit donc à une **banalisation de la surveillance**. De moins en moins de dimensions de la vie quotidienne sont réellement privées, à l'abri de l'accès, du regard et de la connaissance d'autrui. Plusieurs dispositifs de surveillance sont également employés dans des espaces publics, enregistrant ainsi des informations sur les passants (qui n'en sont parfois même pas conscients).

Qu'a à perdre une société où la vie quotidienne des citoyennes et citoyens est ainsi documentée et surveillée par des moyens technologiques ? Un réflexe répandu est de penser que, si l'on n'a rien à cacher, on n'a rien à craindre. Ce raisonnement a été nommé par des chercheurs le sophisme « rien à cacher » (*nothing to hide fallacy*) ou « l'erreur de la surveillance » (*surveillance delusion*)⁴⁴. L'erreur de la surveillance doit être comprise comme une mauvaise appréciation ou une sous-estimation des risques et coûts liés à l'érosion de la vie privée, et tient notamment au fait que ceux-ci sont difficiles à quantifier, et sont souvent diffus dans le temps.

Alors que certaines données semblent isolément anodines, elles peuvent être compilées et agrégées pour finalement révéler des

informations sensibles sur le mode de vie d'un individu. Dans son supplément d'avis sur l'Internet des objets, la Commission présentait un cas de figure où l'on était en mesure de « 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) ⁴⁵ ». Les personnes ne se doutent pas toujours de ce que peuvent révéler les données de leur voiture, ce qui contribue au phénomène de *l'erreur de la surveillance*.

Enfin, le fait de n'avoir rien à cacher à un moment précis ne signifie pas que ce sera toujours le cas — certaines informations peuvent devenir sensibles avec le temps. Par exemple, des personnes dont les historiques de géolocalisation révéleraient qu'elles ont participé à une manifestation ou à un rassemblement politique, ou qu'elles se sont rendues à une clinique d'avortement, pourraient penser sur le moment que ces informations sont anodines, mais certains événements imprévus, voire des changements de régime politique, pourraient faire changer la donne. Ainsi, les coûts de l'érosion de la vie privée pourraient apparaître de façon particulièrement flagrante dans l'éventualité de l'avènement d'un conflit géopolitique. Dans un scénario moins radical, une personne pourrait être indifférente vis-à-vis du fait que ses données sont collectées par un constructeur automobile ; cela ne signifie pas qu'elle accepterait que ses données soient soudainement accessibles à ses proches ou son employeur. De tels scénarios sont pourtant plausibles, notamment en cas de fuite massive de données (voir la section 3.4) ou de harcèlement obsessionnel (voir la section 3.2).

On peut voir l'érosion de la vie privée comme le résultat d'un compromis avec d'autres valeurs, telle la sécurité. Ainsi, il peut parfois s'avérer souhaitable de sacrifier la protection de la vie privée afin d'augmenter la sécurité, en prévenant les accidents de la route ou les crimes, par exemple. Il faut toutefois éviter de trancher trop vite en faveur de gains de sécurité au détriment de la vie privée. Il peut être difficile de bien comprendre les coûts et bénéfices réels des

décisions. Des concessions du côté de la vie privée peuvent mener ultimement à des risques accrus pour la sécurité (cybersécurité et fraude, par exemple). De plus, il importe de s'assurer que ces sacrifices en matière de vie privée s'accompagnent d'un réel gain de sécurité, et les données empiriques à cet effet ne sont pas toujours disponibles. Ce contexte d'incertitude complexifie la recherche du compromis entre vie privée et sécurité.

3.2 La vie privée en famille et les violences intrafamiliales

L'univers des véhicules connectés vient bousculer les paramètres de la vie privée entre les personnes et soulève des questions sur les limites de la surveillance acceptable en famille. Les services connectés proposés par les constructeurs, mais aussi des applications tierces comme Dimo ou Life360, offrent des fonctionnalités de gestion de flotte pour les particuliers. Depuis une application sur son cellulaire, le propriétaire des véhicules (ou, parfois, tous les membres de la famille) peut consulter les lieux où se trouvent les voitures familiales, voire la vitesse et la direction de leur déplacement. Le propriétaire peut aussi recevoir une notification lorsque le véhicule sort d'un paramètre prédéfini, ou lorsqu'il est verrouillé ou déverrouillé par les utilisatrices et utilisateurs secondaires des véhicules. Des rapports de conduite, incluant par exemple les dépassements des limites de vitesse, les freinages brusques ou encore la consultation du téléphone au volant, peuvent être partagés avec les membres de la famille.

Les parents utilisent ces fonctionnalités pour surveiller et contrôler les déplacements de leurs enfants adolescents, ainsi que leur façon de conduire. Cela s'inscrit dans une tendance plus large, celle de la surveillance numérique des enfants (pensons à l'utilisation de logiciels de contrôle parental sur les appareils électroniques ou à l'utilisation des tuiles de géolocalisation, etc.)⁴⁶. Cette intrusion dans la vie privée des membres de la famille est-elle toujours réellement justifiée ?

Premièrement, on peut se demander si la balance entre sécurité et vie privée ne sacrifie pas trop facilement cette dernière. Par exemple,

l'application *Life360* permet de consulter non seulement la localisation en temps réel, mais aussi l'historique complet des déplacements allant des 2 derniers aux 30 derniers jours, selon l'abonnement. Si on peut comprendre pourquoi il peut être rassurant d'avoir accès à la géolocalisation en temps réel de ses enfants, il est plus difficile de comprendre en quoi avoir accès à leur historique de déplacement sur une période prolongée augmente leur sécurité. Deuxièmement, quoique le partage de la localisation soit associé à un plus grand sentiment de sécurité, il faut être prudent et ne pas tenir pour acquis qu'un *sentiment de sécurité* correspond concrètement à une plus grande sécurité⁴⁷. Troisièmement, on peut se questionner sur les potentiels effets négatifs de telles habitudes de surveillance familiale. Des experts craignent, par exemple, que les jeunes ne développent pas leur autonomie et surtout que la relation parent-enfant soit détériorée par l'érosion de la confiance⁴⁸. Dans l'ensemble, il semble qu'il manque de données probantes sur les avantages et les bénéfices promis par la connectivité, mais aussi sur ses inconvénients et ses risques⁴⁹. Il convient donc de faire preuve de prudence et de mener davantage d'études empiriques afin d'être en mesure d'évaluer les gains concrets en matière de sécurité.

Si on peut justifier certaines mesures modérées de surveillance en faisant appel à la sécurité des adolescents et à l'autorité parentale, qu'en est-il dans les relations entre adultes ? Il devient de plus en plus fréquent⁵⁰, notamment chez les jeunes, de partager sa localisation en tout temps avec ses proches — partenaires, membres de la famille ou amis. L'usage d'applications comme *Life360* ou *Dimo* s'inscrit dans une certaine

modification des normes de vie privée dans la société. Si, comme pour les enfants, cela peut amener un sentiment de sécurité, il n'est pas clair que ce soit nécessairement le cas (une étude montre d'ailleurs qu'il est fréquent que les personnes regrettent d'avoir partagé leur localisation⁵¹). Plus encore, ces applications – et les services connectés du constructeur – peuvent être utilisées à mauvais escient par des individus qui ont des comportements contrôlants et violents. Or, il n'est pas facile *a priori* de distinguer un usage « sain », qui serait basé sur la confiance et viserait la sécurité, d'un usage abusif et contrôlant. En fait, plus les pratiques de partage de localisation et de surveillance numérique sont communes et banalisées, plus il est difficile pour les potentielles victimes de les refuser. Cette normalisation crée donc un terreau fertile pour les violences intrafamiliales.

Les auteurs de violences intrafamiliales utilisent de plus en plus de moyens technologiques pour contrôler leurs victimes (logiciels espions sur le cellulaire, caméras cachées, etc.)⁵². Les voitures connectées sont un moyen particulièrement efficace, dangereux et intrusif pour un individu de contrôler ses proches⁵³. Il s'avère par ailleurs difficile pour les victimes de cette surveillance de se rendre compte qu'elles sont surveillées. Les associations luttant contre les violences intrafamiliales soulignent également la grande difficulté d'échapper à cette surveillance technologique. Soulignons que la localisation des maisons d'hébergement doit rester confidentielle pour assurer la sécurité de leurs occupantes et employées, mais cette confidentialité est mise à mal par les technologies de géolocalisation, y compris les voitures — ce qui peut amener certaines personnes à devoir renoncer à leur véhicule, qui au-delà d'un moyen de transport constitue un précieux outil d'indépendance. En outre, échapper à cette traque peut s'avérer vraiment difficile. L'organisme américain Privacy4Cars offre du soutien pour lutter contre le harcèlement obsessionnel (*stalking*) avec une attention particulière pour les victimes d'abus : les étapes à suivre sont nombreuses et complexes⁵⁴. En outre, il arrive que le véhicule et l'abonnement aux services connectés soient légalement au nom du conjoint : dans ce cas, il peut être très difficile, voire impossible, de retirer l'accès de celui-ci aux données télématiques du véhicule.

Au Canada, le Projet de loi C-16, qui criminalise le *contrôle coercitif*, inclut dans la définition du contrôle coercitif le fait de « contrôler, tenter de contrôler ou surveiller les faits et gestes, déplacements ou interactions sociales du partenaire intime, notamment par tout moyen de télécommunication », lorsque cet acte est commis avec l'intention ou sans se soucier de faire croire au partenaire intime que sa sécurité est en danger. Cette définition pourrait donc inclure la surveillance du véhicule du partenaire intime. Toutefois, ce projet de loi adopté en juin 2026 suscite encore des questions : son application devra reposer sur une analyse contextuelle et une interprétation de la situation spécifique du couple. De plus, la criminalisation ne peut pas être la seule solution : des mesures facilitant la prévention des violences et la protection des victimes doivent être mises en place.

Par exemple, aux États-Unis, la *Safe Connection Act* est une loi fédérale qui permet à une victime de violences conjugales de séparer sa ligne téléphonique du compte du conjoint ayant commis des gestes violents. Sur réception d'un document attestant de la violence subie (il peut s'agir d'une copie de la plainte à la police, d'un document fourni par des services médicaux, un centre d'aide aux victimes, une cour de justice, etc.), les fournisseurs de services téléphoniques séparent la ligne de la victime du compte principal, sans l'autorisation de son titulaire et en protégeant les informations personnelles de la victime. Les États de New York et de Californie ont instauré en 2025 des extensions de cette loi qui incluent les services connectés du véhicule⁵⁵.

Enfin, notons que, selon la plupart des politiques de confidentialité, les propriétaires automobiles ont l'obligation d'expliquer aux conductrices et conducteurs occasionnels le contenu de ces politiques et ce qui advient de leurs données. Dans les faits, ces personnes ne sont pas toujours au courant que le propriétaire a accès à des informations précises sur leurs déplacements — que ce soit par malice ou, probablement plus fréquemment, par négligence.

3.3 La surveillance au travail

La connectivité automobile permet aux employeurs et gestionnaires de flotte d'exercer une surveillance accrue sur l'activité des véhicules, à bon ou à mauvais escient. Les objectifs sont l'amélioration des opérations et le maintien de la sécurité. Alors que le nombre d'accidents de la route impliquant des véhicules lourds augmente, certaines entreprises du secteur se tournent vers l'utilisation de dispositifs technologiques qui identifient des comportements à risque (accélération ou freinage brusque, changements de voie rapide, etc.) et envoient un rapport à l'employeur⁵⁶. Certains peuvent être tentés d'avoir recours à des caméras internes au véhicule pour surveiller ces comportements. D'autres, qui ont accès à la localisation en temps réel des véhicules de la flotte, pourraient y voir une occasion de surveiller les déplacements de leur personnel.

Un avis de la Commission sur la gestion algorithmique de la main-d'œuvre, publié en 2023, traite d'enjeux qui s'appliquent aussi à l'utilisation de véhicules connectés au travail, en particulier l'intensification de la surveillance⁵⁷. Ils constituent, en effet, un autre moyen pour les gestionnaires d'étendre le suivi et le contrôle des activités professionnelles.

Les décisions récentes des tribunaux tendent à confirmer la légalité des pratiques de surveillance du personnel, dans la mesure où elles ne sont pas continues et constantes, et qu'elles soient justifiées par des motifs nécessaires, sérieux et raisonnables⁵⁸.

Cela confirme l'analyse de l'avis selon laquelle on observe « une tendance des juges administratifs et des tribunaux à être beaucoup

plus permissifs en matière de surveillance, en se basant sur des hypothèses quant au degré d'intrusion "raisonnable" qui sont plus indulgentes que l'opinion publique dominante »⁵⁹.

Les personnes qui estiment que leur employeur adopte des pratiques abusives peuvent s'adresser aux tribunaux. Toutefois, ce ne sont pas toutes les catégories de personnel qui ont les moyens de contester la légalité des pratiques de surveillance de leur employeur et de défendre leur droit à la vie privée. On peut notamment penser aux personnes dont les conditions de travail sont précaires, ou qui n'ont pas l'appui d'un syndicat.

Plusieurs des recommandations formulées par la Commission dans l'avis sur la gestion algorithmique sont pertinentes à l'analyse des enjeux liés à la surveillance au travail rendue possible par les véhicules connectés :

- **Recommandation 7 :** La Commission recommande que le gouvernement du Québec oblige les employeurs à divulguer le recours à la surveillance électronique au travail, en précisant les tâches qui feront l'objet d'un suivi, la méthode du suivi, les types de données collectées, l'éventuel traitement algorithmique opéré à partir de ces données et la manière dont seront utilisés ces résultats dans la prise de décision.
- **Recommandation 8 :** La Commission recommande que le gouvernement du Québec précise les finalités pour lesquelles la collecte, l'utilisation ou la communication de données devraient être interdites dans les milieux de travail.

3.4 Le piratage et le vol des données personnelles

Les données sont une ressource précieuse pour les acteurs malveillants : elles peuvent être vendues et partagées à des courtiers de données peu scrupuleux, et finissent souvent par circuler sur l'Internet caché (*dark web*). Le cas échéant, elles peuvent servir à des fins de profilage, mais aussi de fraude et d'usurpation d'identité. Or les véhicules connectés sont une

cible de choix pour les cyberpirates. Les stratégies employées par les pirates sont diverses et s'attaquent à des failles de sécurité variées. Tous les canaux de connectivité, à toutes les étapes, peuvent être vulnérables à des cyberattaques⁶⁰.

Les cyberpirates peuvent poursuivre différentes fins : contrôle du véhicule à distance, vol de voiture, installation de rançongiciel, etc. Dans le cadre de notre analyse, nous nous concentrons sur les attaques envers les *données* — plutôt que, par exemple, les attaques visant le contrôle ou le vol du véhicule. Or, en 2024, selon le rapport *Mind the Cybergap : Automotive & Smart Mobility Global Cybersecurity Report 2025* de la firme Upstream, 60 % des incidents de cybersécurité automobile étaient de l'ordre du piratage de données et d'atteintes à la vie privée⁶¹.

Certaines failles sont identifiées par des pirates éthiques (*white-hat hackers*), c'est-à-dire des personnes qui utilisent des techniques de piratage sans intention malveillante, justement pour tester la cybersécurité des systèmes. Par exemple, le pirate éthique Sam Curry a mis au jour, en novembre 2024, une faille de sécurité importante dans le système de Subaru Starlink. En utilisant les informations personnelles de sa mère, qui possédait une automobile Subaru, et des informations accessibles en ligne, comme des adresses courriel d'employés de Subaru, il a réussi à pénétrer dans le portail administrateur de Starlink. Cela lui a permis d'accéder à l'historique complet de géolocalisation du véhicule de sa mère au cours de la dernière année, de s'ajouter comme utilisateur d'un véhicule dont il connaissait le numéro d'immatriculation et de déverrouiller à distance ce véhicule — sans que son propriétaire légitime soit averti⁶². Si cette faille de sécurité avait été exploitée par des acteurs malveillants, cela aurait posé des risques importants pour la sécurité, la vie privée et la propriété privée des clients de Subaru.

Jusqu'à présent, plusieurs incidents de grande envergure ont eu lieu dans l'industrie automobile. Par exemple, une fuite massive de données stockées sur des serveurs Amazon (AWS) en 2024 a exposé les données d'environ 800 000 véhicules électriques du groupe Volkswagen. Ces données, qui incluaient des données de géolocalisation, ont été publiquement accessibles pendant plusieurs mois. Il importe donc de mettre en place des mesures de sécurité adéquates, et ce, tout au long du cycle de stockage et de transfert des données.

Selon le rapport *Mind the Cybergap* de la firme Upstream, en 2024, 65 % des attaques envers les systèmes connectés étaient menées par des acteurs malveillants (*black hat hackers*)⁶³. Toujours en 2024, selon le même rapport, la plupart des attaques (92 %) sont effectuées à distance plutôt que par accès physique. Les attaques à distance exploitent les failles de connectivité courte distance (à proximité du véhicule) ou longue distance (attaque sur l'API, ou *Application Programming Interface*).

Chaque étape de transfert et de stockage des données constitue une vulnérabilité additionnelle face aux menaces de pirates et d'acteurs malveillants. Les données récoltées par les compagnies automobiles sont souvent partagées à des tiers qui sont difficiles à identifier. Dans quelles conditions sont-elles transmises et conservées? Les serveurs sont-ils adéquatement sécurisés? Il importe que les meilleures normes de cybersécurité soient appliquées tout au long du cycle de vie des données, et que le partage ainsi que la multiplication de lieux de stockage des données soient limités au nécessaire. Se pose également un problème de **responsabilité** : si un tiers échoue à protéger adéquatement les données qui lui ont été partagées, malgré le contrat signé avec le constructeur automobile, quelle est la part de responsabilité de ce dernier en cas d'incident?

Dans bien des cas, il est difficile, voire impossible, pour une personne de se rendre compte qu'elle a été, ou est présentement victime d'une cyberattaque qui cible ses données personnelles. Bien souvent, les victimes ne s'en rendent compte que lorsque les autorités ou les services connectés les en informent, ou encore, malheureusement, lorsqu'elles en subissent les conséquences (fraude, vol d'identité) — ce qui peut arriver des mois ou des années plus tard.

La vulnérabilité des systèmes connectés du secteur automobile et de l'ensemble de leurs partenaires pose donc un danger pour les individus et **l'intérêt public**. Il est impératif de mettre en place et de faire respecter des normes élevées en matière de cybersécurité, en prenant en compte que les compétences des pirates avancent au même rythme que l'innovation technologique.

3.5 Les enjeux liés à l'autopartage et à la location de courte durée

La connectivité des véhicules est une des pierres angulaires des **systèmes d'autopartage** : elle permet, notamment, à un utilisateur ponctuel de déverrouiller une voiture réservée à l'aide d'une application mobile. Les flottes des compagnies de location de courte durée « traditionnelle » comprennent également un grand nombre de véhicules connectés. La dépendance de ce secteur commercial à l'industrie de la connectivité appelle donc à mener une réflexion propre aux enjeux qui en découlent.

Le cas des véhicules partagés et loués exacerbe un problème déjà majeur dans l'industrie de la voiture connectée : la **multitude des acteurs**, qui augmente les instances de collecte de données et les risques qui y sont associés, et qui rend difficile **l'attribution de la responsabilité** en cas de problème.

Les entreprises d'autopartage et de location de véhicules ont recours à leurs propres systèmes de télématique, installés sur le véhicule. Elles collectent et utilisent les informations personnelles de leurs clients et sont soumises aux mêmes lois sur la protection des renseignements personnels que les constructeurs automobiles (et que tous les acteurs privés). L'examen des politiques de confidentialité de compagnies d'autopartage ou de location de voitures soulève certaines interrogations.

La politique de confidentialité d'un des services d'autopartage principaux au Québec est relativement précise en ce qui concerne la collecte et l'utilisation des différentes données. Elle précise, par exemple, que les données de géolocalisation ne sont pas collectées en temps réel pendant un trajet, à moins que l'utilisateur en fasse la demande (par exemple, s'il a oublié l'emplacement du stationnement) ou que le véhicule soit volé. Elles sont recueillies à la fin de chaque trajet, afin de permettre à la compagnie de localiser le véhicule entre les réservations. Or d'autres politiques de compagnies offrant des services similaires témoignent d'une approche moins minimaliste. Elles indiquent générer, collecter et utiliser les données de localisation. Pourtant, les fins poursuivies sont les mêmes (assistance routière et services d'urgence ;

repérage d'un véhicule perdu ou volé). Est-il vraiment nécessaire de récolter les données de localisation pendant la location ?

L'historique de localisation d'un véhicule locatif est-il moins révélateur ou moins sensible que celui d'un véhicule particulier ? Il semble a priori que ce soit le cas, puisqu'il ne révèle pas tous les déplacements d'un utilisateur, mais plutôt les différents déplacements de multiples utilisatrices et utilisateurs. Mais il s'agit tout de même d'information sensible. De plus, avant l'avènement des voitures connectées, il aurait été jugé invasif que le locateur demande à connaître tous les trajets effectués avec le véhicule. Aussi, ces données peuvent être analysées pour produire des informations sur les habitudes de la population, même si les données produites ne sont plus associées à des individus (voir la section 3.12).

Même si les locateurs installent leurs propres systèmes de télématique sur leurs véhicules et récoltent des données à leurs fins, cela ne veut pas dire pour autant qu'il n'y a pas de transmission au constructeur. Les utilisatrices et utilisateurs peuvent connecter leurs cellulaires au système d'infodivertissement (pour faire jouer de la musique, passer des appels ou utiliser les services de navigation). Cela soulève plusieurs enjeux et risques. S'il est déjà peu probable que les propriétaires de véhicules lisent les politiques de confidentialité au moment de l'achat, il est encore moins plausible que les utilisatrices et utilisateurs des services d'autopartage en prennent connaissance avant chaque trajet.

Les systèmes d'infodivertissement peuvent conserver certaines informations (historique d'appel, d'adresses rentrées dans le GPS, etc.) localement, et ce, même après la déconnexion du téléphone. Il y a donc un risque que les informations d'une personne soient accessibles pour le client suivant. Qui, le cas échéant, en est responsable ? Le constructeur du véhicule, qui opère le système d'infodivertissement ? Ou la compagnie de location/autopartage, qui met le véhicule à la disposition des individus ? Certaines compagnies remettent au client la responsabilité de supprimer ses renseignements

personnels, données et informations sur les appareils connectés à la fin de sa location. On peut se demander si cette façon de procéder est conforme aux dispositions légales. Même si c'est le cas, cela ne semble pas adéquatement protéger les individus. Qui, en cas d'incident, doit alors être tenu responsable?

Enfin, certaines entreprises ne possèdent pas elles-mêmes d'automobiles et servent plutôt d'intermédiaire entre des particuliers qui mettent

leur véhicule à disposition d'autres particuliers, suivant ainsi un modèle semblable à l'entreprise d'hébergements à court terme Airbnb. Au Québec, c'est le cas de Turo. Cela suscite des interrogations : comment s'assurer que les propriétaires n'ont pas accès aux données personnelles des clients, par les systèmes de télématique et d'infodivertissement, et inversement? Encore une fois, qui est responsable en cas d'incident?

3.6 Le droit d'usage et la réparabilité

En plus des enjeux de vie privée et de surveillance liés à la connectivité et à la collecte de données, les véhicules connectés soulèvent des préoccupations en lien avec les **droits de propriété, d'usage** et à la **réparation**⁶⁴.

Les véhicules connectés comportent de nombreuses composantes électroniques et numériques. En raison de la centralité du système logiciel dans le fonctionnement des véhicules les réparations doivent de plus en plus passer par un accès au logiciel du constructeur : sans ce dernier, il est impossible d'avoir accès aux données diagnostiques, par exemple. Des mises à jour logicielles fréquentes sont requises, notamment pour des raisons de sécurité, ce qui peut créer des cas d'obsolescence prématurée⁶⁵ : par exemple, certaines fonctionnalités peuvent cesser d'exister lorsque le constructeur décide de ne plus mettre à jour une génération de véhicules, même si ces derniers sont encore en bon état. Certaines fonctionnalités peuvent également n'être accessibles que si le client paye un abonnement — même s'il a acheté le véhicule.

De plus, les constructeurs utilisent différents moyens (verrous numériques, logiciels propriétaires, etc.) pour garder le monopole sur les données, limiter l'autodiagnostic, et imposer des restrictions à la réparation. Ils justifient ces mesures au nom de la sécurité, mais les recherches et consultations effectuées par l'Union des consommateurs montrent que « [les risques liés à la cybersécurité] n'ont aucun lien évident avec la réparation indépendante ou le partage des données diagnostiques »⁶⁶. Toujours selon l'Union des consommateurs, la législation canadienne, notamment la *Loi sur le droit d'auteur*, ne « mitige pas les risques associés au droit de propriété identifié ; au contraire, elle permet aux fabricants d'adopter des pratiques qui se révèlent désavantageuses pour les consommateurs⁶⁷ ».

Ces pratiques entravent les droits individuels des consommateurs. Elles limitent les possibilités de faire appel à des mécaniciens automobiles indépendants, menaçant ainsi de créer un enjeu de monopole. Enfin, l'obsolescence et les obstacles à la réparabilité génèrent également d'importantes conséquences environnementales (voir la section 3.8).

3.7 Les enjeux liés à la personnalisation des assurances en fonction des habitudes de conduite

Les données collectées par les voitures connectées fournissent des informations qui peuvent aider à déterminer les circonstances d'un accident. Elles permettent également aux assureurs d'offrir, aux personnes qui acceptent d'y adhérer, des programmes d'assurance à la

conduite (*usage-based insurance* – UBI). Il s'agit de polices personnalisées dont la prime est établie en fonction des habitudes de conduite de la personne assurée. Ce type de calcul actuariel intègre des facteurs tels que la vitesse, la qualité de certaines opérations comme le freinage et

l'accélération, la géolocalisation et les trajets récurrents, les périodes de conduite dans la journée (p. ex. matin, nuit), les distractions potentielles telles que l'usage du téléphone au volant, etc.

Ces calculs permettent d'attribuer des scores de conduite aux personnes qui adhèrent à un programme d'assurance à la conduite. Celles dont la conduite est jugée sécuritaire profiteront d'une prime réduite, alors que la prime de celles dont la conduite est jugée plus à risque pourrait être revue à la hausse. Certaines juridictions interdisent ce type d'assurance (p. ex. Californie⁶⁸). D'autres autorisent la réduction, mais interdisent les augmentations (p. ex. Caroline du Nord⁶⁹). Au Québec et en Ontario, les deux pratiques sont permises⁷⁰. La Colombie-Britannique, le Manitoba et la Saskatchewan ont des systèmes d'assurances automobile entièrement publics et n'offrent pas d'assurance à la conduite⁷¹.

Selon certains, cette pratique a des avantages importants. Par exemple, elle permettrait de rendre la tarification plus équitable et les routes plus sécuritaires en mettant en place des incitatifs à conduire plus prudemment⁷². Cependant, d'autres estiment que cette pratique soulève des enjeux éthiques non négligeables.

Outre les atteintes à la vie privée soulevées précédemment, une des critiques de ce type d'assurance est que certains groupes soient

injustement pénalisés. Par exemple, la conduite de nuit ou dans certains quartiers peut être considérée comme risquée par certains assureurs. Or cela pénalise les personnes qui travaillent de nuit, habitent ou travaillent dans ces quartiers, ces personnes étant souvent socioéconomiquement désavantagées ou racisées⁷³.

Un autre enjeu est que les comportements de conduite soient interprétés sans prendre en compte l'ensemble des éléments du contexte. Par exemple, un freinage brusque pourrait être qualifié de dangereux alors qu'il pourrait s'agir de la bonne manœuvre pour éviter de heurter un piéton ou un cycliste⁷⁴. Ainsi, le fait de conduire régulièrement dans des quartiers densément peuplés pourrait être pénalisé.

Enfin, le manque de **transparence** des assureurs et des courtiers qui fournissent les données ou calculent les scores, ainsi que l'**opacité** des algorithmes de traitement des données lors du calcul des scores, soulèvent des enjeux importants. En effet, ils réduisent de manière importante la capacité de surveillance des pratiques des compagnies d'assurance par les organismes régulateurs, affaiblissent la reddition de comptes des assureurs et nuisent à la possibilité, pour la personne assurée, de comprendre et de contester le score qui lui est attribué.

3.8 Les effets environnementaux grandissants des voitures et des technologies numériques

Les technologies numériques sont souvent présentées comme des leviers clés de la transition écologique, notamment en raison de leur capacité à optimiser des systèmes complexes et à améliorer l'efficacité énergétique. Cela s'applique aussi au secteur des transports et des voitures connectées, le numérique étant alors associé à des promesses comme l'amélioration de la sécurité routière ou l'optimisation des flux de circulation. Pourtant, les conséquences directes et indirectes du numérique sur l'environnement suscitent de plus en plus d'inquiétudes, au point d'être perçues comme une menace réelle à la transition écologique et à la lutte contre les changements climatiques⁷⁵.

Effets directs

Les effets environnementaux directs des voitures connectées correspondent à l'ensemble des dommages écologiques et sociaux résultant du cycle de vie complet des équipements embarqués et de l'infrastructure sur laquelle ils reposent (réseaux de télécommunication, centres de données, terminaux des conductrices et conducteurs, etc.). Cela inclut donc les conséquences de l'extraction des matières premières, l'importante quantité de ressources naturelles, dont plusieurs sont non renouvelables ou limitées, nécessaires à la fabrication et à l'utilisation des appareils, l'espace occupé par les infrastructures du numérique sur le territoire

et les résultantes de la fin de vie de ces nombreux équipements⁷⁶. S'ajoutent à ces effets directs les conflits d'usages et les conséquences que ces besoins grandissants génèrent déjà sur les infrastructures locales, les milieux naturels, la qualité de l'air et la santé des populations environnantes⁷⁷. L'ampleur des répercussions de la fin de vie des appareils numériques est aussi souvent sous-estimée alors qu'en 2022 on estimait que 62 millions de tonnes de déchets d'équipements électriques et électroniques avaient été produites. De celles-ci, seulement 22 % (en 2024) étaient correctement recyclées⁷⁸, le reste générant d'importants coûts environnementaux et des problèmes sanitaires.

Effets indirects

Les transformations numériques occasionnent aussi des changements de pratiques, de comportements et des modes de consommation ou de production qui engendrent des effets indirects sur l'environnement. Des phénomènes socioéconomiques liés à la commercialisation et à l'innovation technologique, comme l'obsolescence, le solutionnisme technologique, l'économie de l'attention et la dépendance au numérique, agissent comme accélérateurs de ces effets⁷⁹.

Le passage vers une connectivité accrue des véhicules peut conduire à la transformation des pratiques de mobilité, des comportements des usagers et usagères et des modèles économiques du secteur automobile, ensemble de transformations qui concourent à l'accroissement des effets environnementaux du numérique. Par exemple, l'intégration de nouvelles fonctionnalités numériques misant sur des logiques d'engagement accentue la collecte de données, intensifie la consommation de contenu et est susceptible d'inciter la clientèle à acquérir plus d'appareils ou à les renouveler plus fréquemment⁸⁰.

Les développements technologiques peuvent aussi être associés à des effets rebonds. Généralement, un effet rebond a lieu lorsque l'amélioration d'un aspect d'un procédé entraîne des conséquences négatives imprévues en raison d'une adoption ou d'une utilisation accrue du produit optimisé⁸¹. Par exemple, les systèmes d'aide à la conduite, de navigation ou de gestion

intelligente du trafic peuvent contribuer à fluidifier la circulation et donc à réduire les émissions de GES associées au transport. Toutefois, l'amélioration du confort, de la sécurité et de l'expérience globale offerte par les voitures connectées pourrait aussi encourager une utilisation accrue du véhicule individuel, au détriment de modes de transport plus sobres, par exemple. Les gains potentiels peuvent donc être partiellement ou totalement annulés par des effets rebonds, avant même d'intégrer à ce calcul les effets environnementaux de l'ensemble du cycle de vie des appareils et de l'infrastructure qui soutiennent ces nouvelles fonctionnalités.

En 2024, la Commission formulait 16 recommandations dans un avis⁸² pour atténuer les effets environnementaux du numérique et soutenir l'adoption de la sobriété numérique. Plusieurs d'entre elles sont pertinentes à l'analyse des enjeux environnementaux propres aux voitures connectées :

Recommandation 4 : La Commission recommande que le gouvernement du Québec légifère afin de rendre obligatoire la divulgation du plus grand nombre possible de données, essentielles à l'évaluation des impacts environnementaux du cycle de vie des technologies numériques mises en marché sur son territoire et des services numériques en ligne utilisés au Québec (consommation d'eau, d'énergie et de métaux rares; émissions de GES; lieux où circulent et sont stockées les données; etc.).

Recommandation 6 : La Commission recommande que le gouvernement du Québec renforce les normes environnementales entourant les technologies et les services numériques, et instaure des incitatifs économiques encourageant les acteurs du numérique à adopter des pratiques sobres et soutenables.

Recommandation 7 : La Commission recommande que le gouvernement du Québec favorise davantage la circularité de l'économie, de manière à réduire, ralentir et boucler les flux de matières, lorsque celle-ci est réellement bénéfique sur le plan environnemental.

Recommandation 8 : La Commission recommande que le gouvernement du Québec s'engage à inciter ou à rendre obligatoire un nombre croissant de pratiques favorisant

l'écoconception des technologies numériques, qu'il favorise ces technologies et les rende attrayantes auprès du grand public.

Recommandation 9 : La Commission recommande au gouvernement du Québec de procéder à des révisions réglementaires périodiques du système REP afin de rétablir le principe du pollueur-payeur et de renforcer la transparence et le dialogue avec toutes les parties prenantes.

Recommandation 10 : La Commission recommande que le gouvernement du Québec s'engage fortement dans la lutte contre toutes les formes d'obsolescence des technologies numériques à l'aide d'outils variés.

Recommandation 12 : La Commission recommande que le gouvernement du Québec réalise des campagnes de sensibilisation et d'information visant l'ensemble de sa population quant aux effets environnementaux positifs et négatifs du numérique, et aux gestes à poser afin de minimiser ses effets négatifs.

Recommandation 16 : La Commission recommande que le gouvernement du Québec encourage et soutienne la création d'espaces favorisant l'augmentation de la littératie numérique, la participation citoyenne dans la démarche de sobriété numérique, ainsi que la mutualisation des appareils.

3.9 L'accès aux données par les services de police

Les données récoltées par les véhicules connectés peuvent être utilisées par les services de police dans l'exercice de leurs mandats, c'est-à-dire la surveillance et la prévention du crime, le maintien de l'ordre et les enquêtes. Parmi les types de données qui pourraient leur être utiles, on compte les données de géolocalisation, celles captées par les caméras embarquées, les historiques d'appels, les contacts, etc.

Vie privée, consentement et ordonnance de la cour

En ce qui a trait à l'accès aux données des véhicules connectés par les services de police, le consentement libre et informé ou la nécessité d'obtenir une autorisation judiciaire sont des mécanismes visant à favoriser la **protection de la vie privée** et, plus particulièrement, à défendre le **droit à la protection contre les fouilles, les perquisitions ou les saisies abusives** (article 8 de la Charte canadienne des droits et libertés).

Il existe différents types d'autorisations judiciaires. Par exemple, un mandat de perquisition autorise les services de police à rechercher et à saisir des preuves d'une infraction (p. ex. perquisition d'un véhicule connecté). L'ordonnance de production (ou de communication), quant à elle, contraint

une personne ou une entreprise à transmettre des documents ou des données (ex. données détenues par un constructeur automobile), sans devoir recourir à une perquisition physique directe.

Pour obtenir une telle autorisation, les services de police doivent démontrer au juge qu'il existe « des motifs raisonnables de croire qu'une infraction a été ou sera commise et que l'information fournira une preuve de cette infraction⁸³ ».

Modalités d'accès aux données du véhicule par les services de police

Les données collectées par les véhicules connectés peuvent être stockées dans le véhicule ou sur des serveurs extérieurs opérés par des entreprises privées. Dans le premier cas, les services de police doivent traiter avec le propriétaire du véhicule, dans le second, avec l'entreprise.

Les données stockées dans le véhicule

L'analyse judiciaire numérique des véhicules est une branche de la criminalistique numérique⁸⁴ qui consiste à récupérer les preuves numériques ou les données stockées dans un véhicule connecté.

Les données récoltées par un véhicule connecté et stockées dans ce même véhicule sont considérées comme appartenant au propriétaire de la voiture⁸⁵. Ainsi, de manière générale, les services de police doivent avoir le **consentement** du propriétaire ou un **mandat de perquisition** pour y avoir accès⁸⁶, mais il existe des exceptions.

Par exemple, selon un jugement de la Cour d'appel de l'Ontario (*R. v. Attard*, 2024 ONCA 616), il n'y a pas d'attente raisonnable en matière de vie privée pour les données captées par l'enregistreur de données d'événement avant et après une collision (*event data recorder* [EDR] ou « boîte noire »). Ces données concernent la vitesse, la direction, l'accélération, le freinage et peuvent être extraites par la police **sans consentement ni autorisation judiciaire**. Cependant, les services de police doivent avoir des **motifs raisonnables** pour saisir et fouiller le véhicule, par exemple s'il y a de bonnes raisons de croire que la vitesse ou une conduite dangereuse est à l'origine d'un accident⁸⁷.

Les données stockées sur des serveurs hors du véhicule

De manière générale, pour avoir accès aux données stockées sur les serveurs d'une entreprise privée (ex. constructeurs automobiles, développeurs d'applications, fournisseurs de services tiers), les services de police doivent obtenir une **ordonnance de production**. Une telle autorisation contraint les entreprises canadiennes ou étrangères opérant au Canada à transmettre aux policiers les documents ou renseignements réclamés dans le cadre d'une enquête criminelle si ceux-ci sont en sa possession ou à sa disposition⁸⁸, c'est-à-dire accessibles depuis le Canada⁸⁹.

Or, une part importante des données collectées par les véhicules connectés au Canada sont entreposées à l'étranger sans accès depuis le Canada. Néanmoins, selon la jurisprudence canadienne, les ordonnances de production s'appliquent également à ces renseignements. Dans un procès opposant le Service de police de la Ville de Montréal et la compagnie américaine Snap Inc. (Snapchat), la Cour supérieure du Québec a conclu que les entreprises opérant au Canada – même virtuellement – doivent transmettre les données visées par un mandat

même lorsqu'elles sont entreposées à l'étranger et qu'elles ne sont pas accessibles depuis le Canada⁹⁰. Dans un autre cas concernant une ordonnance de production canadienne visant Facebook, la Cour d'appel de l'Alberta⁹¹ puis la Cour suprême du Canada⁹² sont arrivées sensiblement à la même conclusion. Malgré ces décisions des tribunaux canadiens, l'application concrète d'une ordonnance judiciaire hors du pays est complexe, notamment en raison de la législation et la souveraineté des pays étrangers.

Surveillance policière

Les véhicules connectés viennent s'ajouter à la liste de nombreux objets connectés que l'on regroupe souvent sous l'appellation *Internet des objets*. Outre les téléphones, tablettes et ordinateurs, ces objets comprennent : les caméras de sécurité résidentielles ; les assistants intelligents munis de micros ; les thermostats munis de capteurs de mouvements ; les montres intelligentes ; des lunettes munies de caméras ; des moniteurs d'indicateurs de santé ou d'activités physiques (ex. Fitbit) ; etc.

Ces objets omniprésents comprennent des caméras, des micros et autres capteurs qui recueillent des données et des renseignements personnels en permanence : géolocalisation, mouvements, visages, photos, séquences audio (ex. conversations) et vidéo, signes vitaux, activité physique, etc. Les véhicules connectés viennent accroître la quantité de données collectées en recueillant notamment les trajets effectués par les personnes et en multipliant les caméras filmant l'espace public. Toutes ces informations sont potentiellement accessibles aux services de police et s'ajoutent aux outils de surveillance des services de police.

Ces données et renseignements peuvent soutenir des enquêtes criminelles⁹³. Cependant, le sentiment d'être observé en permanence peut avoir des effets dissuasifs (*chilling effect*) sur la capacité ou la volonté des personnes d'exprimer leurs opinions, de se réunir pacifiquement et de se mobiliser pour s'opposer à des décisions et actions des autorités⁹⁴. Il s'agit non seulement de **droits et libertés** garantis dans les chartes québécoise et canadienne, mais également d'éléments contribuant à la **santé des démocraties**.

Justification de l'intrusion dans la vie privée

Enfin, la protection de la vie privée est tributaire de la rigueur avec laquelle sont appliqués des mécanismes mis en place. Le consentement des propriétaires de voitures, qu'ils soient eux-mêmes ou une autre personne suspects dans une enquête, doit être libre et informé⁹⁵. Un consentement **libre** est donné sans pression, intimidation, coercition, menace ou influence induite. Un consentement est **informé** lorsque

la personne reçoit, dans un langage accessible et clair, toutes les informations pertinentes : quelles données seront collectées, à quelle fin précise, quels en sont les risques et bénéfices, etc.

Pour ce qui est des autorisations judiciaires, les motifs déclarés par les enquêteurs doivent l'être de bonne foi et fondés sur des faits (et non sur de simples soupçons) puis faire l'objet d'une analyse rigoureuse, impartiale et factuelle par les juges.

3.10 La sécurité nationale

Au Canada, 70 % des véhicules neufs devront être électriques ou hybrides à partir de 2035. D'aucuns croient que l'atteinte de cette cible sera difficile sans l'apport des véhicules chinois plus abordables⁹⁶. En janvier dernier, Ottawa a annoncé qu'un accord commercial a été conclu avec la Chine. En vertu de cet accord, le Canada a fait passer ses droits de douane de 100 % à 6,1 % sur un nombre croissant de véhicules électriques chinois, soit 49 000 la première année pour atteindre 70 000 unités annuellement en 2030⁹⁷.

Cet ajout de véhicules électriques chinois abordables aux 240 000 déjà vendus annuellement au Canada pourrait contribuer aux efforts de réduction des GES au pays, et ce, à moindre coût pour les consommateurs. Cependant, des critiques soulèvent les risques pour la sécurité nationale que représentent ces véhicules en matière d'espionnage et de sabotage.

Risques d'espionnage

Certains enjeux potentiels entourant l'arrivée imminente des véhicules électriques chinois concernent l'espionnage. En effet, les véhicules électriques sont souvent connectés à Internet et munis de nombreux capteurs pouvant recueillir une masse de données, tant à l'intérieur qu'à l'extérieur de la voiture. D'une part, cela permet de collecter des renseignements sensibles au sujet d'acteurs gouvernementaux et d'autres acteurs d'intérêt à l'intérieur du véhicule (ex. enregistrer des conversations⁹⁸). D'autre part, les capteurs orientés vers l'extérieur peuvent

cartographier l'environnement naturel et construit, puis collecter des renseignements sur des sites sensibles (ex. bases militaires) et des infrastructures critiques (ex. centrales et réseaux électriques)⁹⁹.

Ces préoccupations ne concernent pas exclusivement les véhicules électriques chinois. En 2021, les autorités chinoises ont elles-mêmes interdit aux employés du gouvernement de circuler avec des voitures Tesla dans des secteurs sensibles, tels que ceux où sont situés des établissements militaires, certaines agences gouvernementales et autres entreprises appartenant à l'État¹⁰⁰.

Risques de sabotage

D'autres enjeux sont liés à la possibilité de mener des opérations de sabotage. Certaines fonctions des véhicules connectés pourraient être utilisées par des acteurs malveillants pour immobiliser un grand nombre de voitures et entraîner une paralysie du réseau routier¹⁰¹. Par exemple, des constructeurs offrent des fonctionnalités de suivi et de ralentissement ou d'immobilisation du véhicule en cas de vol¹⁰². D'autres fonctions, telles les mises à jour logicielles à distance (*over-the-air* – OTA), pourraient être exploitées¹⁰³. En effet, insérer des logiciels malveillants ou perturber une mise à jour en cours peut rendre les véhicules non opérationnels (voir la section 3.4).

Menaces venant d'acteurs et de pays divers

Il est à noter que ces risques se posent pour tous les véhicules connectés munis de capteurs et offrant des fonctions à distance, quelle que soit leur origine.

Soulignons également que les acteurs pouvant menacer la sécurité nationale par l'intermédiaire des véhicules connectés ne sont pas uniquement des États, mais peuvent aussi être les constructeurs, en association ou non avec des États, ou encore des pirates informatiques indépendants.

Les constructeurs de véhicules connectés recueillent une vaste quantité de données, souvent plus qu'il n'est nécessaire pour les fins déclarées (ex. assurer la performance des fonctionnalités)¹⁰⁴. Or plusieurs États ont des lois qui leur permettent d'accéder aux données des entreprises incorporées dans leur pays, même si ces données sont recueillies à l'étranger (ex. *Cloud Act* et *Foreign Intelligence Surveillance Act* [FISA] aux États-Unis)¹⁰⁵.

Par ailleurs, les données recueillies par les constructeurs sont partagées avec des tiers, notamment des courtiers de données. Ces derniers pourraient les revendre à des agences gouvernementales de pays étrangers¹⁰⁶.

Enfin, des pirates informatiques pourraient exploiter des failles technologiques afin de dérober des données collectées par les véhicules connectés ou de désactiver simultanément un grand nombre de véhicules¹⁰⁷.

Mesures de mitigation potentielles

Différentes stratégies de mitigation des risques sont possibles pour les pays en fonction de leurs contextes particuliers. En voici quelques-unes.

L'approche américaine consiste à imposer 100 % de droits de douane et à interdire l'importation et la vente de véhicules connectés ainsi que de composantes informatiques destinées à ces véhicules en provenance de Chine et de Russie¹⁰⁸. En plus de nuire à la transition vers les voitures électriques, cette approche ne règle pas les problèmes liés aux véhicules connectés provenant des autres pays et abordés précédemment (ex. lois comme la FISA, comportements des courtiers de données et des pirates informatiques).

Une autre approche possible consiste à modifier le cadre législatif afin d'interdire, comme c'est le cas en Europe, le transfert des données d'un pays vers des États qui ne garantissent pas le même niveau de protection¹⁰⁹. Or, dans le contexte actuel, notamment avec un gouvernement fédéral états-unien qui ne respecte pas les lois américaines en matière de protection des données¹¹⁰, il est possible de se demander si cela est suffisant.

La Chine va plus loin en exigeant que les données chinoises restent sur son territoire. À titre d'exemple, les données recueillies par Tesla en Chine sont hébergées localement et l'entreprise affirme qu'elles ne sortent pas du pays¹¹¹. Mais cela est-il souhaitable ou réalisable dans tous les contextes nationaux? Une position intermédiaire pourrait être d'interdire les transferts transfrontaliers de certaines données sensibles seulement¹¹².

Enfin, les pays importateurs pourraient interdire aux véhicules connectés de certains pays de circuler dans des secteurs jugés sensibles ou exiger la désactivation des capteurs dans ces mêmes secteurs¹¹³.

3.11 Les enjeux entourant les flottes gouvernementales

Les gouvernements possèdent et utilisent des parcs de véhicules pour mener à bien leurs activités et services. La connectivité des véhicules offre de réels avantages pour la gestion de ces flottes, mais elle peut aussi poser des risques pour **l'intégrité publique** et la **sécurité nationale**.

Au Québec, le Centre de gestion de l'équipement roulant (CGER) offre aux organisations gouvernementales, paragouvernementales et municipales des services de soutien à l'acquisition, à l'entretien et à la gestion de parcs de véhicules. Le CGER, qui dépend du ministère

des Transports et de la Mobilité durable (MTMD), suit un plan d'électrification des flottes et développe des services d'autopartage et de télémétrie¹¹⁴.

Dans la section précédente, il a été montré que les véhicules connectés utilisés par des acteurs gouvernementaux dans certains secteurs critiques (défense, énergie, etc.) ou circulant dans des zones sensibles peuvent constituer des vulnérabilités pour la **sécurité nationale**. Toutefois, les données récoltées par les véhicules dans le cadre d'activités gouvernementales plus ordinaires peuvent également soulever des enjeux. Par exemple, l'ensemble des données de géolocalisation d'une flotte pourrait être analysé pour dresser un portrait relativement précis d'un secteur d'activité d'une organisation gouvernementale.

Il existe peu de littérature scientifique sur les enjeux éthiques soulevés par les véhicules connectés pour l'administration publique. Ainsi, la Commission soulève des questions et des enjeux d'intérêt pour les responsables de la gestion et du développement des parcs automobiles afin, éventuellement, d'envisager des mesures de mitigation des risques :

- Les enjeux de confidentialité et d'intégrité publique font-ils l'objet d'une analyse lors de l'acquisition des véhicules destinés aux parcs

gouvernementaux et paragouvernementaux? Les contrats incluent-ils des **clauses précises** sur la confidentialité et la gestion des données permettant de mitiger d'éventuels risques?

- Les responsables de l'acquisition sont-ils en mesure de **désactiver** la collecte des données, ou de certaines données, par les constructeurs?
- Les données de **géolocalisation** de ces véhicules sont-elles collectées en tout temps? Si oui, où sont-elles stockées et à qui sont-elles partagées?
- Les données collectées sont-elles **conservées** dans des serveurs situés sur le territoire national? Sont-elles susceptibles de traverser les frontières?
- Les données collectées sont-elles conservées dans des serveurs appartenant au gouvernement? Sont-elles susceptibles d'être conservées par des acteurs privés?
- Les données collectées pourraient-elles éventuellement faire l'objet de demandes d'accès à l'information?
- Certains jeux de données devraient-ils faire partie des données ouvertes rendues disponibles par le gouvernement¹¹⁵?

3.12 La valorisation des données d'utilité publique

Les données ne sont pas seulement source de risques : elles génèrent également des profits. Or ces derniers sont majoritairement au bénéfice des compagnies privées. Selon Pierre Trudel, professeur de droit, l'approche de la « protection des renseignements personnels » est dépassée et ne permet pas de se saisir de certains enjeux importants¹¹⁶. Cet expert avance qu'il serait plus adéquat de concevoir les données comme des ressources collectives. Adopter une telle approche soulève des questions en lien avec l'**équité** et la **répartition de la richesse**, et la **poursuite du bien commun**.

Tout d'abord, le cadre juridique actuel n'empêche pas la commercialisation des données – l'acquisition, l'analyse et l'exploitation des données constituant une part importante de

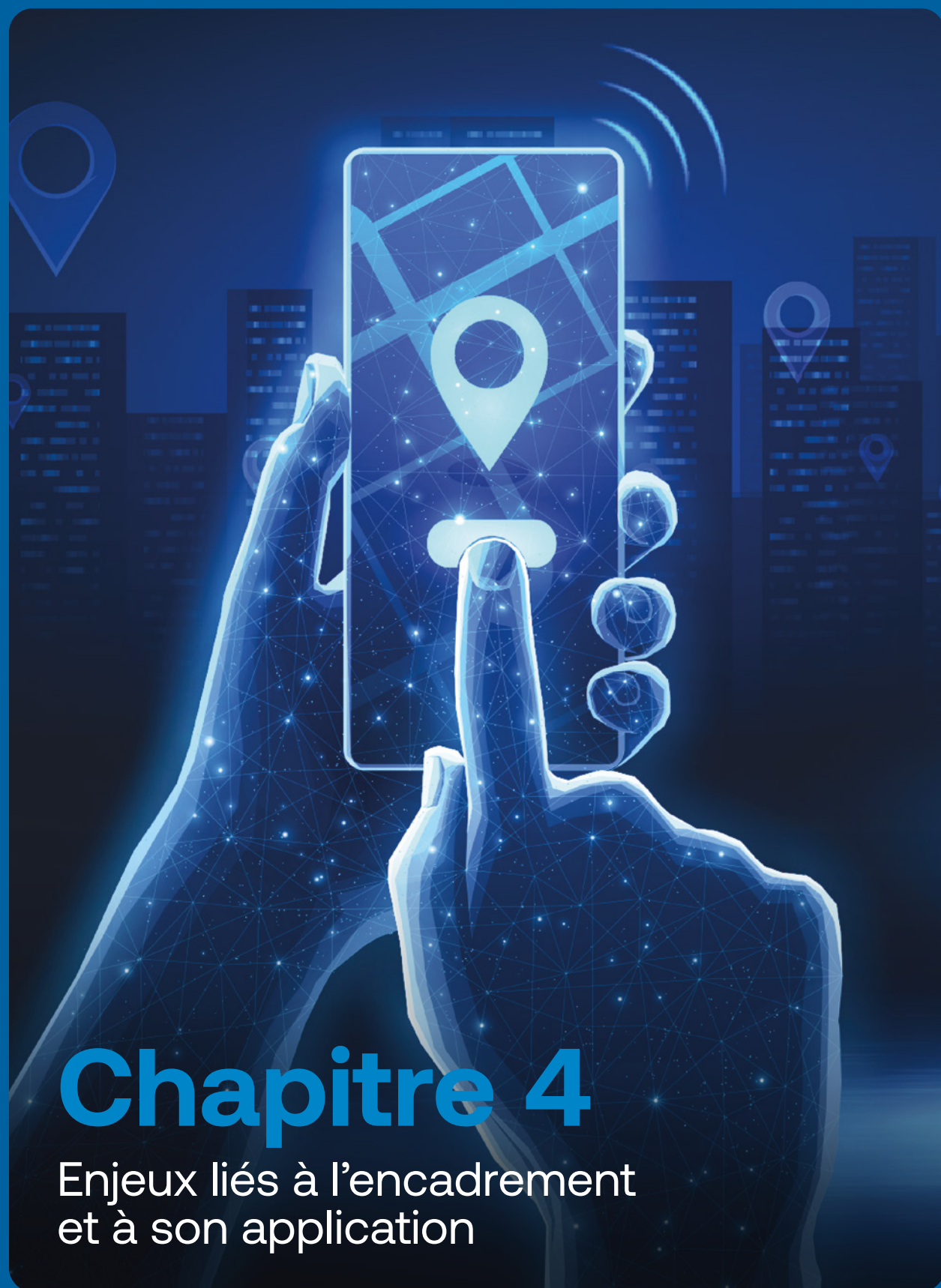
l'économie numérique, elle-même grandissante. La législation actuelle met en place certaines restrictions en ce qui concerne les renseignements personnels (identifiables). Toutefois, la circulation des données qui ne rentrent pas dans cette catégorie est beaucoup plus libre. Or les acteurs privés tirent un profit considérable de ces données – lesquelles peuvent être générées au sujet d'individus ou de groupes, même si elles ne sont pas des renseignements personnels au sens de la loi. On peut par exemple penser aux habitudes de déplacement ou de consommation des citoyennes et citoyens. Ainsi, selon Trudel, « [i]l suffit d'obtenir le consentement de chaque individu pour disposer de la faculté d'extraire de la valeur des gisements de données constituées par les faits et gestes de ceux qui vivent dans le

réseau et dans le monde connecté ¹¹⁷ ». Il s'agirait alors d'un phénomène d'extraction de la valeur des données.

Est-il souhaitable, et même possible, de lutter contre la commercialisation des données ? Ou faut-il plutôt accepter ce phénomène et tenter de s'assurer que les bénéfices de la marchandisation des données sont répartis plus équitablement ?

Envisager les données comme **ressources collectives** ne revient pas uniquement à en penser les **bénéfices économiques**. Au-delà de leur valeur marchande, les données peuvent être utilisées dans le cadre de projets sociétaux et à des fins relevant des acteurs publics. Les données générées par les véhicules connectés

peuvent certes être utilisées à des fins marketing, mais elles peuvent également s'avérer très utiles pour les municipalités et les organismes publics qui gèrent l'administration du transport et des infrastructures routières. Comment s'assurer que les données, en tant que ressource collective, ne sont pas accaparées par des acteurs privés à des fins purement lucratives, et servir des projets collectif et d'intérêt public¹¹⁸ ? Comment trouver l'équilibre entre les droits concurrentiels des entreprises, tels que le droit au **secret industriel**, et les potentiels usages des données pour le **bien commun** ? Ce sont des questions importantes à considérer afin de penser adéquatement la valorisation des données d'utilité publique.



Chapitre 4

Enjeux liés à l'encadrement
et à son application

Cette dernière section s'attarde aux enjeux qui sont liés à l'encadrement requis par les enjeux éthiques soulevés dans la section précédente ainsi qu'à l'application de cet encadrement. Certains de ces enjeux d'encadrement et d'application ont été brièvement soulevés dans ce document, mais il apparaît important d'y revenir et de les détailler davantage afin de prendre adéquatement la mesure des défis qu'ils représentent.

4.1 Une industrie difficile à réguler

Plusieurs caractéristiques du marché des voitures connectées rendent son encadrement particulièrement difficile, notamment la nature des données, et le fait qu'il s'agit d'une industrie opaque et internationale.

Tout d'abord, les données sont, par nature, hautement reproductibles et transférables, sous réserve de la disponibilité des ressources matérielles nécessaires à leur conservation. Cette caractéristique pose un défi unique pour les tentatives d'encadrement des flux de données¹¹⁹. Il est difficile pour les individus de garder la trace de leurs données : qui les possède, qui les partage? De même, une fois que les données sont partagées à des tiers, il est difficile, voire impossible, de s'assurer que ces derniers respectent l'ensemble de leurs obligations. D'où l'importance d'adopter une approche préventive et minimaliste en matière de collecte des données (voir la section 4.4).

Il est très difficile de se renseigner sur les pratiques exactes de l'industrie automobile en ce qui concerne la gestion des données et la protection des renseignements personnels. Les nombreux acteurs impliqués dans cette industrie ne sont pas toujours identifiables. Les politiques de confidentialité mentionnent partager les données à des tiers, à des partenaires ou à des fournisseurs de service. Qui sont-ils? Leurs pratiques sont-elles conformes aux meilleurs standards de l'industrie?

Qui est responsable de s'assurer que les acteurs privés remplissent leurs obligations? C'est là une question de **gouvernance** du secteur. L'application des lois demande des moyens (financiers, matériels, humains) et des capacités d'expertise très importants, et il n'est pas toujours réaliste pour les organisations

publiques de s'en charger. Le risque est donc d'avoir des lois qui ne sont pas appliquées et qui, par conséquent, ne favorisent pas la responsabilisation de l'ensemble des acteurs entourant cette industrie. On peut alors se tourner vers des mesures d'autorégulation de l'industrie (avec des programmes de conformité et de certifications) dans le but de **responsabiliser les entreprises**. Toutefois, la régulation privée a ses limites, notamment en raison des conflits potentiels entre les **intérêts économiques** des acteurs et la visée du **bien commun**.

Alors qu'il a été confirmé aux États-Unis que des acteurs de l'industrie automobile se sont prêtés à certaines pratiques répréhensibles, comme la vente illégale de données personnelles, l'état de la situation est moins clair au Canada. En effet, il n'y a pas eu de cas équivalents portés devant les tribunaux canadiens. Faut-il en conclure que les renseignements personnels des citoyennes et citoyens canadiens sont mieux protégés que ceux de leurs voisins? ou que les organismes de vérification manquent de moyens pour repérer d'éventuelles pratiques illicites? Notons que puisqu'il est plausible que de nombreuses données soient transférées et stockées aux États-Unis, les scandales et pratiques problématiques aux États-Unis pourraient éventuellement sérieusement affecter les consommateurs canadiens. Il apparaît essentiel de mieux comprendre les pratiques de l'industrie canadienne, afin de pouvoir évaluer la **conformité** aux juridictions en vigueur. Une zone d'ombre particulièrement résistante concerne les **courtiers de données** et la **commercialisation des données**. Le fonctionnement de ce marché et l'identité de ces acteurs restent difficiles à saisir avec précision.

Le **manque de transparence** de cette industrie nuit aux pratiques d'**attribution de responsabilité et de reddition de comptes**.

Enfin, le caractère **international** de l'industrie ajoute un degré de difficulté aux efforts d'encadrement. Les États imposent des règles sur la collecte et l'utilisation des renseignements personnels; mais le marché automobile est international et il semble que les données soient fréquemment transférées à l'extérieur des pays

où elles sont récoltées¹²⁰. C'est pourquoi le RGPD (en Europe) et la LPRPSP (au Québec) prévoient des mécanismes visant à s'assurer que les données bénéficient d'une **protection équivalente** à celle prévue localement. Mais la *Loi sur la protection des renseignements personnels et les documents électroniques* (au Canada) ne contient pas de telles clauses. Par ailleurs, on peut s'interroger sur l'**efficacité** de ces mécanismes (voir la section 4.4).

4.2 Les limites du consentement

Le législateur québécois souhaite promouvoir l'**autodétermination informationnelle** des citoyennes et citoyens en leur donnant la possibilité de **consentir** à la collecte de leurs renseignements personnels. Pourtant, les différents organismes qui se sont déjà penchés sur la question sont unanimes : les propriétaires et utilisatrices et utilisateurs de voitures connectées perdent rapidement le contrôle sur leurs données. Ainsi, ces personnes ne peuvent exercer leur **autonomie** en matière de vie privée en ce qui a trait aux voitures connectées.

Plusieurs affirment ainsi que les pratiques de demande de consentement des fabricants automobiles ne permettent pas un consentement véritablement libre, continu et éclairé. Ces

demandes, comme les politiques de confidentialité, manquent à la fois de clarté et de précision. Elles emploient régulièrement des formulations vagues (par ex. *Nous pouvons utiliser les renseignements vous concernant en vue [...] de **fournir nos produits et services***¹²¹). Une étude menée par l'Union des consommateurs souligne que les utilisateurs des services connectés comprennent mal leur contenu : « *Nos résultats révèlent que la majorité de nos répondants ne se souviennent pas avoir consenti à la collecte de données et n'ont pas une compréhension ou les connaissances suffisantes des pratiques pour être capables de donner un consentement éclairé. Même s'ils ont compris ces pratiques, il est clair qu'ils n'en saisissent pas pleinement les risques*¹²² ».

UN LANGAGE SIMPLE ET CLAIR?

Selon la LPRPSP, les demandes de consentement doivent **être formulées dans des termes simples et clairs**.

Qu'est-ce qui constitue un langage simple et clair? Il n'y en a pas de définition dans la législation ni dans la jurisprudence. Toutefois, la CAI propose des ressources pour rédiger les documents dans un langage approprié; il existe également des normes ISO à cet effet¹²³. Ces lignes directrices ne sont toutefois pas contraignantes.

Quand bien même les politiques de confidentialité seraient toutes rédigées dans un langage clair et précis, cela ne permettrait pas pour autant de garantir la qualité du consentement. En effet, les consommateurs les

signent souvent à l'achat du véhicule, sans les lire en détail. En 2008, deux chercheuses ont estimé que cela prendrait environ 244 heures par année, ce qui correspond à 40 minutes quotidiennes, pour un internaute américain moyen

afin de lire les politiques de confidentialité de tous les sites Internet visités. Ces chiffres déjà frappants datent de 2008 ; on peut imaginer qu'ils sont beaucoup plus élevés depuis¹²⁴. Il n'est donc pas surprenant qu'un rapport de 2023 nous apprenne que 56 % des répondants acceptent *toujours ou souvent* les politiques de confidentialité sans les lire. Seulement 18 % indiquent ne jamais, ou presque jamais, accepter une politique de confidentialité sans l'avoir lue¹²⁵. En outre, dans le cas des voitures connectées, ces politiques apparaissent sur l'écran du système d'infodivertissement, dans un format parfois peu adapté à la lecture. Tous ces facteurs peuvent causer chez les individus la **fatigue de consentement**, c'est-à-dire un sentiment de lassitude, d'ennui, de surcharge cognitive voire de cynisme face à des demandes de consentement répétées (sur des sites Internet, des applications, et maintenant, l'écran du véhicule)¹²⁶. Seulement 13 % des personnes ayant répondu au sondage réalisé par l'Union des consommateurs se souviennent avoir reçu une invitation à la collecte des données liées à l'utilisation de leur véhicule ; environ 7 % disent avoir consulté la politique de confidentialité du constructeur¹²⁷.

De plus, les véhicules ne collectent pas uniquement les données des personnes qui signent les demandes de consentement : ils peuvent collecter des renseignements à l'insu des individus, qu'il s'agisse de passagers ou d'une conductrice ou d'un conducteur

occasionnel, sans même les informer ni avoir obtenu leur consentement. Plus encore, les caméras externes peuvent enregistrer des images d'autres usagers de la route : le modèle du consentement est entièrement inefficace pour gérer le problème de la vie privée des passants (*bystander privacy*).

Il faut enfin souligner que le consentement perd de sa valeur lorsqu'il est nécessaire à l'achat ou à l'utilisation d'un véhicule. Même si une personne est mal à l'aise avec la collecte et l'usage de ses renseignements personnels prévus par les politiques de confidentialité et les contrats, va-t-elle pour autant renoncer à utiliser une automobile ? C'est pourquoi il est important qu'il soit toujours possible d'utiliser un véhicule de façon non connectée, sans que cela compromette sa durabilité ou la sécurité des usagers.

Cette **érosion de l'autonomie en matière de vie privée** constitue une perte en soi. Elle est encore plus délétère lorsqu'on examine le contexte dans lequel l'individu moyen semble vulnérable et impuissant **à pouvoir se protéger adéquatement contre de potentiels risques et abus en matière d'atteinte à la vie privée et de sécurité liés à la connectivité des véhicules**. Ainsi, les limites du consentement suscitent un doute quant à l'efficacité de l'approche de l'**autodétermination informationnelle** pour protéger la vie privée des personnes.¹²⁸

4.3 Les défis d'implantation de l'approche minimaliste en matière de collecte, conservation et destruction des renseignements personnels

La réglementation en vigueur, en particulier la LPRPSP, entend protéger les individus contre des atteintes à leur vie privée en forçant les acteurs privés à adopter une approche **minimaliste** en matière de collecte des renseignements personnels. Toutefois, la consultation des politiques de confidentialité et les différents rapports sur les pratiques de l'industrie montrent que ce n'est généralement pas le cas – notamment parce que les fabricants ont de **forts incitatifs économiques** à récolter le plus de données possible.

Collecte et utilisation

Plusieurs exigences légales visent à s'assurer que la collecte est bel et bien minimale, notamment l'exigence selon laquelle les renseignements personnels récoltés doivent être **nécessaires à la poursuite de fins légitimes et sérieuses**. Or, il est permis de se demander ce qui constitue une fin légitime : l'analyse des comportements de consommation des clients à des fins d'incitation comportementale (*nudging*) ou de publicités ciblées en fait-elle partie ? Dans son rapport paru en 2025, l'Union des

consommateurs propose d'aller plus loin en recommandant « l'interdiction totale de la collecte des renseignements personnels qui ne sont pas nécessaires pour le fonctionnement du véhicule ou des services connectés ¹²⁹ ».

La LPRPSP exige que la collecte respecte des critères de **nécessité** et de **proportionnalité**, et que l'entreprise indique quels renseignements sont collectés et quelles fins sont poursuivies. Toutefois, décliner les finalités pour chaque catégorie de renseignement collecté est considéré (notamment par la CAI) comme une **bonne pratique**, mais n'est pas obligatoire. Ainsi, peu des politiques consultées font l'exercice d'arrimer ces deux informations et présentent, en deux blocs, tous les renseignements collectés, puis toutes les raisons afférentes. Or, si on ne sait pas pour quelle fin chaque type de renseignement est collecté, alors on ne peut pas faire l'exercice d'évaluer la **nécessité** de la collecte, ni la **proportionnalité** du risque par rapport au sérieux de la finalité¹³⁰.

Suppression et anonymisation

Une fois que les renseignements personnels ne sont plus utiles, les entreprises ont l'obligation de les **supprimer** ou les **anonymiser** si elles veulent continuer de les utiliser¹³¹.

Par définition, l'anonymisation est irréversible : des renseignements anonymisés ne pourront plus jamais être réassociés à la personne. Dans le cas contraire, on parle de données dépersonnalisées. Néanmoins, les développements technologiques appellent

à faire preuve d'une grande **prudence**. Selon l'avis de la CAI, les développements technologiques, notamment des technologies d'IA, font en sorte qu'il est « quasi impossible de certifier que des renseignements anonymisés ne pourraient pas éventuellement être réidentifiés¹³² ». Qui plus est, l'assemblage d'un grand nombre de données est susceptible de fournir un profil relativement détaillé des personnes, ce qui accroît le risque qu'un croisement mène au rétablissement du lien entre les données et les individus¹³³. Par ailleurs, certaines données sensibles fournissent des informations qui ne peuvent être complètement dissociées des personnes, par exemple, les renseignements de géolocalisation.

Les politiques de confidentialité consultées indiquent que les renseignements personnels sont **détruits ou anonymisés**, sans préciser **à quelles fins** ils pourraient être anonymisés et réutilisés. Une des politiques indique même que les données *dépersonnalisées ou anonymisées* pourraient être « utilisées ou divulguées à quelque fin que ce soit »¹³⁴. Dans ce contexte, il est difficile de savoir précisément ce qu'il advient des renseignements personnels une fois les objectifs atteints. Plus encore, l'irréversibilité de l'anonymisation n'étant pas **standardisée**, on peut s'inquiéter du fait que les constructeurs semblent considérer la destruction et l'anonymisation comme deux options équivalentes : il est clair que la **destruction** offre une protection bien supérieure, en plus de réduire l'effet environnemental du numérique puisque les données n'ont plus à être hébergées (voir la section 3.8).

4.4 L'efficacité limitée des mécanismes en place

Certains des mécanismes de prévention, de régulation et de vérification prévus par le législateur ne semblent pas remplir leur plein potentiel. On note que certaines dispositions en vigueur au Québec n'ont pas d'équivalent dans la législation canadienne¹³⁵; or, c'est à cette dernière que doivent généralement se conformer les acteurs de l'industrie. D'autres raisons sont liées au manque de vérification, de transparence et de régulation dans l'application des lois.

Évaluations des facteurs relatifs à la vie privée (EFVP)

Au Québec, les entreprises ont l'obligation de réaliser des EFVP, notamment lorsqu'elles collectent des renseignements personnels par le biais de systèmes informatiques, et lorsque les données sont communiquées à l'extérieur de la province. Il s'agit de démarches d'analyse d'impact qui permettent de valider la conformité du projet envisagé, d'en analyser les risques et

de mettre en place des stratégies. Les EFVP sont réalisées par les entreprises, mais ne font pas l'objet d'une vérification externe, ni même d'une **obligation de transparence**. Autrement dit, elles s'inscrivent dans une perspective d'**autorégulation** et le public n'y a pas **accès**. On peut donc douter que les EFVP permettent d'atteindre les différentes fins envisagées¹³⁶.

Manque de moyens des organismes régulateurs

Considérant l'**opacité** des pratiques de l'industrie automobile, on ne peut faire un portrait complet de la conformité des pratiques et des risques pour la vie privée qu'au moyen d'**enquêtes**, qui demandent du temps et des ressources importantes, et qui placent les organismes régulateurs dans une position **réactive** plutôt que **préventive**. Or, les gardiens de la vie privée, comme la CAI ou le Commissariat à la vie privée du Canada, ont des moyens limités, ce qui les empêche de jouer pleinement le **rôle de régulateur** dans une industrie aussi importante¹³⁷.

Par ailleurs, les technologies utilisées sont complexes et chaque constructeur développe ses propres systèmes. Réaliser des enquêtes et des audits sur la gestion des données dans l'industrie automobile ne requiert donc pas uniquement des **ressources**, mais également une **expertise pointue**, qui n'est pas facile à trouver.

Conclusion

Ce rapport d'analyse présente une cartographie des enjeux éthiques qui émergent de l'industrie et du marché des véhicules connectés, en particulier en ce qui a trait aux données qui sont produites à partir de cet écosystème.

L'implantation des technologies connectées dans l'écosystème automobile soulève des enjeux et risques éthiques pour la **protection de la vie privée** des individus et des groupes, mais aussi pour la **souveraineté numérique**. Pour déterminer si ces technologies sont au service du **bien commun**, davantage de recherches empiriques sont requises, notamment pour déterminer les **gains concrets en matière de sécurité**, ainsi que **l'impact environnemental** des véhicules connectés. Une **bonification de l'encadrement** est requise; de tels efforts devront prendre en compte le caractère pluridimensionnel des enjeux, et mobiliser différents acteurs et mécanismes régulateurs.

La Commission espère que ce rapport donnera lieu à des travaux complémentaires, en particulier dans l'identification de pistes de solution pour un meilleur encadrement des industries automobiles, des technologies numériques et des flux des données.

Notes et références

1. California Privacy Protection Agency, « CCPA to Review Privacy Practices of Connected Vehicles and Related Technologies ». 31 juillet 2023. <https://privacy.ca.gov/2023/07/cppa-to-review-privacy-practices-of-connected-vehicles-and-related-technologies/>
2. Baule, A. et al. 2024. « Car Connectivity: What Consumers want and are willing to pay ». McKinsey & Company, 8 janvier 2024. <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/car-connectivity-what-consumers-want-and-are-willing-to-pay#/>
3. Singh, S. « Car Companies Can Generate \$1,600 Per Car In Future From Connected Car Services ». *Forbes*, 24 avril 2024. <https://www.forbes.com/sites/sarwantsingh/2024/04/24/car-companies-can-generate-1600-per-car-in-future-from-connected-car-services>.
« Connected Car Market Size, Trends, Statistics Report ». *The Brainy Insights*, septembre 2024. <https://www.thebrainyinsights.com/report/connected-car-market-13481#summary>
4. Caltride, J., Rykov, M. et MacDonald, Z. « What Data Does My Car Collect About Me and Where Does It Go? ». *Confidentialité non incluse*, 6 septembre 2023. <https://www.mozillafoundation.org/fr/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/>
5. Hill, K. « Federal Regulator Questions Carmakers About Unwanted Tracking via Their Apps ». *New York Times*, 11 janvier 2024. <https://www.nytimes.com/2024/01/11/technology/fcc-car-apps-stalking.html>
6. Picchi, A. « GM is selling driver data to insurers without consumers' knowledge ». *CBS News*, 15 août 2024. <https://www.cbsnews.com/news/gm-selling-driver-data-car-insurers-texas-lawsuit/>
7. Shepardson, D. « GM to pay \$12.75 million to settle California driver privacy probe ». *Reuters*, 8 mai 2026. <https://www.reuters.com/sustainability/boards-policy-regulation/gm-pay-1275-million-settle-california-driver-privacy-probe-2026-05-08/>
Kerr, D. « General Motors to pay \$12.75m settlement for selling drivers' location and data ». *The Guardian*, 9 mai 2026. <https://www.theguardian.com/us-news/2026/may/08/general-motors-settlement-driving-location>
8. Hill, K. « Your Car Is Tracking You. Abusive Partners May Be, Too ». *New York Times*, 31 décembre 2023. <https://www.nytimes.com/2023/12/31/technology/car-trackers-gps-abuse.html>
9. Hill, K. « Automakers Are Sharing Consumers' Driving Behavior with Insurance Companies ». *New York Times*, 11 mars 2024. <https://www.nytimes.com/2024/06/09/technology/driver-scores-insurance-data-apps.html>
10. BC Freedom of Information and Privacy Association. *The connected car: Who is in the driver's seat?* 2015.
11. Contant, J. « Connected vehicles: Are clients concerned about data privacy? ». *Canadian Underwriter*, 5 juin 2024. <https://canadianunderwriter.ca/2024/06/05/connected-vehicles-are-clients-concerned-about-data-privacy/>

12. Hill, K. « Federal Regulator Questions Carmakers About Unwanted Tracking via Their Apps ». *New York Times*, 11 janvier 2024. <https://www.nytimes.com/2024/01/11/technology/fcc-car-apps-stalking.html>.

Reuteurs, « Dutch watchdog decides against fine after Tesla alters security cameras ». *Reuters*, 22 février 2023. <https://www.reuters.com/business/autos-transportation/dutch-watchdog-decides-against-fine-after-tesla-alters-security-cameras-2023-02-22/>
13. Delatre, J. « Sharing vehicle data: let's not reinvent the wheel ». *Euractiv*, 26 septembre 2024. <https://www.euractiv.com/section/automated-vehicles/opinion/sharing-vehicle-data-lets-not-reinvent-the-wheel/>

Pinto, D. « Empowering drivers: why Data Privacy in connected cars must be a priority ». *Euractiv*, 4 novembre 2024. <https://www.euractiv.com/section/eet/opinion/empowering-drivers-why-data-privacy-in-connected-cars-must-be-a-priority/>
14. Ce tableau est inspiré de l'échelle d'automatisation des véhicules, qui comporte six niveaux allant d'aucune automatisation (niveau 0) à une automatisation complète en tous lieux et toutes circonstances (niveau 5 ; de tels véhicules n'existent pas à ce jour). Voir :

Transports Canada, « Comprendre les véhicules connectés et automatisés ». *Gouvernement du Canada*, 18 juillet 2019. <https://tc.canada.ca/fr/transport-routier/technologies-novatrices/vehicules-connectes-automatisees/comprendre-vehicules-connectes-automatisees>
15. Privacy4Cars, « Privacy4Cars' Five Levels of Vehicle Connectivity ». *Privacy4Cars*, consulté le 29 juin 2026. Traduction de l'anglais. <https://privacy4cars.com/data-in-cars/p4cs-five-levels-of-vehicle-connectivity/>
16. Stümpfle, J. et al., « The Software-Defined Vehicle: A Comprehensive Study on Current Trends and Challenges ». *IEEE Engineering Management Review*, 2025. DOI: 10.1109/EMR.2025.3636574.
17. Commission de l'éthique en science et en technologie (CEST). *L'Internet des objets, la vie privée et la surveillance – Balises éthiques et recommandations*, 2020. P. 5.
18. Le Goff, S. « Votre voiture devient une télécommande : voici comment Google veut révolutionner votre quotidien maison ». *Menow*, 25 juin 2025. <https://www.menow.fr/votre-voiture-devient-une-telecommande-voici-comment-google-veut-revolutionner-votre-quotidien/>
19. Godin, B. « Et si votre voiture prenait le contrôle de votre maison intelligente ? ». *La Presse*, 31 mai 2024. <https://www.lapresse.ca/auto/2024-05-27/techno/et-si-votre-voiture-prenait-le-controle-de-votre-maison-intelligente.php>
20. À l'heure actuelle, les définitions s'articulent autour de trois grands V (volume, vitesse, variété) auxquels s'ajoutent, de manière variable, trois autres V (validité, valeur, variabilité).
21. Déziel, P. L. « Les limites du droit à la vie privée à l'ère de l'intelligence artificielle : groupes algorithmiques, contrôle individuel et cycle de traitement de l'information ». *Cahiers de propriété intellectuelle*. Vol. 30, n°3, p. 827-847, 2018.
22. Commission d'accès à l'information. « Conservation et destruction des renseignements personnels ». *Commission d'accès à l'information*, consulté le 29 juin 2026. <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/conservation-destruction-renseignements-personnels>

Lubarsky, B. « Re-identification of "anonymized" data ». *Georgetown Law Technology Review*, 2017. <https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/>
23. Voir par exemple la Politique de confidentialité de Mercedes-Benz Canada.

Mercedes-Benz Canada, « Politique de confidentialité ». *Mercedes-Benz*, consulté le 30 juin 2026. <https://www.mercedes-benz.ca/fr/legal-notices/privacy-policy>
24. *Ibid.*
25. Enev et al. « Automobile Driver Fingerprinting ». *Proceedings on Privacy Enhancing Technologies Symposium*, n°1, 2016. DOI : <https://doi.org/10.1515/popets-2015-0029>

26. Conseil canadien des administrateurs en transport motorisé, *Lignes directrices aux administrations canadiennes sur la sécurité des essais et du déploiement des véhicules dotés d'un système de conduite automatisée*, 2022. p. 175.
27. Voir l'avis de la CEST : Commission de l'éthique en science et en technologie (CEST). *La ville intelligente au service du bien commun*, 2017.
28. En outre, puisque ce sont les assurances privées qui couvrent les dommages matériels en cas d'accident, on peut s'interroger sur le rôle des assureurs en cas de cyberattaques : les franchises d'assurance devraient-elles couvrir ces dernières ?
29. Société de l'assurance automobile du Québec, *Données et statistiques 2022*, 2023.
30. Institut de la statistique du Québec, « Estimations de la population au 1^{er} janvier et au 1^{er} juillet et indicateurs d'accroissement, Québec, 1971-2026 ». Québec : Institut de la statistique du Québec, 18 mars 2026. <https://statistique.quebec.ca/fr/produit/tableau/estimation-de-la-population-du-quebec>
31. P-39.1 - Loi sur la protection des renseignements personnels dans le secteur privé, art. 1 (1993, c. 17, a. 1 ; 2002, c. 19, a. 19 ; 2006, c. 22, a. 111 ; 2021, c. 25, a. 100.).
32. CCQ-1991 - Code civil du Québec.
33. C-12 - Charte des droits et libertés de la personne, article 5 (1975, c. 6, a. 5.).
34. Ces lois peuvent être consultées dans la base de données du NCSL (National Conference of State Legislatures) sur les véhicules automatisés : <https://www.ncsl.org/transportation/autonomous-vehicles-legislation-database>.
35. Le droit de garder sa vie privée à l'abri de la connaissance des autres correspond à la vie privée dite *informationnelle*. Le fait de pouvoir prendre des décisions sans ingérence ou contrôle d'autrui relève de la vie privée *décisionnelle*.
36. Une autre critique de cette dichotomie est à trouver du côté des théoriciennes féministes, qui montrent que la catégorie de « sphère privée » comme zone de non-intervention de l'État permet la reproduction de violences et de domination – voir par exemple les travaux de Susan Muller Okin. Okin, S. M. *Justice, gender, and the family*. Basic Books, 1989.
37. C'est par exemple le cas de la théorie de **l'intégrité contextuelle** de Nissenbaum. Selon cette approche, toutes les sphères d'activités humaines sont gouvernées par des *normes de flux de l'information (norms of information flow)*, même celles que l'on considère généralement comme « publiques ». Ces normes régulent quelles données sont appropriées dans un *contexte* précis, comment et avec qui elles peuvent être partagées. Voir : Nissenbaum, H. « Privacy as Contextual Integrity ». *Washington Law Review*, vol. 79, n°1, 2004.
38. Voir l'arrêt Gordon c. Canada (Santé), 2008 CF 258 (CanLII).
39. La CAI définit ainsi la granularité du consentement : « Il doit être demandé pour chacune des fins visées. S'il y a plusieurs finalités, le consentement doit être demandé séparément pour chacune d'elles. Cette granularité permet à la personne concernée de manifester sa volonté clairement, car elle peut accepter ou refuser chaque finalité spécifique ».
- Commission d'accès à l'information (CAI), *Lignes directrices 2023-1 – Consentement : critères de validité, version 1.0*. 31 octobre 2023. p. 4.
40. Certaines campagnes d'utilisateurs mobilisent le pouvoir que leur confère leur position de contributeur des données. Ainsi, ils exercent un levier sur les données (*data leverage*), par exemple au travers de la *contribution consciente aux données (conscious data contribution)* ou de *grèves de données*. Ces formes de militantisme numérique peuvent, à certains égards, porter des revendications d'autodétermination collective. Voir : Vincent, N. et Hecht, B. « Can "Conscious Data Contribution" Help Users to Exert "Data Leverage" Against Technology Companies? ». *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, n°CSCW1, 2021. DOI : [10.1145/3449177](https://doi.org/10.1145/3449177)
41. Dans son rapport quinquennal, la CAI invite à « une vaste réflexion sur l'avenir de la protection des renseignements personnels ». Cet appel à la réflexion collective s'inscrit dans une démarche d'autodétermination collective et de protection de la démocratie.
- Commission d'accès à l'information (CAI), *Transparence et vie privée : protéger la démocratie à l'ère numérique. Rapport quinquennal 2026*. Commission d'accès à l'information, 2026, p. 272.

42. Acronyme des géants du Web : Google, Apple, Facebook, Amazon et Microsoft.
43. Commission de l'éthique en science et technologie (CEST). *Regard éthique sur les effets environnementaux des technologies numériques au Québec : l'impératif de la sobriété numérique*, 2024.
44. Véliz, C. « The Surveillance Delusion? ». dans Véliz, C. (éd.), *Oxford Handbook of Digital Ethics*. Oxford University Press, 2021.
Cofone, I., *The Privacy Fallacy: Harm and Power in the Information Economy*. Cambridge University Press, 2023.
45. Commission de l'éthique en science et en technologie (CEST). *L'Internet des objets, la vie privée et la surveillance – Balises éthiques et recommandations*. 2020. p. 10.
46. Zhu, C. « Parents are finding new ways to monitor their kids. But some experts are concerned ». *CBC*, 23 septembre 2024. <https://www.cbc.ca/radio/thecurrent/parenting-surveillance-concerns-1.7329667>
47. Même cette donnée sur le sentiment de sécurité renforcé par le partage de localisation doit être considérée avec retenue, puisqu'elle résulte notamment d'une étude menée par *Life360*. Voir Beaulieu, C. « Partager sa localisation : entre praticité et intrusion ». *Urbania*, 20 octobre 2025. <https://urbania.ca/article/partager-sa-localisation-entre-praticite-et-intrusion>
48. *Ibid.*
49. L'ensemble de ces considérations peut s'inscrire dans une réflexion plus large sur le statut politique et moral des enfants et des adolescents. Voir par exemple :
Liebel, M. et Meade, P. *Adulthood: A Critical Introduction to Discrimination against children*. University of Bristol Press, 2026.
50. Hughes, A. « Location sharing is part of social life with Gen Z – but it can take a mental toll ». *CBC*, 16 août 2025. <https://www.cbc.ca/news/entertainment/instagram-location-sharing-1.7610355>
51. Quinlan, K. et Koeber, J. « Location Sharing Survey: 62 % of Americans Share Locations, Many Regret It ». *All About Cookies*, 1^{er} mai 2026. <https://allaboutcookies.org/location-sharing-survey>
52. Dimond, J. P., Fiesler, C. et Bruckman, A.S. « Domestic violence and information communication technologies ». *Interacting with Computers*, vol. 23, n°5, p. 413-421, 2011. DOI : <https://doi.org/10.1016/j.intcom.2011.04.006>
Dragiewicz, M. et al. « Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms ». *Feminist Media Studies*, vol. 18, n° 4, p. 609-625, 2018. DOI : <https://doi.org/10.1080/14680777.2018.1447341>
Landry, A. « La technologie, l'arme invisible pointée sur les victimes de violence conjugale ». *Radio Canada*, 4 décembre 2022. <https://ici.radio-canada.ca/recit-numerique/4979/technologie-victimes-violence-conjugale>
Corbeil, R. « La technologie comme arme de contrôle ». *La Gazette des femmes*, 13 novembre 2025. <https://gazettedesfemmes.ca/25692/la-technologie-comme-arme-de-contrôle/>
53. Marin, S. « Traque technologique : les refuges pour femmes victimes de violence contre-attaquent ». *Le Devoir*, 3 avril 2023. <https://www.ledevoir.com/actualites/societe/787730/traque-technologique-traque-technologique-les-refuges-pour-femmes-victimes-de-violence-contre-attaquent>
54. Privacy4Cars, « Free Privacy and Safety Resources for Survivors ». *Privacy4Cars*, consulté le 29 juin 2026. <https://privacy4cars.com/survivor-abuse-guide/>
55. Kourinian, A. « New state laws protect abuse survivors from misuse of vehicle connectivity ». *IAPP*, 14 juillet 2025. <https://iapp.org/news/a/new-state-laws-protect-abuse-survivors-from-misuse-of-vehicle-connectivity>
56. Morasse, M.-E. et Bourquin, C. Dossier « Danger des camions lourds. Objectif : freiner l'hécatombe » (2 articles). *La Presse*, 10 octobre 2025. <https://www.lapresse.ca/actualites/danger-des-camions-lourds/objectif-freiner-l-hecatombe/2025-10-10/la-technologie-pour-prevenir-des-tragedies.php>
57. Commission de l'éthique en science et en technologie (CEST). *La gestion algorithmique de la main-d'œuvre : analyse des enjeux éthiques*, 2023. p. 44.

58. L'arrêt Bridgestone Firestone concerne un cas de filature, mais les trois principes établis sont pertinents pour les autres formes de surveillance : les motifs doivent être sérieux, nécessaires et raisonnables. Voir par exemple : *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (csn) c. Trudeau*, 1999 CanLII 13295 (QC CA) ; *Hydro-Québec et Syndicat des employé-e-s de techniques et de bureau d'Hydro-Québec (SCFP-FTQ, section locale 2000)*.

Proulx, B. « Surveillance des données GPS par l'employeur – un outil controversé ». *RBD Avocats*, 28 octobre 2025. <https://rbdavocats.com/surveillance-des-donnees-gps-par-employeur-un-outil-controverse/>

Cain Lamarre, « Un arbitre reconnaît la légalité de systèmes de surveillance GPS installés sur les véhicules de l'entreprise ». *Cain-Lamarre*, 19 juillet 2024. <https://cainlamarre.ca/ressources/publications/un-arbitre-reconnait-la-legalite-de-systemes-de-surveillance-gps-installes-sur-les-vehicules-de-lentreprise/>

Commission d'accès à l'information (CAI), Décision 13859380 Canada Inc., 20 mai 2025.
59. Commission de l'éthique en science et en technologie (CEST). *La gestion algorithmique de la main-d'œuvre : analyse des enjeux éthiques*. 2023. p. 49. L'avis cite Charbonneau, É. et Doberstein, C., « COVID-19 et l'avenir de la surveillance du travail dans le secteur public », *A+, le carrefour des acteurs publics*, vol. 7, n° 2, 2020.
60. Vakulov, A. « Cybersecurity Threats to Modern Cars: How Hackers Are Taking Control ». *Forbes*, 25 janvier 2025. <https://www.forbes.com/sites/alexvakulov/2025/01/25/cybersecurity-threats-to-modern-cars-how-hackers-are-taking-control/>
61. Upstream Security Ltd. *Mind the Cybergap: Automotive & Smart Mobility Global Cybersecurity Report*, 2025.
62. Curry, S. « Hacking Subaru: Tracking and Controlling Cars via the STARLINK Admin Panel ». *Sam Curry*, 23 janvier 2025. <https://samcurry.net/hacking-subaru>
63. Upstream Security Ltd. *Mind the Cybergap: Automotive & Smart Mobility Global Cybersecurity Report*, 2025.
64. Union des consommateurs. *Voitures connectées : les consommateurs risquent-ils de perdre le contrôle?*, 4 décembre 2025.
65. *Ibid.*, p. 5.
66. *Ibid.*, p. 58.
67. Union des consommateurs. *Sommaire du rapport final du projet de recherche. Voitures connectées : les consommateurs risquent-ils de perdre le contrôle ?*, 4 décembre 2025.
68. Ben Shahr, O. « Privacy Protection, At What Cost? Exploring the Regulatory Resistance to Data Technology in Auto Insurance ». *Journal of Legal Analysis*, vol. 15, n°1, p. 129-157, 2023. DOI: <https://doi.org/10.1093/jla/laad008> ; Jaynes, C. « Telematics bill could change how insurance rates are calculated ». *CapitolWeekly*, 23 avril 2026. <https://capitolweekly.net/telematics-bill-could-change-how-insurance-rates-are-calculated/>
69. Gordon, B. « NC Answers: Why are some safe driving insurance discounts not allowed in North Carolina ». *Citizen Times*, 16 mars 2022. <https://www.citizen-times.com/story/news/2022/03/16/north-carolina-safe-driver-insurance-discounts-limited-driving-laws-nc-progressive-rates-state-farm/9416668002/> ; Tom Needham Insurance Agency, « Insuring Your Electric Vehicle in North Carolina: 2025 Costs, Discounts & Telematics Hacks ». *Tom Needham Insurance Agency*, 14 juillet 2025. <https://tomneedhaminsurance.com/insuring-your-electric-vehicle-in-north-carolina-2025-costs-discounts-telematics-hacks/> ; Martin, R. « Car Insurance with Telematics ». *The Zebra*, 12 mai 2026. <https://www.thezebra.com/auto-insurance/policies/car-insurance-telematics/>
70. Rosanes, M. « Usage-based car insurance – the pros and cons ». *Insurance Business*, 31 janvier 2022. <https://www.insurancebusinessmag.com/ca/news/automotor/usagebased-car-insurance--the-pros-and-cons-323737.aspx>
71. McKale, S. « Is usage-based car insurance right for you? ». *Square One*, 18 septembre 2025. <https://www.squareone.ca/resource-centres/car-insurance/usage-based-insurance>
72. Ben Shahr, O. « Privacy Protection, At What Cost? Exploring the Regulatory Resistance to Data Technology in Auto Insurance ». *Journal of Legal Analysis*, vol. 15, n°1, p. 129-157, 2023. DOI : <https://doi.org/10.1093/jla/laad008>

73. Waddell, K. « What You're Giving Up When You Let Your Car Insurer Track You In Exchange for Discounts ». *ConsumerReports*, 7 octobre 2021. <https://www.consumerreports.org/money/car-insurance/how-car-insurance-telematics-discounts-really-work-a1549580662/>

Kravitz, D. « Your Car May Be Spying On You. Here's How to Get It to Stop ». *ConsumerReports*, 4 mars 2025. <https://www.consumerreports.org/electronics/personal-information/how-to-stop-your-car-from-collecting-sharing-driving-data-a1233378612/>
74. Waddell, K. « What You're Giving Up When You Let Your Car Insurer Track You In Exchange for Discounts ». *ConsumerReports*, 7 octobre 2021. <https://www.consumerreports.org/money/car-insurance/how-car-insurance-telematics-discounts-really-work-a1549580662/>

Orosz, M. « Telematics Insurance: Pay less for safer driving ». *iSure*, 5 février 2026. <https://isure.ca/inews/telematics-insurance-better-premiums-safer-roads/>
75. Commission de l'éthique en science et en technologie (CEST). *Regard éthique sur les effets environnementaux des technologies numériques au Québec : l'impératif de la sobriété numérique*, 2024.
76. *Ibid.*
77. Corneau, M. « La face sombre des centres de données ». *Radio-Canada*, 5 avril 2025. <https://ici.radio-canada.ca/recit-numerique/12404/centres-donnees-energie-decouverte>
78. Baldé, C.P. et al. *Rapport mondial sur les déchets d'équipements électriques et électroniques*. 2024.
79. Commission de l'éthique en science et en technologie (CEST). *Regard éthique sur les effets environnementaux des technologies numériques au Québec : l'impératif de la sobriété numérique*, 2024. p. 38.
80. The Shift Project. « Climat : l'insoutenable usage de la vidéo en ligne ». *The Shift Project*, 2019. <https://theshiftproject.org/publications/climat-insoutenable-usage-video/>
81. Commission de l'éthique en science et en technologie (CEST). *Regard éthique sur les effets environnementaux des technologies numériques au Québec : l'impératif de la sobriété numérique*, 2024. p. 34.
82. Commission de l'éthique en science et en technologie (CEST). *Regard éthique sur les effets environnementaux des technologies numériques au Québec : l'impératif de la sobriété numérique*, 2024. p. 38.
83. Gouvernement du Canada, « Accès légal ». *Gouvernement du Canada*, 23 juin 2026. <https://www.canada.ca/fr/services/police/servicespolice/crime-prevention-du-crime/acces-legal.html>
84. GRC en C.-B. « Services de criminalistique numérique ». *Gendarmerie Royale du Canada*, 28 juillet 2025. <https://grc.ca/fr/cb/services-police/services-criminalistique-numerique>
85. Happer, A. « Motor Vehicle Data – Ownership and Accessibility ». *CEP Forensic*, 26 mars 2024. <https://cep-experts.ca/motor-vehicle-data-ownership-and-accessibility/>
86. Par exemple, les services de police doivent avoir le consentement du ou de la propriétaire ou une autorisation judiciaire pour obtenir des images et vidéos de crimes captés par les caméras de voitures Tesla. Cela a été le cas, par exemple, à la suite de vandalisme sur un véhicule Tesla (avec consentement) ou dans le cadre d'une enquête pour homicide (avec mandat de perquisition). Voir : Klender, J. « Tensla Sentry Mode captures another keying incident, this time in Canada ». *Teslarati*, 12 octobre 2019. <https://www.teslarati.com/tesla-sentry-mode-captures-another-keying-incident-this-time-in-canada/>

Wilson, M. « Oakland Police Attempt to Seize Canadian's Tesla to Access Possible Sentry Mode Crime Footage ». *Drive Tesla Canada*, 2 septembre 2024. <https://driveteslacanada.ca/news/oakland-police-attempt-to-seize-canadians-tesla-to-access-possible-sentry-mode-crime-footage/>
87. Tran, S. « No Reasonable Expectation Of Privacy In Vehicle Black Box Data In Ontario ». *Deeth Williams Wall*, 18 septembre 2024. <https://www.dww.com/articles/no-reasonable-expectation-of-privacy-vehicle-black-box-data-ontario>

Carolino, B. « Ontario Court of Appeal admits event data recorder evidence in car accident case ». *Law Times*, 1^{er} septembre 2024. <https://www.lawtimesnews.com/practice-areas/personal-injury/ontario-court-of-appeal-admits-event-data-recorder-evidence-in-car-accident-case/388250>

88. Voir les articles 487.014 à 487.018 du *Code criminel* du Canada, L.R.C. 1985, c. C-46.
89. Barrison & Manitus. « The Digital Dragnet: Ten Realities of Electronic Privacy Law ». *Barrison & Manitus*, consulté le 29 juin 2026. <https://criminallawoshawa.com/the-digital-dragnet-ten-realities-of-electronic-privacy-law/>
90. Pinsonnault, G. « La Cour supérieure du Québec conclut que les entreprises devront communiquer des renseignements aux policiers – même des données stockées à l'étranger ». *McMillan*, 24 janvier 2023. <https://mcmillan.ca/fr/perspectives/publications/la-cour-superieure-du-quebec-conclut-que-les-entreprises-devront-communiquer-des-renseignements-aux-policiers-meme-des-donnees-stockees-a-letranger/>
91. Querry, Q. et Kolos, N. « Canadian case law trending to compel production of data by foreign corporations to Canadian law enforcement ». *Mccarthy Tétrault*, 4 mai 2023. <https://www.mccarthy.ca/en/insights/blogs/canadian-appeals-monitor/canadian-case-law-trending-to-compel-production-of-data-by-foreign-corporations-to-canadian-law-enforcement>
92. Mostowfi, M. « Expanding the scope of production orders: Virtual presence brings data around the world into the purview of Canadian law enforcement ». *Dentons Commercial Litigation Blog*, 15 novembre 2023. <https://www.commerciallitigationblog.com/expanding-the-scope-of-production-orders-virtual-presence-brings-data-around-the-world-into-the-purview-of-canadian-law-enforcement/>
93. Solon, O. « Insecure wheels: Police turn to car data to destroy suspects' alibis ». *NBC News*, 28 décembre 2020. <https://www.nbcnews.com/tech/tech-news/snitches-wheels-police-turn-car-data-destroy-suspects-alibis-n1251939>

Schooley, M., Riley, N. et Rex, K. « Karen Read trial expert questioned over Lexus data, professional credentials ». *CBS News*, 20 mai 2025. <https://www.cbsnews.com/boston/news/karen-read-trial-live-today-day-19-shanon-burgess/>

Vargas, E. « Parked Tesla turns star witness in Oakland encampment killing ». *hoodline*, 5 mai 2026. <https://hoodline.com/2026/05/parked-tesla-turns-star-witness-in-oakland-encampment-killing/>
94. Díaz, Á. « When Police Surveillance Meets the "Internet of Things" ». *Brennan Center for Justice*, 13 décembre 2020. <https://www.brennancenter.org/our-work/research-reports/when-police-surveillance-meets-internet-things>
95. Gouvernement du Québec, « Critères de validité d'un consentement ». *Gouvernement du Québec*, 20 octobre 2025. <https://www.quebec.ca/gouvernement/travailler-gouvernement/normes-gouvernance-pratiques-internes/protection-des-renseignements-personnels/consentement/validite-dun-consentement>

Commissariat à la protection de la vie privée du Canada, « Lignes directrices pour l'obtention d'un consentement viable ». *Commissariat à la protection de la vie privée du Canada*, 11 août 2025. https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les-entreprises/collecte-de-renseignements-personnels/consentement/gl_omc_201805/
96. Thurton, D. « A trade war with China over EVs could slow Canada's low-carbon transition, group warns ». *CBC*, 30 juin 2024. <https://www.cbc.ca/news/politics/electric-vehicles-china-canada-trade-tariffs-1.7250503>
97. La Presse canadienne. « Carney conclut un accord avec la Chine sur les véhicules électriques et le canola ». *Radio-Canada*, 16 janvier 2026. <https://ici.radio-canada.ca/nouvelle/2221219/mark-carney-accord-chine-vehicules-electriques-canola-fruits-mer>
98. Lewis, J.A. « Connected Car and Spying ». *Center for Strategic & International Studies*, 1^{er} octobre 2024. <https://www.csis.org/analysis/connected-cars-and-spying>
99. Fixler, A. et McSween, K. « Poland Bans Chinese Cars From Military Sites Over Spying Fears ». *Foundation for Defense of Democracies*, consulté le 30 juin 2026. <https://www.fdd.org/analysis/2026/02/20/poland-bans-chinese-cars-from-military-sites-over-spying-fears/>
100. Levin, T. « China is reportedly restricting use of Tesla cars by its military and government workers ». *Business insider*, 19 mars 2021. <https://www.businessinsider.com/china-tesla-ban-military-government-personnel-2021-3>

101. Marshal, A. et Knight, W. « The White House Warns Cars Made in China Could Unleash Chaos on US Highways ». *Wired*, 29 février 2024. <https://www.wired.com/story/china-cars-national-security-threat-investigation/>
102. Bassler, H. « VERIFY: How much control does OnStar have over vehicles? ». *12 News*, 31 mars 2021. <https://www.12news.com/article/news/verify/verify-onstar-car-how-much-control-vehicle-police-pursuit/75-9ab58549-0c21-4dfc-9e68-c1a096efddce>
103. Stevens, T. « How OTA Updates Will Change Your Life for Better – and Worse ». *Motortrend*, 9 mars 2023. <https://www.motortrend.com/features/over-the-air-car-updates>
104. Agence France Presse. « Votre voiture vous espionne, selon une étude ». *Radio-Canada*, 7 septembre 2023. <https://ici.radio-canada.ca/nouvelle/2008741/voiture-donnees-personnelles-protection-tesla-nissan>
105. DiMarco, A. « Beyond Borders: Is our private data exposed to US surveillance? What the CLOUD Act and FISA mean for Canadian Data Sovereignty ». *Linkedin*, 6 avril 2025. <https://www.linkedin.com/pulse/beyond-borders-our-private-data-exposed-us-what-cloud-alex-dimarco-wjtnc/>
106. Joffe-Block, J. « Your data is everywhere. The government is buying it without a warrant ». *npr*, 25 mars 2026. <https://www.npr.org/2026/03/25/nx-s1-5752369/ice-surveillance-data-brokers-congress-anthropic>
107. Vivek, S. et al. « Cyber-physical risks of hacked Internet-connected vehicles ». *Physical Review E*, 2019. DOI: [10.1103/PhysRevE.100.012316](https://doi.org/10.1103/PhysRevE.100.012316)
108. Barr, L. « US to ban Russia, Chinese software and hardware in vehicles ». *abcnews*, 2025. <https://abcnews.com/Politics/us-ban-russian-chinese-software-hardware-vehicles/story?id=117627935>
109. Beaumier, G. « Véhicules électriques chinois : Le faux débat de la sécurité nationale ». *Options politiques*, 11 février 2026. <https://policyoptions.irpp.org/fr/2026/02/vehicules-electriques-chinois/>
110. Gerstein, J. et Cheney, K. « DOGE's access to federal data is 'an absolute nightmare', legal experts warn ». *Politico*, 2 mars 2025. <https://www.politico.com/news/2025/02/03/doge-treasury-usaid-donald-trump-011538>
111. Toh, M. « Elon Musk responds to spying concerns in China: Trust us, we're just like TikTok ». *CNN*, 22 mars 2021. <https://www.cnn.com/2021/03/22/tech/elon-musk-tesla-china-military-ban-intl-hnk>
112. Ekott, U., Che, Z. et Tantratian, A. « Connected Vehicles and Data Privacy & Sovereignty in the Global South ». *Tech Policy*, 23 octobre 2024. <https://www.techpolicy.press/connected-vehicles-and-data-privacy-sovereignty-in-the-global-south/>
113. *Ibid.*
114. Ministère des Transports et de la Mobilité durable, « Centre de gestion de l'équipement roulant (CGER) : notre offre de service », *Gouvernement du Québec*, consulté le 30 juin 2023. <https://www.transports.gouv.qc.ca/fr/services/cger/a-propos/Documents/Offre-services-CGER.pdf>

Ministère des Transports et de la Mobilité durable, *Politique gouvernementale d'acquisition des véhicules*, 2026. https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/transports/ministere-des-transport/publications-amd/Politiques_ministerielles/politique-gouvernementale-acquisition-des-vehicules.pdf
115. Partenariat données Québec, « Données Québec ». *Gouvernement du Québec*, consulté le 30 juin 2026. <https://www.donneesquebec.ca/>

Boudreau, C. « La réutilisation des données ouvertes au Québec : du développement économique à la transparence gouvernementale ». *Revue internationale des sciences administratives*, vol. 87, n°4, p. 771-789, 2021. DOI : <https://doi.org/10.3917/risa.874.0771>
116. Trudel, P. « Les données massives, ressources collectives des univers connectés ». Dans Biancalana, C. et Montigny, É., *Démocratie artificielle : les effets des mégadonnées sur la politique, la politique et les politiques*. Presses de l'Université Laval, 2025.
117. *Ibid.* p. 53.
118. Certaines données gouvernementales et municipales sont accessibles dans le portail *Données Québec*. Des organisations de la société civile (entreprises, OBNL) peuvent également rendre disponibles des jeux de données en format ouvert, sur une base volontaire.

119. Wong, W., Duncan, J. et Lake, D. « Why data about people are so hard to govern ». *Regulation & Governance*, vol. 19, 2025. DOI: <https://doi.org/10.1111/rego.12591>
120. Toutes les politiques de confidentialité consultées indiquaient que les données pourraient être transférées à l'international (ou autre formulation similaire) : faut-il en comprendre que c'est systématiquement le cas ? Ou bien les constructeurs incluent-ils une telle clause pour couvrir tous les cas de figure ? Il est difficile de le savoir.
121. On Star, « Politique de confidentialité ». On Star, consulté le 30 juin 2026. <https://www.onstar.ca/fr/legal/privacy-statement>
122. Union des consommateurs. *Voitures connectées : les consommateurs risquent-ils de perdre le contrôle?* Union des consommateurs, 4 décembre 2025. p. 88.
123. Commission d'accès à l'information (CAI), *Rédiger une politique de confidentialité – Guide explicatif pour les entreprises*, décembre 2023. p. 9-11.

Commission d'accès à l'information (CAI), *Lignes directrices 2023-1 – Consentement : critères de validité, version 1.0*, 31 octobre 2023. p.19-20.
124. McDonald, A. M. et Cranor, L. F. « The cost of reading privacy policies ». *Isjlp*, vol. 4, 2008.
125. Les autres réponses sont : ceux qui acceptent parfois des politiques de confidentialité sans les avoir lues (22 %), et ceux qui n'ont pas répondu ou n'utilisent pas internet (4 %).

McClain, C. et al. « How Americans View Data Privacy ». *Pew Research Center*, 18 octobre 2023. <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>
126. Chen, M, et Chen, M. « Trust, Privacy Fatigue, and the Informed Consent Dilemma in Mobile App Privacy Pop-Ups: A Grounded Theory Approach ». *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 20, n°3, 2025. DOI: <https://doi.org/10.3390/jtaer20030179>.

UX Magazine. « Consent Fatigue: Are We Designing People into Compliance ». *Medium*, 5 mai 2026. <https://uxmag.medium.com/consent-fatigue-are-we-designing-people-into-compliance-a04928cfba9f>
- Association du Barreau Canadien.
« Éviter la fatigue du consentement ». *ABC*, 26 septembre 2023. <https://cba.org/fr-ca/our-impact/cba-influence/avoiding-consent-fatigue/>
127. Union des consommateurs. *Voitures connectées : les consommateurs risquent-ils de perdre le contrôle?*, 4 décembre 2025. p. 75.
128. S'appuyant sur des arguments semblables, la CAI remet également en question le paradigme de l'autodétermination informationnelle, ou du contrôle individuel : « à la lumière des enjeux du monde numérique, la Commission doute que cette approche garantisse un niveau de protection satisfaisant de la vie privée, en particulier à la lumière de l'asymétrie de pouvoir qui existe entre les personnes et les organisations ».

Commission d'accès à l'information (CAI), *Transparence et vie privée : protéger la démocratie à l'ère numérique. Rapport quinquennal 2026*. Commission d'accès à l'information, 2026. p. 143.
129. Union des consommateurs. *Voitures connectées : les consommateurs risquent-ils de perdre le contrôle?*, 4 décembre 2025. p. 173.
130. Pour la CAI, bien que le critère de nécessité constitue une balise importante pour protéger le droit à la vie des personnes, il est trop souvent mal compris et appliqué de manières variables. Elle propose des recommandations pour améliorer sa compréhension et son opérationnalisation.

Commission d'accès à l'information (CAI), *Transparence et vie privée : protéger la démocratie à l'ère numérique. Rapport quinquennal 2026*. Commission d'accès à l'information, 2026.
131. *P-39.1 - Loi sur la protection des renseignements personnels dans le secteur privé*, art. 23 (1993, c. 17, a. 1 ; 2002, c. 19, a. 19 ; 2006, c. 22, a. 111 ; 2021, c. 25, a.100).
132. Commission d'accès à l'information (CAI), « Conservation et destruction des renseignements personnels ». *Commission d'accès à l'information*, consulté le 30 juin 2026. <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privées/conservation-destruction-renseignements-personnels>

133. Lubarsky, B. « Re-identification of "anonymized" data ». *Georgetown Law Technology Review*, 2017. <https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/>
134. Par exemple, la Politique de confidentialité d'Audi précise : « Dans la mesure où nous sommes autorisés à le faire en vertu des lois applicables, nous pouvons dépersonnaliser ou anonymiser vos renseignements personnels, et utiliser et divulguer ces informations dépersonnalisées ou anonymisées à quelque fin que ce soit (y compris pour développer, gérer et maintenir notre entreprise et nos affaires) sans autre préavis ».
- Audi Canada, « Politique de confidentialité d'Audi Canada ». *Audi Canada*, consulté le 30 juin 2026. <https://www.audi.ca/fr/models/q3/new-q3/2026/aperçu/#oneLayer=/fr/tools/navigation/layer/clause-de-non-responsabilite/confidentialite/>
135. C'est par exemple le cas des Évaluations de facteurs relatifs à la vie privée (EFVP) et de l'obligation de protection équivalente en matière de vie privée.
136. Kablan, S., Oulaï, A. et Mignault, P. « L'évaluation des facteurs relatifs à la vie privée : pour un équilibre entre l'objectif de protection des renseignements personnels et la responsabilité des entreprises ». *Les Cahiers de droit*, vol. 64, n°2, 2023. p. 397-437. <https://doi.org/10.7202/1101118ar>
- La CAI émet elle aussi des réserves quant à l'efficacité des EFVP et affirme « qu'il y a lieu de revoir la manière dont elle est codifiée dans les lois, le tout dans un objectif de clarté, de proportionnalité des efforts et de transparence ».
- Commission d'accès à l'information (CAI), *Transparence et vie privée : protéger la démocratie à l'ère numérique. Rapport quinquennal 2026*. Commission d'accès à l'information, 2026, p. 227-228.
137. Voir par exemple : Commission d'accès à l'information (CAI), *Transparence et vie privée : protéger la démocratie à l'ère numérique. Rapport quinquennal 2026*. Commission d'accès à l'information, 2026, p. 307-322.

Membres du comité d'expertes et d'experts

Ce rapport est une publication officielle de la Commission de l'éthique en science et en technologie. Pour son élaboration, la Commission s'est appuyée sur l'avis de personnes expertes. Elle préserve néanmoins son indépendance et les positions contenues dans ce rapport ne reflètent pas nécessairement les opinions des personnes consultées.

Présidence de la Commission

Luc Bégin

Professeur associé
Faculté de philosophie
Université Laval
Président de la Commission de l'éthique en science et en technologie

Sébastien Gambs

Professeur titulaire
Département d'informatique
Université du Québec à Montréal

Serge Kablan

Professeur titulaire
Département de management
Faculté des sciences de l'administration
Université Laval

Membres du comité d'expertes et d'experts

Ulrich Aïvodji

Professeur adjoint
Département de génie logiciel et TI
École de technologie supérieure

Guillaume Beaumier

Professeur adjoint
École nationale d'administration publique

Céline Castets-Renard

Professeure titulaire
Faculté de droit
Université d'Ottawa

Marc-Kevin Daoust

Professeur enseignant
Département des enseignements généraux
École de technologie supérieure

Commission de l'éthique en science et en technologie

Président

Luc Bégin

Professeur associé
Faculté de philosophie
Université Laval
Président de la Commission de l'éthique
en science et en technologie

Membres

Julie Cailliau

Directrice
Observatoire des tout-petits

Guillaume Chicoisne

Directeur des programmes scientifiques
Institut de valorisation des données (IVADO)

Nathalie de Marcellis-Warin

Professeure
Département de mathématiques et de génie
industriel
Polytechnique Montréal
Présidente-directrice générale, CIRANO

Miriam Fahmy

Conseillère en transfert des connaissances
Territoires innovants en économie sociale
et solidaire (TIESS)

Sébastien Gambs

Professeur
Département d'informatique
Université du Québec à Montréal

Caroline Jonnaert

Directrice
Avocate
Agente de marques et responsable
de la protection des données
Cabinet ROBIC

Éric Montpetit

Vice-Doyen
Professeur titulaire
Faculté des arts et des sciences
Université de Montréal

Quoc Dinh Nguyen

Gériatre, épidémiologiste et chercheur
Centre hospitalier de l'Université de Montréal

Nathalie Orr Gaucher

Médecin d'urgence pédiatrique
Centre hospitalier universitaire Sainte Justine

Daniel Weinstock

Vice-doyen à la recherche et professeur
Faculté de droit
Université McGill

Observatrice

Annie Blouin

Directrice
Direction du soutien aux organisations
Ministère de l'Économie, de l'Innovation
et de l'Énergie



Commission
de l'éthique
en science
et en technologie

Québec

