

RAPPORT FINAL DU PROJET DE RECHERCHE

VOITURES CONNECTÉES : LES CONSOMMATEURS RISQUENT-ILS DE PERDRE LE CONTRÔLE ?

4 décembre 2025

Union des consommateurs a reçu du financement en vertu du Programme de contributions pour les organisations sans but lucratif de consommateurs et de bénévoles d'Innovation, Sciences et Développement économique Canada. Les opinions exprimées dans ce rapport ne sont pas nécessairement celles d'Innovation, Sciences et Développement économique Canada ou du gouvernement du Canada.

union
des consommateurs

UNION DES CONSOMMATEURS, LA FORCE D'UN RÉSEAU

Union des consommateurs est un organisme à but non lucratif qui regroupe 16 groupes de défense des droits des consommateurs. La mission d'Union des consommateurs est de représenter et défendre les droits des consommateurs, en prenant en compte de façon particulière les intérêts des ménages à revenu modeste. Les interventions d'Union s'articulent autour des valeurs chères à ses membres : la solidarité, l'équité et la justice sociale, ainsi que l'amélioration des conditions de vie des consommateurs aux plans économique, social, politique et environnemental.

NOTRE VISION

La structure d'Union des consommateurs lui permet de maintenir une vision large des enjeux de consommation tout en développant une expertise pointue dans certains secteurs d'intervention, notamment par ses travaux de recherche sur les nouvelles problématiques auxquelles les consommateurs doivent faire face ; ses actions, de portée nationale, sont alimentées et légitimées par le travail terrain et l'enracinement des associations membres dans leur communauté.

NOTRE MISSION

Union des consommateurs agit principalement sur la scène nationale, en représentant les intérêts des consommateurs auprès de diverses instances politiques ou réglementaires, sur la place publique ou encore par des recours collectifs. Parmi ses dossiers privilégiés de recherche, d'action et de représentation, mentionnons le budget familial et l'endettement, l'énergie, les questions liées à la téléphonie, la radiodiffusion, la télédistribution et Internet, la santé, les produits et services financiers ainsi que les politiques sociales et fiscales.



Table des matières

1	Introduction	5
2	La voiture connectée	7
2.1	Définition de la voiture connectée	7
2.2	L'omniprésence de la connectivité.....	8
2.3	Technologies présentes dans la voiture connectée	9
2.4	Données générées, collectées et communiquées par la voiture connectée.....	15
2.5	Fonctionnalités connectées.....	19
2.6	Autres utilisations des technologies connectées	22
2.7	Faits saillants	26
3	Quels risques pour les consommateurs ?.....	27
3.1	Risques et enjeux pour la vie privée.....	27
3.2	Atteinte au droit de propriété	45
3.3	Atteinte au droit à la réparation	54
3.4	Risques liés à la sécurité du véhicule (vol, cybersécurité).....	64
3.5	Faits saillants	67
4	La parole aux consommateurs	70
4.1	Faits saillants du sondage	71
4.2	Faits saillants des entrevues	77
4.3	Analyse	84
4.4	Faits saillants	88
5	L'adéquation de la législation canadienne	90
5.1	La protection de la vie privée et des renseignements personnels : l'encadrement législatif	90
5.2	Analyse : adéquation de l'encadrement de la protection de la vie privée.....	99
5.3	Le droit de propriété et le droit à la réparation dans le contexte numérique...	109
5.4	Analyse : adéquation de l'encadrement du droit de propriété	119
5.5	Vers un droit à la réparation canadien ? Le droit à la réparation au Québec..	122
5.6	Le cadre législatif international	127
5.7	Faits saillants	134
6	Analyse de données fournies par l'industrie	138
6.1	Introduction et méthodologie	138
6.2	Présentation des services connectés sur le site Web	138

6.3	Conditions d'utilisation : les documents examinés.....	141
6.4	Politique de confidentialité.....	143
6.5	Conditions affectant le droit de propriété de l'utilisateur.....	147
6.6	Faits saillants	150
7	Point de vue des parties prenantes et des experts	152
7.1	Introduction	152
7.2	La protection de la vie privée	153
7.3	Droits de propriété, droit à la réparation et la protection des consommateurs	157
7.4	Faits saillants	167
8	Conclusions et recommandations	169
8.1	Conclusions	169
8.2	Recommandations	171

1 Introduction

La voiture est l'un des biens de consommation les plus importants. Important en termes de coûts : qu'elles soient louées, achetées neuves ou d'occasion, les paiements de voiture représentent une dépense importante pour les consommateurs. Important aussi quant à sa fonction : pour plusieurs, la voiture est essentielle pour se rendre au travail, emmener les enfants à l'école, faire des courses et se déplacer. Pour de nombreuses personnes au Canada, la vie quotidienne n'est pas possible sans voiture.

Les voitures évoluent aujourd'hui d'une manière qui présente des risques graves et urgents pour les consommateurs. Aujourd'hui, les voitures sont de plus en plus « connectées ». La plupart des nouvelles voitures vendues au Canada sont équipées de dispositifs technologiques qui permettent la connexion à Internet ou à un réseau cellulaire. Cette connectivité permet aux véhicules d'envoyer au fabricant des données, y compris des renseignements personnels de l'utilisateur, des renseignements sur le véhicule et des données de diagnostic ou de réparation, et ce, sans l'intervention du propriétaire du véhicule. Elle permet également au véhicule de recevoir des données, ce qui permet au fabricant ou à l'utilisateur de contrôler à distance certaines de ses fonctionnalités.

Certes, la connectivité permet une variété de nouvelles activités utiles : navigation en direct, contrôle à distance de certaines fonctions (chauffage, déverrouillage, démarrage, etc.), appel des services d'urgence automatique en cas d'accident, création des points d'accès Wi-Fi dans la voiture, options de divertissement connectées, etc.

Mais la connectivité présente aussi des risques. Elle permet l'intrusion dans la vie privée de l'utilisateur, car la voiture connectée peut collecter et communiquer une quantité massive de données sur l'utilisateur au fabricant. Ce dernier peut partager ces données avec des tiers tels que des assureurs, des courtiers en données, des partenaires marketing et ainsi de suite. Il existe aussi des risques de piratage et de fuites de données. De plus, la connectivité a un impact sur le droit de propriété du consommateur sur sa voiture. Même après l'acquisition d'une voiture connectée par le consommateur, le fabricant retient un contrôle important sur le bien, étant capable de le mettre à jour à distance, de bloquer ou débloquer des fonctionnalités et de limiter ce qui peut être fait avec son logiciel. Cela permet non seulement au fabricant de modifier l'offre de service après l'acquisition du véhicule, mais cela peut également avoir un impact sur la réparation.

La technologie est en constante évolution et elle est utilisée à diverses fins : pour personnaliser les primes d'assurance, pour permettre aux créanciers de localiser les véhicules des débiteurs en cas de retard de paiement, pour exiger le paiement d'un abonnement pour l'accès à certaines fonctions de la voiture, pour diagnostiquer et même réparer certains problèmes à distance, et ainsi de suite.

Compte tenu de l'importance de leurs véhicules pour les consommateurs et de l'essor important de la connectivité dans les véhicules dans les années récentes, nous avons choisi d'examiner et d'évaluer les risques posés par la connectivité sur les droits des consommateurs et de déterminer de quelle manière ces conséquences peuvent être atténuées.

Notre recherche s'est concentrée sur les risques posés aux droits à la vie privée des consommateurs et à leurs droits de propriété, y compris le droit à la réparation.

Pour ce faire, nous avons effectué :

- une revue de la littérature ;
- un sondage auprès de plus de 1 000 consommateurs canadiens ;
- des entrevues avec des consommateurs qui possèdent des véhicules connectés ;
- un examen de l'encadrement législatif fédéral et provincial canadien concernant la protection de la vie privée, la propriété intellectuelle et le droit à la réparation ;
- un survol des cadres juridiques internationaux concernant spécifiquement les véhicules connectés ;
- une analyse des sites Web et des conditions de service de trois fabricants (Toyota, Tesla, Ford) ;
- des entrevues avec trois experts en matière de réparation de véhicule ;
- des entrevues avec intervenants en plusieurs domaines, notamment le droit de la consommation, de la vie privée et à la réparation.

Quelques sujets ne sont pas abordés dans ce rapport. D'abord, nous ne faisons aucun commentaire sur l'électrification des véhicules. Une voiture connectée peut être électrique, à essence ou hybride. Nous ne traitons pas non plus des questions liées à la conduite autonome, bien que certains véhicules connectés aient cette capacité. Les risques liés à la conduite autonome sont largement distincts des risques liés à la connectivité. Néanmoins, les constats de la recherche s'appliquent à l'aspect connecté des véhicules autonomes.

Ce rapport se concentre exclusivement sur l'impact de la connectivité sur les consommateurs. Il ne s'intéresse donc pas non plus aux activités commerciales telles que la gestion de flotte ni aux activités étatiques telles que le développement des systèmes de transport intelligents.

Enfin, les questions du vol et du piratage des véhicules dépassent largement le cadre de ce rapport. Nous n'abordons ces questions que lorsqu'elles sont liées à la protection de la vie privée et aux droits de propriété.

2 La voiture connectée

Cette section présente la notion de voiture connectée : qu'est-ce qu'une voiture « connectée » ? Quelles sont les technologies qui permettent la connectivité et qui sont présentes dans ces voitures ? Quels types de données une voiture connectée peut-elle générer, collecter et communiquer ? Quelles fonctionnalités et utilisations la connectivité permet-elle ?

2.1 Définition de la voiture connectée

Il existe plusieurs définitions de véhicule connecté ou de voiture connectée. Une notion est commune à toutes les définitions : une voiture connectée est une voiture qui peut communiquer sans fil avec le monde extérieur¹. Dans ce rapport, nous définirons une voiture connectée comme **toute voiture pouvant recevoir ou envoyer des données via un réseau cellulaire ou l'Internet.**

Cette définition large englobe une vaste gamme de véhicules, y compris les premières voitures équipées de la capacité de passer des appels ou d'envoyer des SMS en cas d'accident routier, jusqu'aux voitures les plus modernes qui sont capables d'envoyer des téraoctets de données par Internet chaque jour. Cependant, cette définition exclut les véhicules qui sont « connectés » au monde extérieur uniquement par l'intermédiaire d'un dispositif externe, tel qu'un téléphone cellulaire. Une voiture connectée est une voiture dotée d'une capacité de communiquer **directement** par le réseau mobile ou par l'Internet. Il est également important de noter que cette définition n'inclut pas les véhicules qui reçoivent des signaux GPS ou d'autres signaux satellites, mais qui n'ont aucune autre forme de connectivité².

¹ Par ex., OFFICE QUEBECOIS DE LA LANGUE FRANÇAISE, « Voiture connectée », *Grand dictionnaire terminologique* (2017), en ligne : <<https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8869106/voiture-connectee>> (consulté le 13 février 2025); TRANSPORTS CANADA, « Véhicules connectés et automatisés » (10 février 2025), en ligne : <<https://tc.canada.ca/fr/transport-routier/technologies-novatrices/vehicules-connectes-automatisees>> (consulté le 13 février 2025); U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), « Vehicle Data Privacy: Industry and Federal Efforts Under Way but NHTSA Needs to Define Its Role » (2017), en ligne : <<https://www.gao.gov/products/gao-17-656>> (consulté le 21 octobre 2024); Jed CHONG, *Automated and connected vehicles: status of the technology and key policy issues for Canadian Governments*, 2016-98-E, Ottawa, Library of Parliament, 2016, p. 1, en ligne : <<https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/BackgroundPapers/PDF/2016-98-e.pdf>>; Zaigham MAHMOOD, *Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks for the IoV*, Cham, Springer International Publishing AG, 2020, p. 5.

² Une voiture équipée d'un récepteur de signaux satellites, y compris un récepteur GPS, peut bien sûr être une voiture connectée, mais seulement si elle est connectée à un réseau mobile ou à Internet. Un véhicule doté seulement d'un système satellite, comme le GPS, reçoit un signal

Tout type d'automobile, que ce soit une voiture à essence, électrique ou hybride, est connecté s'il répond à cette définition.

2.2 L'omniprésence de la connectivité

Au cours de la dernière décennie, la connectivité est devenue de plus en plus courante dans les voitures, et n'est plus une fonctionnalité réservée aux véhicules de luxe. Elle devient même rapidement omniprésente. Dans son rapport de 2017, le *Government Accountability Office* (GAO) des États-Unis a constaté que treize des seize fabricants automobiles les plus populaires au pays vendaient des véhicules connectés et que quatre d'entre eux fournissaient des services connectés dans tous leurs véhicules³. En 2018, Ford a annoncé que tous ses nouveaux véhicules vendus en Amérique du Nord seraient dotés d'une capacité de se connecter au réseau cellulaire 4G, pour ne citer qu'un exemple⁴. Par l'année 2020, environ 91 % des nouvelles voitures vendues aux États-Unis ont été dotées d'un certain degré de connectivité⁵. Selon une estimation, 95 % des nouveaux véhicules vendus dans le monde seront connectés d'ici 2030⁶.

Parallèlement, les fonctions connectées deviennent omniprésentes. Pour ne prendre que deux exemples sur le marché canadien, nous avons observé que tous les modèles 2024 et 2025 figurant sur le site Web de Toyota Canada en septembre 2024 étaient équipés de la fonctionnalité *Remote Connect*, qui permet aux utilisateurs de déverrouiller les portes, de démarrer ou d'arrêter le moteur à partir d'une application mobile⁷. En 2024, GM a annoncé que tous ses véhicules de 2025 sont maintenant équipés des fonctions de base de son service connecté OnStar⁸.

satellite et calcule sa position en fonction de celui-ci, mais n'envoie pas d'information au monde extérieur. Dans un véhicule non connecté, aucune information ne quitte le véhicule.

³ U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), préc., note 1, p. 10.

⁴ FORD MEDIA CENTER, « Ford Readies North America's Freshest Lineup by 2020 with Onslaught of Connected New Trucks, SUVs and Hybrids » (2018), en ligne :

<<https://media.ford.com/content/fordmedia/fna/us/en/news/2018/03/15/ford-readies-north-americas-freshest-lineup-by-2020.html>> (consulté le 13 mars 2025).

⁵ ABI RESEARCH, « The Connected Car Market Will Endure a 15% Shipment Decline, Flat Revenues in 2020; Sales Return on Trend Early 2022 » (2020), en ligne :

<<https://www.prnewswire.com/news-releases/the-connected-car-market-will-endure-a-15-shipment-decline-flat-revenues-in-2020-sales-return-on-trend-early-2022-301100761.html>> (consulté le 13 mars 2025).

⁶ Michele BERTONCELLO, Christopher MARTENS, Timo MOLLER et Tobias SCHNEIDERBAUER, « Unlocking full value from data from connected cars », *McKinsey & Company* (2021), en ligne : <<https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data>> (consulté le 13 mars 2025).

⁷ TOYOTA CANADA, « Multimédia et Services connectés », en ligne :

<<https://www.toyota.ca/fr/discover/connected-services/multimedia/>> (consulté le 13 mars 2025).

⁸ « Tous les véhicules 2025 sont maintenant équipés des fonctions de base OnStar », en ligne : <<https://www.onstar.ca/fr/standard-content>> (consulté le 13 mars 2025).

2.3 Technologies présentes dans la voiture connectée

La voiture connectée moderne est le produit de deux tendances technologiques : l'intégration croissante des composants électroniques dans la voiture - aujourd'hui, les ordinateurs - et l'augmentation de la connectivité avec le monde extérieur. Dans cette section, nous examinerons l'évolution de cette technologie.

2.3.1 L'intégration de composantes électroniques et de systèmes de diagnostic à la voiture

On doit remonter aux 1970s pour voir l'intégration des premiers appareils électroniques à l'architecture d'une voiture. Ces appareils ont été initialement conçus pour surveiller la performance du moteur. Des préoccupations d'ordre environnemental ont accéléré ce processus et ont poussé l'industrie automobile à intégrer de plus en plus de fonctions électroniques aux nouveaux véhicules, permettant ainsi le contrôle des émissions de polluants atmosphériques⁹. La technologie a, dès le départ, été utilisée à d'autres fins que le contrôle des émissions liées aux fonctions du moteur. En 1980, General Motors a commencé à utiliser un convertisseur catalytique contrôlé par ordinateur, qui permettait non seulement de contrôler les émissions polluantes, mais avait aussi des fonctions d'autodiagnostic. Au milieu des années 80, plusieurs constructeurs automobiles avaient aussi emboîté le pas et créé leur propre système de contrôle du moteur et de diagnostic par ordinateur¹⁰.

À la fin des années 80, les ordinateurs jouaient un rôle important dans les automobiles comme systèmes électroniques de gestion du moteur¹¹. Déjà, à cette époque, les automobiles sont équipées de plusieurs capteurs et unités de commande électronique (ECU, pour l'acronyme anglais de « *electronic control unit* »), c'est-à-dire de petits ordinateurs dans l'automobile permettant l'activation d'opérations particulières¹². Comme la communication efficace entre les différents ECU nécessitait un protocole de communication, le *Controller Area Network* (CAN), fut inventé au début des années 80 et

⁹ M. FORELLE, « The material consequences of “chipification”: The case of software-embedded cars », (2022) 9-1 *Big Data Soc.*, 5, en ligne : <<https://doi.org/10.1177/20539517221095429>>; L'introduction, en 1970, du Clean Air Act (CAA) par le Congrès américain avait pour objectif d'améliorer la qualité de l'air et visait spécifiquement le secteur automobile. En effet, l'utilisation croissante du véhicule à moteur était désignée comme un contributeur direct à l'augmentation de la pollution de l'air aux États-Unis : UNITED STATES ENVIRONMENTAL PROTECTION AGENCY, « Clean Air Act Requirements and History », EPA (2023), en ligne : <<https://www.epa.gov/clean-air-act-overview/clean-air-act-requirements-and-history>> (consulté le 16 juillet 2024).

¹⁰ M. FORELLE, préc., note 9, 5.

¹¹ Sven BEIKER, *The mobility diaries: connecting the milestones of innovation leading to ACES*, Warrendale, Pa, SAE International, 2022.

¹² BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, *The Connected Car: Who is in the Driver's Seat?*, Vancouver, 2015, p. 22, en ligne : <<https://fipa.bc.ca/connected-car/>>.

standardisé en 1993¹³. Encore à ce jour, c'est le protocole de communication standardisé le plus fréquemment utilisé dans les automobiles¹⁴.

Dès 1985, le *California Air Resource Board* entrevoit tout le potentiel de ces développements technologiques pour contrôler plus facilement les émissions polluantes. L'État américain adopte donc une loi afin que tous les modèles automobiles, à partir de 1988, disposent d'un système informatisé pour le diagnostic du moteur. Ces systèmes sont connus sous le nom d'OBD-I (*On-board Diagnostics*). N'étant pas normalisés, les codes de diagnostic utilisés par ces systèmes ainsi que leur fonctionnement variaient d'une marque de voiture à l'autre¹⁵.

En 1996, l'Agence de protection de l'environnement des États-Unis impose l'adoption du système OBD-II pour toutes les voitures vendues aux États-Unis. Le système normalisait plusieurs codes de diagnostic utiles à la réparation du véhicule, et un port standardisé dans la voiture y donnait accès¹⁶. Avec le port OBD-II, les réparateurs et propriétaires de voitures ont pu accéder à certaines données importantes à la réparation de l'automobile à l'aide d'un outil d'analyse facilement accessible. En 1999, la législation canadienne a été harmonisée avec celle des États-Unis¹⁷.

Depuis l'adoption de l'OBD-II, les voitures n'ont cessé d'évoluer. Aujourd'hui, les capteurs et les ECU ne sont pas seulement utilisés pour réguler le moteur et pour fournir de l'information diagnostique, mais aussi pour surveiller et gérer presque chaque système dans l'automobile, tel que la transmission, le freinage, les coussins gonflables, le contrôle des vitres, la climatisation, le divertissement et la télématique¹⁸. À l'heure actuelle, une voiture peut être équipée de plus de 150 ECU et peut contenir une centaine de millions de lignes de code — soit environ six fois plus de code que ce qui se retrouve dans un avion de passagers standard¹⁹!

La présence de ces capteurs et ordinateurs rend possible la collecte d'une grande quantité d'information sur le fonctionnement du véhicule. L'augmentation exponentielle des données générées par l'automobile et la complexification de son architecture électronique amènent aujourd'hui leur lot de défis, mais ce n'est qu'une partie de l'histoire de la voiture connectée. Ce qui rend une voiture connectée est sa capacité de communiquer ces données à distance, ce qui est possible grâce à la télématique.

¹³ Karl Henrik JOHANSSON, Lars NIELSEN et Martin TORNGREN, « Vehicle Applications of Controller Area Network », dans W.S. LEVINE et D. HRISTU-VARSAKELIS (dir.), *Handbook of Networked and Embedded Control Systems*, Birkhäuser Boston, coll. Control Engineering, 2005 à la page 3.

¹⁴ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 22.

¹⁵ M. FORELLE, préc., note 9, 5.

¹⁶ Lothar DETERMANN et Bruce PERENS, « Open cars », (2017) 32-2 *Berkeley Technol. Law J.*, 955, en ligne : <<https://dx.doi.org/10.15779/Z38XD0QX6F>>.

¹⁷ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 11.

¹⁸ *Id.*, p. 22.

¹⁹ MCKINSEY & COMPANY, *Cybersecurity in Automotive: mastering the challenge*, 2020, p. 6, en ligne : <<https://www.gsaglobal.org/wp-content/uploads/2020/03/Cybersecurity-in-automotive-Mastering-the-challenge.pdf>>.

2.3.2 La télématique

Le terme « télématique », inventé en 1978, réfère à un « ensemble des services de nature ou d'origine informatique pouvant être fournis à travers un réseau de télécommunication²⁰ ».

Une voiture connectée typique utilise une technologie communément appelée *Telematics Control Unit* (TCU). Le TCU standard est un module d'interface sans fil qui permet la communication de données par un moyen de télécommunication, souvent le réseau cellulaire ou le Wi-Fi. Le module est connecté à une unité centrale qui coordonne l'échange de données du véhicule avec le TCU du véhicule. Il intègre habituellement un récepteur GPS²¹. Le TCU peut ainsi transmettre des données collectées par le véhicule, telles que sa localisation ou l'état de son moteur, à l'extérieur du véhicule — à un centre d'appel ou à un serveur, par exemple — en utilisant un moyen de télécommunication. Il peut également recevoir des données du monde externe, telles que les mises à jour, la musique ou les cartes virtuelles, et les transmettre au système approprié du véhicule²². Ainsi, des services connectés tels que l'aide à la navigation, l'assistance en cas d'accident, les services d'infodivertissement, les mises à jour en direct et le contrôle du véhicule à distance ont notamment pu être déployés grâce au système²³.

Le développement de chacun de ces services ne s'est pas fait à la même vitesse et les premiers services rendus disponibles se concentraient principalement sur le guidage routier et des services liés à la sécurité en cas d'accident²⁴. Le développement du positionnement par satellite dans les années 1980 mène à la création du premier système de navigation automobile destiné aux consommateurs²⁵. En 1996, GM intègre à ses véhicules *OnStar*, une technologie sans fil qui permet la communication avec un centre de service en cas d'accident. Au départ, seule la communication verbale entre les occupants du véhicule et le service d'assistance *OnStar* est possible, mais rapidement le système est amélioré pour permettre la transmission automatique des données de localisation du véhicule. Au courant des années 2000, l'offre de services utilisant la technologie sans fil s'élargit. Dès 2003, *OnStar* offre des fonctions telles que l'aide à la navigation, la localisation du véhicule en cas de vol et les services automatiques de secours à distance²⁶. Le déploiement de ce dernier service est rendu possible grâce à

²⁰ OFFICE QUEBECOIS DE LA LANGUE FRANÇAISE, « Télématique », *Grand dictionnaire terminologique*, en ligne : <<https://vitrlinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26536714/telematique>> (consulté le 13 mars 2025).

²¹ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, *The Connected Car: Who is in the Driver's Seat?*, Vancouver, 2015, p. 27, en ligne : <<https://fipa.bc.ca/connected-car/>>.

²² *Id.*

²³ Ali KARIMI, Johan OLSSON et Johan RYDELL, *A Software Architecture Approach to Remote Vehicle Diagnostics*, Master Thesis in Informatics, Sweden, IT University of Göteborg, Göteborg University and Chalmers University of Technology, 2004, p. 3, en ligne : <https://gupea.ub.gu.se/bitstream/handle/2077/1120/Nr_8_AK,_J0,_JR.pdf?sequence=1>.

²⁴ *Id.*

²⁵ Angelika KRÓL et Tomasz ROKICKI, « Telematics in car fleet management », dans Elżbieta J. SZYMAŃSKA (dir.), *Economics and Organization of Logistics*, Scientific Journal of Warsaw University of Life Sciences, 2021 à la page 82.

²⁶ Jeffrey WISHART, Yan CHEN, Steven COMO, Narayanan KIDAMBI, Duo LU et Yezhou YANG, « Chapter 3 : Connectivity », dans *Fundamentals of Connected and Automated Vehicles*, SAE International, 2022, p. 45-69 à la page 50.

l'envoi par le module télématique des données diagnostiques du véhicule à un opérateur qui peut suggérer le déploiement d'un service d'assistance immédiat ou la planification d'un rendez-vous pour effectuer les réparations nécessaires²⁷.

En 2004, BMW est le premier fabricant automobile à intégrer à ses véhicules une carte SIM qui permet l'accès à un réseau mobile et ainsi à Internet²⁸. Les utilisateurs de ces voitures peuvent, par exemple, accéder à leur messagerie en ligne ainsi que se renseigner sur les conditions météorologiques et les prévisions d'embouteillage²⁹. En 2009, Chrysler est un des premiers fabricants automobiles à intégrer une fonctionnalité qui permet à la voiture de générer un point d'accès sans fil ; les occupants peuvent ainsi connecter leurs appareils électroniques au Wi-Fi de la voiture³⁰. Audi a été le premier fabricant à proposer un point d'accès sans fil 4G LTE, en 2014³¹.

Comme indiqué plus haut, presque tous les nouveaux véhicules fabriqués en Amérique du Nord sont aujourd'hui équipés d'une unité télématique. Notre étude des documents et des sites Web des fabricants suggère que la plupart des TCU actuels sont conçus pour se connecter via la 4G LTE. Cela permet au véhicule (et à ses occupants) de communiquer avec le monde extérieur de diverses manières, par exemple en envoyant ou en recevant des SMS, des appels téléphoniques ou en se connectant à l'Internet via des données mobiles. En outre, les voitures connectées sont généralement capables de communiquer avec d'autres appareils à courte distance via le Bluetooth, ou de se connecter à Internet par le biais d'une connexion Wi-Fi locale³².

Depuis plus de dix ans, les fabricants expérimentent la communication des données des véhicules vers d'autres véhicules et vers l'infrastructure routière³³. Ces initiatives sont largement entreprises dans le cadre du développement de la conduite autonome ou de systèmes de transport intelligents. Nous ne nous y attarderons pas, puisque ces préoccupations dépassent le cadre de notre étude.

2.3.3 Le système d'infodivertissement

L'histoire de la voiture connectée reste incomplète sans un regard sur le système d'infodivertissement. Le système d'infodivertissement (un mot-valise constitué des mots *information* et *divertissement*) est un « équipement embarqué qui regroupe les fonctions de géonavigation, de téléphonie, ainsi que l'accès à des contenus audio et vidéo ou à des services en ligne³⁴ ». Ce système est utilisé dans la voiture connectée pour contrôler et

²⁷ A. KARIMI, J. OLSSON et J. RYDELL, préc., note 23, p. 17.

²⁸ J. WISHART et al., préc., note 26 à la page 50.

²⁹ « Connected Car : Its history, stages and terms », *BMW.com* (24 octobre 2019), en ligne : <<https://www.bmw.com/en/innovation/connected-car.html>> (consulté le 28 mars 2025).

³⁰ J. WISHART et al., préc., note 26 à la page 50.

³¹ *Id.* à la page 51; William FLEMING, « Forty-Year Review of Automotive Electronics: A Unique Source of Historical Information on Automotive Electronics », (2015) 10-3 *IEEE Veh. Technol. Mag.* 80-90, 82, DOI : 10.1109/MVT.2015.2447851.

³² BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 28.

³³ J. WISHART et al., préc., note 26 aux pages 52-53.

³⁴ OFFICE QUEBECOIS DE LA LANGUE FRANÇAISE, « Système d'infodivertissement », *Grand dictionnaire terminologique* (2022), en ligne : <<https://vitrlinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26561331/systeme-dinfodivertissement>> (consulté le 17 mars 2025).

accéder à certains services connectés. Il est également important comme interface de communication avec le téléphone cellulaire de l'utilisateur.

Les véhicules sont depuis longtemps équipés de systèmes permettant au conducteur d'accéder à des services de divertissement, de navigation et de téléphonie. Les voitures ont été équipées pour la première fois de radios dans les années 1920 (popularisées dans les années 1950 et 1960) et de téléphones de voiture dans les années 1950 (popularisés dans les années 1970 et 1980)³⁵. Un tourne-disque embarqué a été inventé dans les années 1950 et des lecteurs de cassettes ont été introduits à la fin des années 1960, avant d'être remplacés par des lecteurs de CD et des ports auxiliaires. Les services de géolocalisation par satellite ont été introduits dans certains véhicules dans les années 1980, et le GPS est devenu disponible dans les années 1990. Les premiers systèmes de navigation embarqués affichaient la position du véhicule sur une carte virtuelle préchargée qui était affichée sur un écran dans la voiture. Au départ, aucune de ces fonctions de communication, de divertissement ou de navigation n'était reliée à une autre ; ce n'est qu'à la fin des années 1990 qu'elles ont été intégrées dans un système unique, connu sous le nom de système d'infodivertissement³⁶. Les systèmes d'infodivertissement modernes comportent généralement un écran d'affichage et peuvent être contrôlés par un écran tactile, des boutons, ou même la commande vocale³⁷.

Dans les années 1990 et 2000, les téléphones de voiture sont devenus moins populaires et ont finalement été remplacés par une technologie permettant à l'utilisateur de connecter son téléphone cellulaire au véhicule. L'intégration de la technologie Bluetooth, qui permet une communication sans fil à courte distance entre les appareils, a permis aux consommateurs de coupler leur téléphone à leur voiture afin de passer des appels en mains libres dans certains véhicules à partir de 2001. Dans les années 2000, les fabricants ont également commencé à déployer des services propriétaires permettant aux utilisateurs de contrôler et d'utiliser certaines fonctions du téléphone par l'intermédiaire du système d'infodivertissement du véhicule. Par exemple, en 2007, Ford a commencé à équiper ses véhicules de SYNC, un système d'infodivertissement qui permet aux utilisateurs de connecter leurs téléphones et d'autres appareils au véhicule et de contrôler des fonctions telles que la musique ou les appels téléphoniques à l'aide de commandes vocales. Les versions ultérieures de ce service ont permis une plus grande intégration entre les appareils, par exemple en permettant au système d'infodivertissement d'afficher ou de lire à haute voix les messages SMS de l'utilisateur³⁸. Tous les autres grands

³⁵ Les premiers téléphones de voiture sont antérieurs aux réseaux mobiles et fonctionnaient par radio.

³⁶ Gerrit MEIXNER, Carina HÄCKER, Björn DECKER, Simon GERLACH, Anne HESS, Konstantin HOLL, Alexander KLAUS, Daniel LÜDDECKE, Daniel MAUSER, Marius ORFGEN, Mark POGUNTKE, Nadine WALTER et Ran ZHANG, « Retrospective and Future Automotive Infotainment Systems—100 Years of User Interface Evolution », dans Gerrit MEIXNER et Christian MÜLLER (dir.), *Automotive User Interfaces: Creating Interactive Experiences in the Car*, Cham, Springer International Publishing, 2017, p. 3-53 aux pages 8-13, DOI : 10.1007/978-3-319-49448-7_1; W. FLEMING, préc., note 31, 82.

³⁷ G. MEIXNER et al., préc., note 36 aux pages 24-26.

³⁸ *Id.* aux pages 8-13; J. WISHART et al., préc., note 26 à la page 50; W. FLEMING, préc., note 31.

fabricants automobiles ont également développé et intégré des fonctionnalités similaires dans leurs véhicules³⁹.

Au départ, le seul moyen de coupler le téléphone au véhicule était d'utiliser le système d'infodivertissement propriétaire (par exemple, Ford SYNC)⁴⁰. En 2010, des chercheurs ont proposé un système normalisé qui permettrait au cellulaire de « devenir la plateforme d'application pour l'environnement automobile, tandis que le système [d'infodivertissement embarqué] est responsable de l'entrée et de la sortie de l'utilisateur⁴¹ ». En d'autres termes, le système d'infodivertissement agirait simplement comme un mécanisme de contrôle et de sortie pour le téléphone intelligent. Cette idée a donné lieu à la création de MirrorLink, une norme ouverte conçue pour permettre à l'utilisateur d'exécuter des applications sur son cellulaire plutôt que par l'intermédiaire du logiciel du fabricant de son automobile. L'idée était de permettre une plus grande interopérabilité : plutôt que d'utiliser un logiciel « fermé », propre à chaque marque ou modèle de véhicule, pour contrôler les fonctions des téléphones et afficher leur contenu, tous les fabricants automobiles pouvaient utiliser le logiciel ouvert Mirrorlink pour ce faire⁴². Apple a développé *Apple CarPlay*, un système similaire, propre aux téléphones iPhone (plateforme iOS) et Google en a développé un pour Android, appelé *Android Auto*. Ces services permettent aux utilisateurs de contrôler et d'utiliser des applications mobiles, telles que les services de navigation et de divertissement, les appels et SMS, Siri, etc., par l'intermédiaire du système d'infodivertissement du véhicule⁴³. Apple CarPlay et Android Auto sont désormais largement utilisés⁴⁴.

Dans les véhicules connectés, le système d'infodivertissement est utilisé pour contrôler les paramètres de connectivité et pour accéder à certaines fonctions connectées. Le système peut être utilisé pour accéder à des options d'infodivertissement connectées, comme la diffusion de musique ou de vidéos, l'information en temps réel sur la circulation

³⁹ Voir BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 48 pour une liste de noms de ces services.

⁴⁰ Sauf pour certaines fonctionnalités, comme le Bluetooth. Raja BOSE, Jörg BRAKENSIEK et Keun-Young PARK, *Terminal mode: transforming mobile devices into automotive application platforms*, *Proceedings of the 2nd International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, Pittsburgh Pennsylvania, ACM, AutomotiveUI '10: International Conference on Automotive User Interfaces and Interactive Vehicular Applications, 11 novembre 2010, p. 148-155, p. 148-149, DOI : 10.1145/1969773.1969801.

⁴¹ Notre traduction. *Id.*, p. 150.

⁴² MirrorLink a été largement utilisé, mais a été abandonné en 2023. CAR CONNECTIVITY CONSORTIUM, « MirrorLink® Operations Sunsetting », *Car Connectivity Consortium* (8 septembre 2021), en ligne : <<https://carconnectivity.org/mirrorlink-operations-sunsetting-by-september-30-2023/>> (consulté le 17 mars 2025).

⁴³ G. MEIXNER et al., préc., note 36 aux pages 23, 39; BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 54.

⁴⁴ Voir les résultats de notre sondage à la section 4 du rapport. Selon une étude McKinsey réalisée en 2023, la plupart des nouveaux véhicules sont équipés d'Apple CarPlay ou d'Android Auto, et près de la moitié des acheteurs de voitures n'achèteraient pas un véhicule n'ayant pas cette technologie : Felix RUPALLA, Alexander MATTHEY, Tobias SCHNEIDERBAUER et Dasha ZUYEVA, « Consumer perceptions on connected car services », *McKinsey & Company* (2023), en ligne : <<https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/how-do-consumers-perceive-in-car-connectivity-and-digital-services>> (consulté le 17 mars 2025).

routière, l'accès aux courriels, etc. Lorsque le véhicule est réellement connecté (selon notre définition), il est possible d'accéder à ces services directement sur le système d'infodivertissement du véhicule, sans qu'il soit nécessaire de se connecter à un cellulaire⁴⁵.

En 2017, Google a introduit un système d'exploitation pour les systèmes d'infodivertissement des véhicules appelé Android Automotive Operating System (« AAOS », à ne pas confondre avec Android Auto). AAOS est une version du système d'exploitation mobile Android, adapté pour les véhicules. Le système permet l'utilisation de certaines applications Android qui sont soit préchargées par le fabricant ou Google, soit téléchargées par l'utilisateur via le Car Play Store⁴⁶. Ceci permet l'utilisation des applications mobiles dans la voiture, en utilisant le système d'infodivertissement, et ce, sans connexion à un appareil cellulaire⁴⁷. Contrairement à d'autres systèmes ou applications d'infodivertissement, AAOS s'interface directement avec l'ECU central⁴⁸. Cela signifie que Google, par l'intermédiaire de l'AAOS, pourrait théoriquement accéder directement aux données générées par le véhicule ou pourrait contrôler le véhicule à distance. Les risques associés à l'accès aux données du véhicule et à son contrôle à distance seront examinés à la section 3.

2.4 Données générées, collectées et communiquées par la voiture connectée.

Dans la section précédente, nous avons décrit trois technologies essentielles à la voiture connectée : les composants électroniques, les systèmes télématiques et les systèmes d'infodivertissement. Équipée de ces technologies, la voiture moderne est connectée. Une étude indique qu'une voiture connectée peut générer 25 gigaoctets de données par heure⁴⁹, un chiffre qui augmentera considérablement à mesure que les véhicules deviendront de plus en plus connectés et autonomes. Selon une autre étude, le volume serait d'environ quatre téraoctets par jour⁵⁰. La présente section donne un aperçu de la manière dont les véhicules connectés génèrent et communiquent des données.

⁴⁵ G. MEIXNER et al., préc., note 36 à la page 23.

⁴⁶ « Qu'est-ce qu'Android Automotive ? », *Android Open Source Project*, en ligne : <https://source.android.com/docs/automotive/start/what_automotive?hl=fr> (consulté le 17 mars 2025).

⁴⁷ Bulut GOZUBUYUK et Mert D. PESÉ, *Poster: PRIDRIVE: An Advanced Privacy Analysis Tool for Android Automotive*, *Proceedings Symposium on Vehicle Security & Privacy*, San Diego, CA, USA, Internet Society, Symposium on Vehicle Security & Privacy, 2024, DOI : 10.14722/vehiclesec.2024.25024.

⁴⁸ *Id.*

⁴⁹ Shah Khalid KHAN, Nirajan SHIWAKOTI, Peter STASINOPOULOS et Matthew WARREN, « Cybersecurity regulatory challenges for connected and automated vehicles – State-of-the-art and future directions », (2023) 143 *Transp. Policy* 58-71, 64, DOI : <https://doi.org/10.1016/j.tranpol.2023.09.001>.

⁵⁰ Daniel CHOI et Paul Benjamin LOWRY, *Balancing the Commitment to the Common Good and the Protection of Personal Privacy: Consumer Adoption of Sustainable, Smart Connected Cars*, SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 13 octobre 2023, p. 2, DOI : 10.1016/j.im.2023.103876.

Il est important de noter que les technologies qui permettent aux véhicules connectés de transmettre des données au monde extérieur permettent également au véhicule de **recevoir** des données. Cela permet aux fabricants, aux utilisateurs ou à des tiers de communiquer avec la voiture et de lui envoyer, par exemple, des mises à jour logicielles et des commandes. Cette caractéristique des voitures connectées sera examinée plus en détail dans la section 2.5.

2.4.1 Données générées et collectées par le véhicule

Comme nous l'avons vu plus haut, la voiture connectée moderne est composée de nombreux ECU, ou ordinateurs, qui remplissent diverses fonctions telles que le contrôle du système moteur, du système de freinage, etc. Ces composantes sont également capables de générer des données, en mesurant, surveillant et transmettant ou sauvegardant des informations sur les systèmes dont ils font partie⁵¹.

En général, les composantes électriques d'une voiture connectée moderne sont capables de générer ou de collecter les renseignements suivants :

- **Données sur l'état du véhicule et données diagnostiques** : comme nous l'indiquons ci-dessus, la fonction initiale de nombreux ECU et capteurs embarqués dans les véhicules était de contrôler et de surveiller le fonctionnement des systèmes du véhicule. Les voitures connectées collectent désormais des données sur l'état de presque tous les systèmes du véhicule, tels que l'état du moteur, les niveaux d'huile, l'état des portes, des fenêtres, des essuie-glaces, du coffre et des phares, la pression des pneus, la vitesse, l'accélération, etc.⁵². Ces informations peuvent être utilisées pour diagnostiquer les problèmes du véhicule et, dans ce contexte, sont appelées données de diagnostic ou données diagnostiques.
- **Localisation du véhicule** : les voitures connectées sont généralement équipées de récepteurs GPS, ce qui permet au véhicule de déterminer sa position.
- **Renseignements sur les habitudes de conduite** : Les voitures modernes sont de plus en plus souvent équipées de capteurs et de caméras qui surveillent le comportement du conducteur, par exemple en détectant s'il change de voie, s'il freine ou accélère brusquement⁵³, le moment de la journée où il conduit et sa

⁵¹ Ce type de mesure à distance est également connu sous le nom de télémétrie, à ne pas confondre avec le terme télématique.

⁵² BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 22.

⁵³ Melanie SWAN, « Connected Car: Quantified Self becomes Quantified Car », (2015) 4-1 *J. Sens. Actuator Netw. JSAN* 2-29, 9, DOI : 10.3390/jsan4010002; BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 9; Wolfgang KERBER et Daniel GILL, « Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation », (2019) 10 *JIPITEC* 10 244-256, 247.

vitesse moyenne⁵⁴, s'il semble fatigué, s'il utilise son téléphone ou s'il est distrait de quelque manière que ce soit⁵⁵.

- **Informations sur le monde extérieur du véhicule** : certaines voitures connectées contiennent également des capteurs qui surveillent des éléments du monde extérieur, tels que la météo et les conditions de circulation⁵⁶, ou, dans le cas des véhicules autonomes, la proximité d'autres voitures, d'infrastructures ou de piétons.
- **Renseignements sur le conducteur ou les passagers** : certaines voitures collectent également des informations sur les personnes présentes dans la voiture, telles que le nombre de passagers et leur poids⁵⁷. Les véhicules qui offrent une conduite automatisée sont généralement équipés de capteurs sur le volant ou de caméras qui détectent les mouvements des yeux et de la tête afin de s'assurer que le conducteur est attentif⁵⁸. Certaines entreprises travaillent sur des capteurs capables de détecter des informations sur le conducteur, telles que son rythme cardiaque, sa respiration⁵⁹.

En outre, les systèmes d'infodivertissement des voitures connectées peuvent également collecter et générer des données. Si une personne interagit directement avec le logiciel propriétaire du système, ce dernier peut enregistrer **les choix de divertissement et l'historique de navigation de l'utilisateur**. Si l'utilisateur connecte son téléphone au système, ce dernier peut également collecter **des informations provenant de son téléphone, comme l'historique de ses appels, son répertoire et ses coordonnées, ainsi que le contenu de ses messages SMS**⁶⁰.

Enfin, il est important de noter que toutes ces données peuvent être regroupées avec des données permettant l'identification du véhicule, comme le numéro d'identification du véhicule (VIN), le numéro de sa carte SIM ou sa localisation à un moment donné. Ces données peuvent, à leur tour, être regroupées avec d'autres renseignements qui

⁵⁴ Vladimir KAPLUN et Michael SEGAL, « Breaching the privacy of connected vehicles network », (2019) 70-4 *Telecommun. Syst.* 541-555, DOI : 10.1007/s11235-018-00544-6.

⁵⁵ VOLVO, « Your Volvo car will understand you when you're not at your best – and step in when you need support » (21 septembre 2022), en ligne : <<https://www.media.volvocars.com/global/en-gb/media/pressreleases/304020/your-volvo-car-will-understand-you-when-youre-not-at-your-best-and-step-in-when-you-need-support>> (consulté le 17 mars 2025).

⁵⁶ W. KERBER et D. GILL, préc., note 53, 244.

⁵⁷ D. CHOI et P. B. LOWRY, préc., note 50, p. 2; Justin KLOCZKO, *Connected Cars and the Threat to Your Privacy*, Consumer Watchdog, 2022, p. 5, en ligne : <https://consumerwatchdog.org/wp-content/uploads/2022/08/2022-03_CWD-TELEMATICS-REPORT-March-2022_0.pdf>; W. KERBER et D. GILL, préc., note 53, 244.

⁵⁸ THE COUNCIL OF CANADIAN ACADEMIES, *Choosing Canada's Automotive Future*, Ottawa, 2021, p. 75-76.

⁵⁹ M. SWAN, préc., note 53, 9.

⁶⁰ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 24, 63-64; J. KLOCZKO, préc., note 57, p. 9-10.

permettent l'identification de l'utilisateur⁶¹. Comme nous le verrons dans la section 5, cela signifie que toutes ces données collectées par l'une ou l'autre des composantes peuvent être considérées comme des renseignements personnels au sens de la législation canadienne en matière de protection de la vie privée.

2.4.2 La communication de données

Grâce à son système télématique, la voiture connectée est capable de communiquer des données presque continuellement entre le véhicule et le monde extérieur⁶². Par exemple, BMW fournit une liste des données qu'elle recueille sur certains modèles, allant de l'altitude du véhicule et la pression des pneus à « l'évaluation de style de conduite ». Selon l'entreprise, ces données sont transmises au fabricant « régulièrement »⁶³. Dans son rapport de 2017, le *Government Accountability Office* des États-Unis a constaté que 13 des 16 fabricants automobiles étudiés ont déclaré collecter, utiliser et partager des données telles que la localisation et les opérations de la voiture, comme la pression des pneus, dans au moins certains modèles de véhicules⁶⁴.

Les données générées ou collectées par la voiture connectée peuvent être communiquées à diverses parties. Par exemple, les données de diagnostic et les données relatives au véhicule peuvent être envoyées directement sur les serveurs du fabricant ; les demandes d'assistance routière peuvent être envoyées à un centre d'appel ou aux services d'urgence ; les informations relatives à l'âge ou à la localisation de l'utilisateur peuvent être envoyées aux assureurs ou aux gestionnaires de flottes de location. Certaines données peuvent également être communiquées à l'utilisateur, par exemple, sur une application mobile fournie par le fabricant⁶⁵. Si les données sont communiquées par le réseau mobile, ils passent entre les mains des fournisseurs de télécommunications. Certaines voitures connectées sont également en mesure de communiquer avec d'autres véhicules ou des infrastructures, une fonctionnalité qui est principalement utilisée dans le contexte des véhicules autonomes⁶⁶.

⁶¹ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 61.

⁶² M. FORELLE, préc., note 9, 1.

⁶³ BMW GROUP, *Catalogue des données télématiques BMW CarData*, novembre 2024, en ligne : <Accessible sur <https://bmw-cardata.bmwgroup.com/thirdparty/public/car-data/overview>>; voir aussi BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 23.

⁶⁴ U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), préc., note 1 résumé du rapport.

⁶⁵ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 26-27.

⁶⁶ LE COMITÉ SENATORIAL PERMANENT DES TRANSPORTS ET DES COMMUNICATIONS, *Paver la voie : Technologie et le futur du véhicule automatisé*, Ottawa, Rapport du Comité sénatorial permanent des transports et des communications, 2018, p. 17, en ligne : <[https://sencanada.ca/content/sen/committee/421/TRCM/Reports/COM_RPT_TRCM_Automated Vehicles_f.pdf](https://sencanada.ca/content/sen/committee/421/TRCM/Reports/COM_RPT_TRCM_Automated_Vehicles_f.pdf)>.

2.5 Fonctionnalités connectées

Les technologies connectées évoquées ci-dessus donnent accès à de nouvelles fonctionnalités. Dans cette section, nous passerons en revue certaines des fonctionnalités connectées les plus courantes, c'est-à-dire celles qui dépendent de la connexion à Internet ou à un réseau cellulaire du véhicule.

L'information sur laquelle cette partie du rapport est basée provient d'une recherche faite en 2024 sur les sites Web des principaux fabricants automobiles, sauf indication contraire dans une note de bas de page. Nous ne faisons pas d'individualisation des différents fabricants dans cette section, car les types de fonctionnalités décrites ci-dessous sont offerts par la plupart d'entre eux. Pour des exemples précis, voir la section 6 du présent rapport.

2.5.1 Infodivertissement connecté

Comme décrit dans la section ci-dessus, les voitures connectées sont équipées de systèmes d'infodivertissement. Si un véhicule est connecté à l'Internet ou au réseau mobile, le système d'infodivertissement peut fournir des services d'information, de communication ou de divertissement connectés, tels que la diffusion de vidéos ou de musique, de l'information en temps réel sur la circulation routière et de la navigation et des services de communication comme le courriel.

2.5.2 Point d'accès sans fil

Si la voiture a une connexion Internet, elle peut également générer un point d'accès Wi-Fi. Ceci permet au conducteur et aux passagers de connecter d'autres appareils à l'Internet du véhicule.

2.5.3 Services de sécurité routière

Les capteurs d'un véhicule peuvent déterminer s'il y a eu un accident, et le TCU du véhicule peut transmettre automatiquement cette information à un centre d'appel ou aux services d'urgence afin d'obtenir une assistance. Comme décrit ci-dessus, il s'agit de l'une des plus anciennes utilisations de la télématique dans les véhicules et c'est désormais une fonctionnalité largement disponible dans les voitures connectées⁶⁷.

⁶⁷ Sur les 13 fabricants automobiles étudiés dans le rapport du GAO qui proposaient des services connectés, tous offraient à leurs clients ce service : U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), préc., note 1, p. 13.

2.5.4 Localisation et surveillance de la voiture à distance

Les voitures connectées peuvent transmettre leurs données de localisation au fabricant ; les fabricants peuvent, à leur tour, donner accès à cette information aux utilisateurs du véhicule. Cela permet à l'utilisateur ou à des tiers autorisés (par ex., la police) de localiser ou de surveiller le véhicule à distance. Par exemple, les consommateurs peuvent utiliser une application mobile couplée au véhicule pour vérifier s'il a franchi une zone déterminée ou s'il a dépassé certaines vitesses. Cette fonction est parfois vendue comme une mesure antiviol ou un moyen de surveiller les enfants adolescents.

2.5.5 Contrôle à distance

Étant donné que le TCU d'une voiture connectée peut recevoir des données du monde extérieur et les transmettre à l'ECU central, les voitures connectées peuvent recevoir des commandes et être contrôlées à distance. Par exemple, les consommateurs peuvent coupler leur téléphone intelligent ou d'autres appareils intelligents avec le véhicule afin de le démarrer à distance, de déverrouiller ou de verrouiller les portes, ou de démarrer la climatisation.

2.5.6 Mises à jour à distance

Comme les voitures connectées peuvent recevoir des données, elles sont capables de recevoir des mises à jour logicielles en direct qui peuvent corriger des bogues ou d'autres problèmes liés au logiciel du véhicule.

2.5.7 Blocage et déblocage de fonctionnalités à distance, abonnements

La même technologie permet aux fabricants de restreindre ou d'autoriser à distance certaines utilisations de la voiture. Par exemple, la capacité de la batterie de certains modèles Tesla est limitée par un logiciel et cette limite peut être supprimée par le fabricant au moyen de mises à jour logicielles à distance. Par exemple, en 2017, Tesla a été en mesure de procéder, à distance, à l'amélioration de la capacité des batteries de ses véhicules se trouvant en Floride afin de permettre aux conducteurs de parcourir de plus grande distance à l'approche de l'ouragan Irma⁶⁸.

Cette fonctionnalité permet aux fabricants de bloquer l'accès à des fonctions déjà intégrées dans la voiture et, le cas échéant, d'obliger le consommateur à payer un

⁶⁸ Simon USBORNE, « How did Tesla make some of its cars travel further during Hurricane Irma? », *The Guardian*, sect. Technology (11 septembre 2017), en ligne : <<https://www.theguardian.com/technology/shortcuts/2017/sep/11/tesla-hurricane-irma-battery-capacity>> (consulté le 17 mars 2025).; Natasha TUSIKOV, « Precarious Ownership of the Internet of Things in the Age of Data », dans B. HAGGART, K. HENNE et N. TUSIKOV, *Information, Technology and Control in a Changing World*, Palgrave Macmillan, Cham, coll. International Political Economy Series, 2019, p. 121-148 aux pages 136-137, en ligne : <https://doi.org/10.1007/978-3-030-14540-8_6>.

abonnement pour les déverrouiller. Par exemple, BMW a tenté de vendre des abonnements pour débloquent l'accès aux sièges chauffants dans les voitures qui en étaient déjà équipées, une idée qui s'est avérée controversée⁶⁹. De même, Mercedes a limité la fonctionnalité du moteur sur certains modèles, obligeant les consommateurs à payer un abonnement pour obtenir des vitesses d'accélération plus élevées⁷⁰.

2.5.8 Diagnostic à distance

Les voitures connectées collectent en continu des données sur le véhicule, qui peuvent donner un aperçu de son état de santé et de ses besoins en matière d'entretien. Le véhicule peut transmettre ces renseignements au fabricant, qui peut choisir de les fournir aux utilisateurs ou à des tiers, comme les concessionnaires, les assureurs ou les mécaniciens indépendants. Ces données peuvent être utilisées pour détecter ou diagnostiquer à distance des problèmes et pour avertir les consommateurs ou les concessionnaires de la nécessité d'un rendez-vous d'entretien.

2.5.9 Intégration dans « l'Internet des objets »

Les voitures connectées peuvent être associées à d'autres objets connectés, ce qui leur permet de faire partie de l'Internet des objets. Par exemple, certains constructeurs se sont associés à Samsung pour permettre aux utilisateurs d'intégrer le véhicule à SmartThings, une application permettant de contrôler les objets intelligents. Cela permettrait à l'utilisateur non seulement de contrôler à distance certaines fonctionnalités de la voiture, par exemple avec son téléphone intelligent, mais aussi d'utiliser le système de communication de la voiture pour contrôler sa porte de garage, ses appareils électroménagers ou son chauffage⁷¹.

2.5.10 Assurances personnalisées et conseils de conduite

La connectivité permet aux compagnies d'assurance de proposer désormais des polices d'assurance personnalisées (autrement connus sous le nom d'assurance basée sur l'utilisation). Pour offrir des primes personnalisées, les assureurs collectent des données sur le véhicule et le conducteur, telles que leurs habitudes de freinage et d'accélération,

⁶⁹ Alistair CHARLTON, « BMW Wants To Charge You A Subscription For Your Heated Seats », *Forbes*, sect. Cars & Bikes (2 juillet 2020), en ligne : <<https://www.forbes.com/sites/alistaircharlton/2020/07/02/bmw-wants-to-charge-you-a-subscription-for-your-heated-seats/>> (consulté le 17 mars 2025); Alistair CHARLTON, « BMW Drops Controversial Heated Seats Subscription Service », *Forbes*, sect. Cars & Bikes (7 septembre 2023), en ligne : <<https://www.forbes.com/sites/alistaircharlton/2023/09/07/bmw-drops-controversial-heated-seats-subscription-to-refocus-on-software-services/>> (consulté le 17 mars 2025); M. FORELLE, préc., note 9, 8.

⁷⁰ Jess WEATHERBED, « Mercedes is charging \$1,200 a year for faster acceleration », *The Verge* (23 novembre 2022), en ligne : <<https://www.theverge.com/2022/11/23/23474969/mercedes-car-subscription-faster-acceleration-feature-price>> (consulté le 17 mars 2025).

⁷¹ Bertrand GODIN, « Et si votre voiture prenait le contrôle de votre maison intelligente ? », *La Presse*, sect. Auto (27 mai 2024), en ligne : <<https://www.lapresse.ca/auto/2024-05-27/techno/et-si-votre-voiture-prenait-le-controle-de-votre-maison-intelligente.php>> (consulté le 17 mars 2025).

la vitesse moyenne du véhicule, l'utilisation du téléphone au volant, la localisation du véhicule et le moment de la journée où la voiture est utilisée, afin d'établir un profil de risque du conducteur⁷². Ces données peuvent être soit collectées par le fabricant et partagées avec l'assureur, soit collectées par l'assureur lui-même à l'aide d'un dispositif utilisé dans le véhicule, tel qu'une application mobile sur le téléphone de l'utilisateur⁷³.

2.6 Autres utilisations des technologies connectées

La technologie connectée permet également un certain nombre d'usages qui ne sont pas destinés aux consommateurs, mais qui profitent plutôt aux fabricants et à des tiers tels que les assureurs, les courtiers en données et l'État. La présente section donne un aperçu de certaines de ces utilisations.

2.6.1 Collecte de données pour l'usage interne par les fabricants

Les fabricants utilisent les technologies connectées pour recueillir des données à leurs propres fins. Le rapport 2017 du GAO a constaté que douze des treize fabricants étudiés collectaient des données sur les véhicules à des fins internes, telles que la recherche et le développement, la recherche sur la sécurité des véhicules, ou à des fins de marketing⁷⁴. Les politiques de protection de la vie privée étudiées aux points 3.1 et 6 mentionnent d'ailleurs ces objectifs.

2.6.2 Vente de données pour des fins commerciales

Les fabricants de voitures connectées utilisent les données générées et collectées par les véhicules connectés à des fins commerciales, par exemple en les vendant à des tiers. En raison d'un manque de transparence sur cette question, l'étendue de cette pratique n'est pas tout à fait claire (voir section 3.1). Toutefois, la Fondation Mozilla a constaté que 76 % des 25 plus importants fabricants automobiles ont déclaré qu'ils pouvaient vendre les données de l'utilisateur⁷⁵. Il semble que les acteurs de l'industrie considèrent qu'il s'agit d'une importante source de revenus potentiels⁷⁶.

BC FIPA a observé que les fabricants de voitures connectées affirment avoir subi des pressions de la part de sociétés de publicité pour partager des données,

⁷² J. KLOCZKO, préc., note 57, p. 14-15; Kaveh WADDELL, « What You're Giving Up When You Let Your Car Insurer Track You In Exchange for Discounts », *Consumer Reports* (7 octobre 2021), en ligne : <<https://www.consumerreports.org/money/car-insurance/how-car-insurance-telematics-discounts-really-work-a1549580662/>> (consulté le 17 mars 2025).

⁷³ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 51.

⁷⁴ U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), préc., note 1, p. 13.

⁷⁵ MOZILLA FOUNDATION, « What Data Does My Car Collect About Me and Where Does It Go? », **Privacy Not Included: A Buyer's Guide for Connected Products*, en ligne : <<https://foundation.mozilla.org/fr/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/>> (consulté le 19 mars 2025).

⁷⁶ M. BERTONCELLO, C. MARTENS, T. MOLLER et T. SCHNEIDERBAUER, préc., note 6.

depuis au moins 2015⁷⁷. Certains fabricants ont déjà expérimenté avec la vente de données pour les fins publicitaires :

One example is GM Marketplace, which was launched in 2017 and is now installed on more than four million GM vehicles. It allows drivers to use the touch screen in the vehicle to buy coffee, doughnuts, make restaurant and hotel reservations, and prepay for gasoline. The app is free to consumers (who register with Marketplace vendors directly), but GM shares data about drivers' buying patterns (not financial information) with the vendors, who pay GM either a flat rate or a monthly fee based on the number of consumer "impressions" they receive⁷⁸.

En 2024, Ford a déposé une demande de brevet pour un système de présentation de publicités ciblées à bord des véhicules. Le système utiliserait les informations recueillies par le véhicule, y compris les informations de localisation, la vitesse, les informations sur la circulation routière et les « signaux audio à l'intérieur du véhicule » tels que les commandes vocales et les conversations dans la voiture, pour présenter des publicités ciblées à l'utilisateur pendant le trajet, par l'intermédiaire du système d'infodivertissement⁷⁹.

Les fabricants vendent également des données à des entreprises tels les courtiers en données. Ces entreprises achètent et revendent des données à des fins diverses ; en combinant des données provenant de sources multiples, elles peuvent établir des profils et faire des inférences sur les consommateurs. Palantir, société d'analyse de données, a conclu un partenariat avec Stellantis, l'entreprise qui exploite de nombreuses marques telles que Chrysler, Jeep, Citroën et bien d'autres⁸⁰. High Mobility, un courtier spécialisé dans les données automobiles, a un partenariat avec 36 % des marques automobiles (9 au total) étudiées par Mozilla⁸¹.

En 2024, un article du New York Times a rapporté que GM partageait des données de conduite avec des courtiers en données, qui les revendaient à des assureurs. L'article raconte l'histoire d'un conducteur de Chevrolet Bolt dont le taux d'assurance a soudainement augmenté de plus de 20 %. Lorsque le consommateur interroge son assureur sur cette augmentation, un agent lui répond que la décision a été prise sur la base d'informations fournies par LexisNexis Risk Solutions, un courtier en données, qui a préparé un rapport de 258 pages sur l'homme. Ce rapport comprenait :

more than 130 pages detailing each time he or his wife had driven the Bolt over the previous six months. It included the dates of 640 trips, their start and end times,

⁷⁷ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 19.

⁷⁸ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, 2019 Update, *The Connected Car: Who is in the Driver's Seat*, Vancouver, 2019, p. 8, en ligne : <<https://fipa.bc.ca/2019-update-to-the-connected-car/>>. Ce service a été abandonné en 2022.

⁷⁹ Himanshu VERMA, et Fling TSENG, 20240289844 A1, Dearborn, MI, en ligne : <<https://www.scribd.com/document/767763945/20240289844>> (consulté le 18 mars 2025).

⁸⁰ PALANTIR, « Palantir Automotive & Mobility Solutions », en ligne : <<https://www.palantir.com/offerings/automotive-mobility/>> (consulté le 18 mars 2025).

⁸¹ MOZILLA FOUNDATION, préc., note 75.

*the distance driven and an accounting of any speeding, hard braking or sharp accelerations. The only thing it didn't have is where they had driven the car*⁸².

Ces informations avaient été collectées par le fabricant automobile, GM, dans le cadre d'un service destiné à offrir un score et des conseils de conduite ; les données recueillies ont été ensuite fournies au courtier en données, qui les transmettait ensuite aux assureurs. Selon le New York Times, Kia, Subaru et Mitsubishi contribuent également à la banque de données de LexisNexis, qui affirme avoir recueilli des données sur plus de 10 millions de véhicules⁸³.

2.6.3 Utilisation publique

Enfin, les acteurs publics utilisent également les données générées par les voitures connectées. Ces données peuvent être utilisées par les organismes chargés de l'application de la loi ou de la surveillance. Les acteurs étatiques britanniques ont déclaré qu'ils considéraient les systèmes d'infodivertissement comme un nouvel outil pour la police scientifique⁸⁴. Le scientifique en chef de la Cyber Crime Center du Department of Defense américain a évoqué le fait que les données des véhicules connectés peuvent être extraites et utilisées comme preuves numériques : « Si vous avez une Tesla et un iPhone, nous ne pouvons pas fouiller dans votre téléphone, mais nous pouvons obtenir des données de la télématique de la voiture⁸⁵ ». Les fabricants automobiles partagent aussi les données des utilisateurs lorsqu'ils y sont contraints par une décision de justice⁸⁶.

Les acteurs étatiques obtiennent parfois eux aussi ces données par le biais de partenariats avec des fabricants ou des entreprises spécialisées dans l'agrégation ou l'extraction de données⁸⁷. Par exemple, la société Palantir, qui collecte et analyse les données des véhicules⁸⁸, a conclu des contrats avec la police de Los Angeles et le

⁸² Kashmir HILL, « Automakers Are Sharing Consumers' Driving Behavior With Insurance Companies », *The New York Times* (11 mars 2024), en ligne : <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html> (consulté le 17 mars 2025).

⁸³ *Id.* L'article nomme également un autre courtier en données, Verisk.

⁸⁴ PRIVACY INTERNATIONAL, *Connected Cars: What Happens to Our Data on Rental Cars?*, Privacy international, 2017, p. 4, en ligne : https://privacyinternational.org/sites/default/files/2017-12/cars_briefing.pdf.

⁸⁵ Notre traduction. Amy KLUBER, « AI Boosts DOD Cyber Crime Center Digital Forensics », *GovCIO Media & Research* (24 octobre 2024), en ligne : <https://govciomedia.com/ai-boosts-dod-cyber-crime-center-digital-forensics/> (consulté le 18 mars 2025).

⁸⁶ U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), « Vehicle Data Privacy: Industry and Federal Efforts Under Way but NHTSA Needs to Define Its Role » (2017), p. 14, en ligne : <https://www.gao.gov/products/gao-17-656> (consulté le 21 octobre 2024).

⁸⁷ En effet, le gouvernement des États-Unis a déjà acheté des données collectées à partir de téléphones mobiles, permettant ainsi aux acteurs étatiques d'accéder à des informations qui, autrement, ne pourraient être obtenues que par le biais d'un mandat : Shreya Tewari WALTER-JOHNSON Fikayo, « New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data | ACLU », *American Civil Liberties Union* (18 juillet 2022), en ligne : <https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data> (consulté le 18 mars 2025).

⁸⁸ PALANTIR, préc., note 80.

Department of Homeland Security (DHS)⁸⁹. Une division du DHS a également commandé des kits de criminalistique d'une entreprise spécialisée dans l'extraction des données, afin de collecter les données des voitures et des téléphones portables qui y ont été précédemment couplés, ce qui leur permettrait de recueillir des données sur la localisation, les contacts, les communications, le comportement de la voiture et du conducteur, etc.⁹⁰. En 2023, Ford a déposé une demande de brevet pour une technologie qui permettrait aux voitures de surveiller la vitesse des autres véhicules et d'envoyer ces informations directement à la police⁹¹.

Les fabricants de voitures connectées sont également obligés de mettre en œuvre des lois ou des politiques gouvernementales. Par exemple, l'Union européenne exige que les nouveaux véhicules soient équipés d'un service d'appels d'urgence automatique⁹². Certains pays utilisent déjà la communication entre véhicules et infrastructures à des fins publiques, par exemple pour faire respecter les droits de stationnement, ou aux frontières et sur les routes à péage⁹³.

En Chine, l'État exige ouvertement des fabricants de voitures connectées qu'ils lui communiquent certaines données collectées⁹⁴. Au début de l'année 2025, le Department of Commerce des États-Unis a interdit la vente et l'importation de matériel et de logiciels pour des véhicules connectés en provenance de Chine et de Russie. La décision invoque la menace posée par la présence de ces acteurs dans la chaîne d'approvisionnement, citant « l'accès illimité aux acteurs malveillants à ces systèmes connectés et aux données qu'ils collectent », ainsi que le besoin de se défendre contre le cyberespionnage et de protéger l'infrastructure de transport américain⁹⁵. La décision tient compte du fait que « certains matériels et logiciels utilisés dans les véhicules connectés pourraient permettre la collecte massive d'information sensible, y compris des données de géolocalisation, des enregistrements audio et vidéo et d'autres analyses du cycle de vie⁹⁶ ». Malheureusement, comme nous allons le voir dans la prochaine section du rapport, ces mêmes risques s'appliquent aussi bien dans le contexte intérieur.

⁸⁹ J. KLOCZKO, préc., note 57, p. 4.

⁹⁰ *Id.*, p. 4, 13-14.

⁹¹ Stephen EDELSTEIN, « Future Fords might detect speeding and report you to the cops », *Motor Authority* (25 juillet 2024), en ligne : <https://www.motorauthority.com/news/1143913_future-fords-might-detect-speeding-and-report-you-to-the-cops> (consulté le 4 novembre 2024).

⁹² BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 15-16.

⁹³ *Id.*, p. 15-16.

⁹⁴ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 78, p. 9-10.

⁹⁵ Notre traduction. THE WHITE HOUSE, « FACT SHEET: Safeguarding America from National Security Risks of Connected Vehicle Technology from China and Russia », *The White House* (14 janvier 2025), en ligne : <<https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2025/01/14/fact-sheet-safeguarding-america-from-national-security-risks-of-connected-vehicle-technology-from-china-and-russia/>> (consulté le 18 mars 2025).

⁹⁶ Notre traduction. *Id.*

2.7 Faits saillants

La voiture connectée est un véhicule qui peut envoyer et recevoir des données à distance, via le réseau cellulaire ou l'Internet. La plupart des nouvelles voitures fabriquées en Amérique du Nord sont connectées d'une manière ou d'une autre.

La voiture connectée d'aujourd'hui est le résultat de deux tendances technologiques. Tout d'abord, les voitures sont devenues de plus en plus informatisées au cours des cinquante dernières années et contiennent désormais de nombreux composants électroniques. Cette évolution permet de surveiller et de contrôler électroniquement de nombreux systèmes du véhicule, qu'il s'agisse du moteur, du système de freinage, des vitres, de la climatisation ou du système d'infodivertissement. Ces unités électroniques sont non seulement nécessaires au fonctionnement du véhicule, mais elles lui permettent également de générer de grandes quantités de données. Deuxièmement, les véhicules sont de plus en plus capables de transmettre et de recevoir des données du monde extérieur par l'intermédiaire de leurs unités télématiques. Ces unités télématiques fonctionnent généralement sur le réseau cellulaire ou Wi-Fi, ce qui permet aux véhicules de transmettre et de recevoir des données par le biais de données mobiles, de SMS et d'Internet.

Les voitures connectées sont capables de générer et de collecter des données sur un large éventail de sujets, tels que l'état du véhicule, les données de diagnostic, la localisation du véhicule, les caractéristiques et l'identité du conducteur, le comportement du conducteur, les passagers, les informations sur l'environnement extérieur, les choix d'infodivertissement et l'utilisation des services connectés.

La technologie présente dans ces véhicules donne accès à de nouvelles fonctionnalités connectées. Les fonctionnalités offertes dépendent de chaque voiture, mais, en général, une voiture connectée a la capacité de diffuser du contenu de divertissement, d'offrir la navigation connectée, de générer des points d'accès sans fil, d'envoyer des données de diagnostic et de conduite au monde extérieur, d'obtenir de l'aide en cas d'accident, de télécharger des mises à jour en direct (ce qui permet le déblocage ou le blocage d'autres fonctionnalités à distance) et d'être contrôlée ou localisée à distance. En plus d'offrir ces fonctionnalités connectées, les fabricants utilisent les technologies connectées à d'autres fins. Par exemple, ils peuvent collecter des données sur les véhicules à des fins internes telles que la recherche, le développement et le marketing, et les vendre à des tiers, y compris des courtiers en données et des assureurs. Les acteurs publics ont également un intérêt pour ces données aux fins de développement d'infrastructures, de surveillance et d'application de la Loi.

3 Quels risques pour les consommateurs ?

Dans cette section, nous allons examiner les risques et les enjeux pour les consommateurs que pose la connectivité dans les voitures.

Les principaux enjeux identifiés dans la littérature se répartissent en deux larges catégories : ceux qui sont liés à la vie privée et les renseignements personnels, et ceux qui sont en lien avec le droit de la propriété.

3.1 Risques et enjeux pour la vie privée

Déjà dans les années 90 et au début des années 2000, des craintes d'atteintes à la vie privée liées à la technologie intégrée aux véhicules ont été soulevées. Un article publié par le New York Times en 2003 a noté que des tiers pouvaient écouter les appels téléphoniques passés par l'intermédiaire du système OnStar et que ce dernier avait déjà été utilisé par les forces de l'ordre pour retrouver l'auteur d'un délit de fuite⁹⁷. Dans une recherche de 2005 consacrée à ce sujet, l'auteur conclut que la collecte de données des technologies connectées dans les voitures nuit au droit à la vie privée des individus de deux manières :

*Firstly, data subjects are unable to control all the personal information collected about them. There are too many data sources and too many stakeholders seeking data. Secondly, the lack of binding regulation forces citizens either to accept the loss of privacy, or to lose out on the benefits (security and services)*⁹⁸.

Ces conclusions s'appliquent toujours aux voitures connectées d'aujourd'hui. En effet, les risques pour la vie privée posés par les voitures connectées n'ont fait que s'accroître au fil du temps, à mesure que la technologie connectée a progressé et s'est répandue dans les véhicules.

Au cours de la dernière décennie, de nombreux autres rapports de recherche ont été rédigés sur ce sujet, et plusieurs d'entre eux ont tiré la sonnette d'alarme quant aux risques que les voitures connectées font peser sur la vie privée des consommateurs. En particulier, le rapport *The Connected Car: Who is in the Driver's Seat*, publié en 2015 par le BC Freedom of Information and Privacy Association (BC FIPA), a constaté des lacunes importantes dans les politiques de protection de la vie privée des fabricants de voitures connectées⁹⁹. Ce constat a été réaffirmé dans une mise à jour du rapport publiée en 2019¹⁰⁰. Plusieurs autres rapports se sont penchés sur la question et ont identifié des

⁹⁷ John SCHWARTZ, « This Car Can Talk. What It Says May Cause Concern. », *New York Times* (29 décembre 2003), en ligne : <<http://www.nytimes.com/2003/12/29/business/this-car-can-talk-what-it-says-may-cause-concern.html>> (consulté le 28 octobre 2024).

⁹⁸ Carlos RODRIGUEZ CASAL, « Privacy within in-car systems », (2005) 7-1 *Info*, 73.

⁹⁹ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12.

¹⁰⁰ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 78.

risques majeurs pour la vie privée des consommateurs¹⁰¹. Les problèmes de protection de la vie privée posés par les voitures connectées sont également de plus en plus souvent évoqués dans les médias, car les consommateurs commencent à être confrontés plus fréquemment à ces risques et à leurs conséquences. Cette section fait la synthèse de la recherche sur cette question.

3.1.1 Collecte massive de renseignements personnels

Comme décrit dans la section 2, les voitures connectées sont capables de générer, de collecter et de communiquer d'énormes quantités d'informations. Elles recueillent non seulement des renseignements sur le véhicule, sa localisation, ses passagers et ses utilisateurs, mais aussi des données provenant des appareils qui y sont connectés, telles que les téléphones intelligents des utilisateurs. Un système d'infodivertissement dans une voiture connectée peut collecter des informations sur les contacts d'une personne, son emploi du temps, l'utilisation de son téléphone, ainsi que ses choix en matière de navigation, de divertissement et de communication. En plus de toutes les données générées et collectées par la voiture, les fabricants automobiles peuvent également avoir accès à des renseignements sur l'utilisateur collectés auprès du concessionnaire, par exemple, tels que leurs revenus, leur statut d'emploi, leur situation matrimoniale, leur historique de crédit, etc.

L'étendue de cette collecte de données n'est pas claire, bien que nous ayons mentionné dans la section 2 que certains véhicules peuvent transmettre des dizaines de gigabits de données par jour au fabricant. Comme nous le verrons ci-dessous, tous les grands fabricants automobiles indiquent dans leurs politiques qu'ils collectent, utilisent et partagent les données collectées et générées par le véhicule¹⁰². Les renseignements collectés sont souvent personnels, sensibles et difficiles, voire impossibles, à dépersonnaliser ou à anonymiser. L'anonymisation est le processus qui consiste à transformer des données de manière à ce qu'elles ne puissent pas être identifiées à une personne. Elle est, en théorie, irréversible. La dépersonnalisation est le processus qui consiste à supprimer les identifiants directs des données, ce qui rend plus difficile l'identification d'une personne. Toutefois, les données dépersonnalisées peuvent être identifiées à une personne de manière indirecte. (Voir la section 5.1.2 pour les définitions juridiques de ces termes.)

Une grande partie des données collectées par les véhicules peuvent être considérées comme des renseignements personnels, qui sont définis dans la législation canadienne comme des renseignements concernant une personne identifiable ou d'information qui

¹⁰¹ Par exemple : U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), préc., note 86; PRIVACY INTERNATIONAL, préc., note 84; CONSUMER WATCHDOG, *Connected Cars and the Threat to Your Privacy*, 2022, en ligne : <<https://consumerwatchdog.org/reports/connected-cars-and-threat-your-privacy/>> (consulté le 21 octobre 2024); MOZILLA FOUNDATION, « It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy », **Privacy Not Included: A Buyer's Guide for Connected Products*, en ligne : <<https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>> (consulté le 29 octobre 2024).

¹⁰² Section 6 du rapport. MOZILLA FOUNDATION, préc., note 101.

peut être liée indirectement à une personne identifiable¹⁰³. C'est le cas pour toute information pouvant être associée directement à l'utilisateur du véhicule, par exemple le numéro d'identification du véhicule (NIV), le numéro de la carte SIM, le nom de la personne ou ses coordonnées. On peut toutefois aussi considérer comme renseignement personnel toute information qui peut être liée à la personne d'une façon indirecte, telle que son lieu de stationnement, ses habitudes de conduite, ses préférences musicales ou son niveau de vigilance, notamment si cette information est ou peut être associée à d'autres informations permettant d'identifier la personne, telles que le NIV.

Une information est considérée comme personnelle si elle révèle quelque chose sur l'identité, les caractéristiques ou les activités d'une personne, par exemple ses informations financières, son âge, l'historique de sa localisation, son état de santé, ses croyances, etc. Ainsi, même les informations qui, à première vue, semblent impersonnelles ou peu révélatrices peuvent être des informations personnelles. Par exemple, les données de localisation du véhicule et celles sur l'état du moteur peuvent être considérées comme des renseignements personnels si elles révèlent d'une façon indirecte le lieu de travail de la personne, ses heures de travail, etc.¹⁰⁴. Plus les informations sont recoupées avec d'autres renseignements, plus elles en révèlent sur la personne.

En outre, une grande partie de ces informations personnelles sont sensibles, en particulier lorsqu'elles sont regroupées avec d'autres informations sur la personne¹⁰⁵. Certaines données collectées ou générées par les fabricants de voitures connectées sont explicitement sensibles (par exemple, des informations financières). Cependant, même des informations qui ne semblent pas sensibles, telles que l'heure d'ouverture d'une portière, peuvent être extrêmement révélatrices lorsqu'elles sont combinées à d'autres informations telles que la localisation du véhicule, les habitudes de l'utilisateur, ses contacts, l'historique de ses appels, etc. Par exemple, une fuite de données chez Volkswagen en 2024 a révélé les données de localisation précises chaque fois qu'un véhicule était stationné. Même si la base de données ne contenait pas de noms, les chercheurs ont pu facilement identifier des personnes associées à ces données. Lorsque

¹⁰³ Voir la section 5.1.2 pour une discussion de la notion légale des renseignements personnels. BARBARA VON TIGERSTROM, *Information & Privacy Law in Canada*, Toronto, Irwin Law Inc., 2020, p. 301-303.

¹⁰⁴ *Id.*, p. 302-305; U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), préc., note 86, p. 9.

¹⁰⁵ Nous utilisons ici le terme « sensible » de manière générale, mais la notion juridique de sensibilité est abordée à la section 5.1.2. Comme l'explique le Commissariat à la protection de la vie privée du Canada, la sensibilité est évaluée en fonction du contexte. Certaines informations, comme les données médicales et financières, les informations relatives à la réputation, à la sexualité, aux croyances religieuses ou philosophiques, sont presque toujours considérées comme sensibles. Des données apparemment inoffensives peuvent devenir sensibles lorsqu'elles sont combinées à d'autres renseignements qui mènent à une déduction sensible. Voir OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, « Interpretation Bulletin: Sensitive Information » (16 mai 2022), en ligne : <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_10_sensible/> (consulté le 29 octobre 2024).

ces données ont été associées à une personne identifiable, elles révélaient plusieurs faits plus ou moins sensibles sur la personne : son lieu de travail, sa salle de sport, ses restaurants préférés, ses consultations avec des professionnels de la santé, etc.¹⁰⁶. Comme l'a indiqué le journal *Der Spiegel International* à propos de la fuite, ce type de données se prête à une utilisation abusive par le biais de la fraude, du chantage et même de l'espionnage.

En combinant ou en agrégeant une multitude de données, les fabricants de voitures connectées et les fournisseurs de services peuvent tirer des conclusions sophistiquées et sensibles sur les consommateurs¹⁰⁷. En effet, les politiques de confidentialité des fabricants de voitures connectées semblent envisager explicitement qu'ils collecteront ou déduiront des informations sensibles sur les utilisateurs qu'il semble difficile d'obtenir directement. Par exemple, la Fondation Mozilla a constaté que les politiques de Nissan et de Kia réfèrent à la collecte d'informations sur l'activité sexuelle de la personne et que « six fabricants automobiles disent qu'ils peuvent collecter vos "informations génétiques" ou vos "caractéristiques génétiques"¹⁰⁸ ». Comme le souligne une organisation américaine de défense des consommateurs, « nos voitures en savent plus sur nous que nous n'en savons sur nous-mêmes, avec des informations telles que le poids, la tension artérielle, l'orientation sexuelle, la race, le statut économique, jusqu'aux portes qui s'ouvrent et l'heure à laquelle vous avez appuyé sur le frein¹⁰⁹ ».

Comme nous le verrons dans la section 6, les fabricants affirment parfois qu'ils peuvent utiliser ou partager des données « à toutes fins » lorsqu'elles sont dépersonnalisées ou anonymisées. Toutefois, certains types de données sont devenus très difficiles à dépersonnaliser ou à anonymiser à l'ère des mégadonnées (ou *big data*). Bien que l'anonymisation reste possible, il s'agit d'un processus rigoureux et technique qui va bien au-delà de la simple suppression des renseignements identifiables d'un ensemble de données¹¹⁰. Étant donné la quantité de données collectées sur une personne, il est souvent facile de réidentifier des informations dépourvues des critères d'identification en

¹⁰⁶ Voir la section 3.4.1 pour plus d'information sur cette fuite. Patrick Beuth FLÜPKE, Max HOPPENSTEDT, Michael KREIL, Marcel ROSENBAACH et Rina WILKIN, « We Know Where You Parked: Massive Data Breach at VW Raises Questions about Vehicle Privacy », *Der Spiegel*, sect. International (3 janvier 2025), en ligne : <<https://www.spiegel.de/international/business/we-know-where-you-parked-massive-data-breach-at-vw-raises-questions-about-vehicle-privacy-a-4b1cb926-2edb-42ea-92fb-5000cd378fc5>> (consulté le 15 janvier 2025).

¹⁰⁷ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 65; Silvia ZHANG, « Who Owns the Data Generated by Your Smart Car? », (2018) 32-1 *Harv. J. Law Technol.* 299-320, 304.

¹⁰⁸ Notre traduction. MOZILLA FOUNDATION, préc., note 101.

¹⁰⁹ Notre traduction. CONSUMER WATCHDOG, préc., note 101, p. 6.

¹¹⁰ Ulrich AIVODJI, DESCHENES, CAROLINE, et WILSON, FREDERIC, « L'anonymisation des renseignements personnels au Québec : pistes de conformité technologiques et pratiques pour les entreprises privées », dans BARREAU DU QUEBEC - SERVICE DE LA FORMATION CONTINUE, *Développements récents en matière de protection des renseignements personnels et droit de l'intelligence artificielle* (2025), Éditions Yvon Blais, 571, coll. Éditions Yvon Blais, Montréal, 2025, p. 113-160, en ligne : <<https://edoctrine.caij.qc.ca/developpements-recents/571/c-ac8208b874e24a6c8364f7d8b5cc4372>> (consulté le 18 mars 2025).

les combinant avec d'autres informations révélatrices¹¹¹. La facilité de la réidentification est parfois étonnante : comme le décrit BC FIPA, en 2006, des chercheurs ont pu réidentifier les auteurs de critiques de films anonymes sur la base des caractéristiques de ces critiques et de quelques données provenant d'autres messages publiés en ligne¹¹². Plus récemment, des chercheurs ont constaté que les données de géolocalisation précises sont « hautement uniques » et que seuls quatre « points de données spatio-temporelles étaient suffisants pour identifier de manière unique 95 % des individus étudiés dans un ensemble de données de 1,5 million de personnes¹¹³ ». Une enquête menée en 2019 par le New York Times a également démontré à quel point il est facile de réidentifier les données de localisation et de les attribuer à des personnes identifiables. Les enquêteurs ont identifié de nombreuses personnes à partir d'un vaste ensemble de données en utilisant uniquement les données de localisation et d'autres informations facilement disponibles, telles qu'un message sur un réseau social ou le lieu de travail de la personne¹¹⁴. Comme le soulignent les auteurs, les données de localisation sont particulièrement faciles à réidentifier avec une personne spécifique, car :

In most cases, ascertaining a home location and an office location was enough to identify a person. Consider your daily commute: Would any other smartphone travel directly between your house and your office every day¹¹⁵?

Dans la fuite de Volkswagen mentionnée ci-dessus, un ensemble de données contenant des noms ou coordonnées d'utilisateurs a pu être lié à un autre ensemble de données contenant des points de géolocalisation, ce qui a permis la réidentification de celles de géolocalisation¹¹⁶.

Bien entendu, les fabricants automobiles, les courtiers en données et d'autres entreprises agrègent les données et ont donc accès à de nombreux points de données bien plus détaillés que ceux auxquels le public a normalement accès. C'est pourquoi :

Describing location data as anonymous is “a completely false claim” that has been debunked in multiple studies, Paul Ohm, a law professor and privacy researcher

¹¹¹ CONSUMER WATCHDOG, préc., note 101, p. 2; BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 12; COMMISSARIAT A LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « L'Internet des objets - Introduction aux enjeux relatifs à la protection de la vie privée dans le commerce de détail et à la maison » (17 février 2016), en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2016/iot_201602/> (consulté le 29 octobre 2024).

¹¹² BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 67.

¹¹³ Notre traduction. Yves-Alexandre DE MONTJOYE, César A. HIDALGO, Michel VERLEYSEN et Vincent D. BLONDEL, « Unique in the Crowd: The privacy bounds of human mobility », (2013) 3-1376 *Sci. Rep.* 1-5, DOI : 10.1038/srep01376.

¹¹⁴ Stuart A. THOMPSON et Charlie WARZEL, « Opinion | Twelve Million Phones, One Dataset, Zero Privacy », *The New York Times* (19 décembre 2019), en ligne : <<https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>> (consulté le 29 octobre 2024).

¹¹⁵ *Id.*

¹¹⁶ P. B. FLÜPKE, M. HOPPENSTEDT, M. KREIL, M. ROSENBAACH et R. WILKIN, préc., note 106.

at the Georgetown University Law Center, told us. “Really precise, longitudinal geolocation information is absolutely impossible to anonymize.”

“D.N.A.,” he added, “is probably the only thing that’s harder to anonymize than precise geolocation information.”¹¹⁷

Comme nous le verrons dans la section 5.1, lorsque la loi définit l'anonymat, elle exige que les données soient modifiées de manière à rendre irréversiblement impossible l'identification de la personne. Nous nous interrogeons donc sur la légitimité de la pratique des fabricants qui déclarent pouvoir utiliser des données dépersonnalisées ou anonymisées à n'importe quelle fin, alors que la réidentification de ce type de données s'avère assez facile.

En plus de collecter des quantités massives de renseignements personnels qui sont difficiles à anonymiser ou à dépersonnaliser, les fabricants cherchent aussi à conserver et à utiliser des données indéfiniment. Par exemple, en 2011, GM a tenté de modifier les conditions générales d'OnStar afin d'autoriser la collecte et le partage de données même après la fin de l'abonnement¹¹⁸. Dans leurs politiques de confidentialité, les fabricants se réservent souvent le droit de conserver les données pour une durée vaguement définie ; peu d'entre eux s'engagent à ne conserver les renseignements personnels que pendant une période spécifique¹¹⁹.

3.1.2 Partage de données avec des tiers

Les données générées et collectées par les voitures connectées sont parfois également collectées par des tiers ou partagées avec eux, et souvent à l'insu de l'utilisateur. De très nombreux acteurs autres que les fabricants peuvent avoir accès à certaines des données générées par les voitures connectées, par exemple les concessionnaires automobiles, les fournisseurs de services de télécommunication, les courtiers en données, les compagnies d'assurance, les fournisseurs de services tiers, les fournisseurs d'applications (Google et Apple, par exemple), les agences de location de voitures, les prêteurs, l'État et même d'autres consommateurs.

Certains de ces tiers obtiennent des données directement du véhicule connecté ou du consommateur, en contribuant à la fourniture d'un service connecté. Par exemple, les fournisseurs de services de télécommunications ont nécessairement accès à certaines des informations transmises par les véhicules sur leurs réseaux.

D'autres tiers ne collectent pas eux-mêmes les données, mais les obtiennent du fabricant. Les politiques de confidentialité des fabricants montrent que ces derniers partagent des

¹¹⁷ Notre soulignement. S. A. THOMPSON et C. WARZEL, préc., note 114.

¹¹⁸ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 18.

¹¹⁹ Voir la section 6 du rapport ; sur les 3 fabricants étudiés, seul Toyota a indiqué dans sa politique de confidentialité un échéancier précis pour la suppression des renseignements personnels. CONSUMER WATCHDOG, préc., note 101, p. 20. BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 78, p. 29.

données avec des tiers non nommés, qui ne jouent pas ou peu de rôle dans la fourniture d'un service connecté, par exemple des sociétés de marketing¹²⁰. L'analyse de la Fondation Mozilla a révélé que 84 % des politiques des fabricants automobiles analysées déclarent partager les données des utilisateurs avec des tiers non nommés et, comme indiqué ci-dessus (section 2.6.2), 76 % des fabricants se réservent le droit de vendre les renseignements personnels des utilisateurs¹²¹. Le rapport du *Government Accountability Office* (GAO) des États-Unis de 2017 a également constaté que les politiques de protection de la vie privée sont vagues sur ce point ; 13 des fabricants automobiles étudiés ont déclaré qu'ils « ne partageaient généralement pas de données avec des tiers non affiliés », mais certains ont cité des exemples de partage de données avec des concessionnaires affiliés ou des compagnies d'assurance. Ils ont nié partager des données avec des courtiers en données, mais certains ont déclaré partager et utiliser des données dépersonnalisées plus largement que des données non dépersonnalisées¹²². Comme indiqué à la section 2.6.2, il est établi que certains fabricants partagent effectivement des données avec des courtiers ou des agrégateurs ; nous pouvons donc conclure que soit les pratiques ont changé depuis la publication du rapport du GAO, soit ces entreprises sont considérées comme des « affiliés » ou des « prestataires de services », soit les données partagées sont « dépersonnalisées » selon la définition du fabricant.

Le partage des données avec des tiers présente plusieurs risques pour les consommateurs. Comme le souligne le BC FIPA, « chaque entité supplémentaire qui a accès aux données représente un point de vulnérabilité supplémentaire en cas d'accès et d'utilisation non autorisés ou non souhaités¹²³ ». En outre, les consommateurs peuvent ne pas se rendre compte qu'un tiers a accès à leurs informations personnelles et que ces informations peuvent être partagées avec d'autres acteurs à des fins multiples. Cette situation est bien illustrée par le cas, mentionné précédemment, du consommateur dont les données relatives à ses habitudes de conduite ont été partagées par le fabricant avec un courtier en données, puis revendues à son assureur, le tout à son insu¹²⁴.

Certains de ces tiers disposent de leurs propres ensembles de données concernant la personne, soit à partir de leurs propres interactions avec elle, soit à partir d'autres ensembles de données achetées. Ainsi, ils peuvent agréger les données de la voiture connectée avec ces informations pour générer de nouvelles déductions sur la personne. Même si le consommateur était à l'aise avec la collecte initiale des données, il est possible qu'il ne le soit pas avec les déductions faites à partir de leur agrégation.

L'impact de ce partage et de cette agrégation peut être subtil ou passer inaperçu pour le consommateur, qui peut ne jamais connaître l'étendue des données collectées à son sujet. L'impact peut aussi être plus apparent, par exemple en influant sur les publicités

¹²⁰ Voir la section 6. BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 108.

¹²¹ MOZILLA FOUNDATION, préc., note 101.

¹²² U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), préc., note 1, p. 14-15, 19.

¹²³ Notre traduction. BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 73.

¹²⁴ Section 2.6.2.

auxquelles le consommateur est exposé, ou en influençant certains prix ; ses primes d'assurance¹²⁵, par exemple, ou ses coûts¹²⁶.

En outre, le véhicule conserve en mémoire certaines données collectées jusqu'à ce qu'elles soient effacées, ce qui peut entraîner un partage involontaire des données entre les utilisateurs du véhicule. Plusieurs rapports ont fait état de situations dans lesquelles des consommateurs ont restitué des véhicules loués ou revendu leur voiture sans avoir préalablement effacé leurs données. Cela permet au nouveau propriétaire ou à l'utilisateur suivant d'accéder à des renseignements sensibles, tels que le nom de l'utilisateur précédent, sa liste de contacts et son historique d'appels. Cela peut même permettre au nouveau propriétaire ou au prochain utilisateur d'identifier l'utilisateur précédent et de le retrouver. Les consommateurs ignorent généralement que leurs données sont collectées et sauvegardées par le véhicule, et ne prennent donc pas les mesures nécessaires pour empêcher cette divulgation accidentelle¹²⁷.

3.1.3 Absence de consentement valable

Comme nous le verrons à la section 5.1, le consentement est un concept fondamental dans la législation en matière de la protection de la vie privée. Sauf exception, le droit à la collecte, à l'utilisation et au partage en dépend. Le consentement n'est considéré comme valable que s'il est libre et éclairé. L'examen de la littérature sur les pratiques des fabricants des voitures connectées en matière de protection de la vie privée suggère que les renseignements personnels des consommateurs sont souvent collectés, utilisés et communiqués sans leur consentement valable.

3.1.3.1 Absence de consentement éclairé

Les pratiques des fabricants de voitures connectées en matière de collecte, d'utilisation et de partage de données manquent souvent de transparence, de sorte qu'il est difficile – voire parfois impossible – pour les consommateurs de les comprendre.

Le Commissariat à la protection de la vie privée du Canada a publié des lignes directrices pour aider à clarifier ce qui est nécessaire, en matière d'information, pour que les consommateurs soient en mesure de donner un consentement éclairé. Il souligne par

¹²⁵ Voir l'exemple de Kashmir HILL, « Automakers Are Sharing Consumers' Driving Behavior With Insurance Companies », *The New York Times* (11 mars 2024), en ligne : <<https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>> (consulté le 30 octobre 2024).

¹²⁶ Bertin MARTENS et Frank MUELLER-LANGER, « Access to digital car data and competition in aftermarket maintenance services », (2020) 16-1 *J. Compet. Law Econ.* 116-141, 116, DOI : <https://doi.org/10.1093/joclec/nhaa005>.

¹²⁷ PRIVACY INTERNATIONAL, préc., note 84; Catherine HARROP, « Digital dirt: Why the data you leave in a rental car could threaten your privacy », *CBC News* (26 janvier 2017), en ligne : <<https://www.cbc.ca/news/canada/new-brunswick/digital-data-left-in-cars-1.3948659>> (consulté le 30 octobre 2024); LA FACTURE, « Quand des applis d'autos menacent votre vie privée », *Radio Canada* (22 mars 2022), en ligne : <<https://ici.radio-canada.ca/tele/la-facture/site/segments/reportage/395132/auto-vehicule-connecte-vie-privee-application-onstar-demarre>> (consulté le 30 octobre 2024).

ailleurs l'importance d'insister sur certains éléments clés afin de chercher à obtenir un consentement valide.

Bien que ces lignes directrices soient assez détaillées, nous notons que le Commissariat souligne l'importance de mettre l'accent sur les éléments suivants pour obtenir un consentement valide :

- Les renseignements personnels qui seront recueillis ;
- Les tiers auxquels les renseignements personnels seront communiqués ;
- Les fins auxquelles les renseignements personnels seront recueillis, utilisés ou communiqués ;
- Le risque de préjudice et autres conséquences.

Le Commissariat note également l'importance de permettre aux consommateurs d'accéder facilement à l'information nécessaire pour prendre une décision éclairée dans son intégrité¹²⁸.

La littérature suggère (et notre recherche dans la section 6 le confirme) que les fabricants ne respectent ces principes que dans les grandes lignes, et que leurs politiques sont tellement lacunaires qu'il est très difficile de comprendre exactement quelles sont leurs pratiques en matière de collecte de données. BC FIPA, la Fondation Mozilla, et le GAO ont tous mené des études approfondies sur les politiques de confidentialité des fabricants de voitures connectées¹²⁹. Leurs conclusions peuvent être résumées comme suit :

Les politiques sont rédigées de manière vague et générale lorsqu'elles décrivent quelles données sont collectées et partagées, et à quelles fins. Bon nombre des clauses les plus importantes, telles que celles qui expliquent quelles données sont collectées, comment elles sont utilisées et avec qui elles sont partagées, utilisent des termes vagues et sont incomplètes. Par exemple, les fabricants disent qu'ils collectent des informations « à des fins commerciales légitimes », une expression qui n'a pas de signification claire, ou ils utilisent des listes non exhaustives pour décrire les informations collectées et les personnes avec lesquelles elles sont partagées¹³⁰.

¹²⁸ COMMISSARIAT A LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Lignes directrices pour l'obtention d'un consentement valable » (24 mai 2018), en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gl_omc_201805/ (consulté le 19 mars 2025).

¹²⁹ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12; BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 78; U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), préc., note 1; MOZILLA FOUNDATION, préc., note 101. Les trois organisations ont analysé les contrats des fabricants et ont tenté de s'entretenir avec les représentants d'au moins quelques fabricants.

¹³⁰ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 101-104; BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 78, p. 23, 27, 29, 32; U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), préc., note 1, p. 17-18; MOZILLA FOUNDATION, préc., note 101; un rapport d'Option consommateurs est parvenu à ce même constat en ce qui concerne l'Internet des objets de manière plus générale : Jules BELANGER, Jeremy DE BEER et

La publication *The Drive* a tenté de clarifier certaines clauses contractuelles en contactant quatre fabricants pour obtenir des détails sur la vente de données télématiques à des tiers, car les politiques de confidentialité des entreprises n'étaient pas claires à ce sujet. Deux des entreprises (Ford et BMW) ont refusé de commenter et Honda s'est contentée de renvoyer la journaliste à sa politique de confidentialité sur laquelle elle demandait justement des précisions. Seule Kia a fourni une réponse, mais même cette réponse soulève plus de questions qu'elle n'en résout. L'entreprise a indiqué que Kia America ne vendait pas de données de géolocalisation des véhicules à des tiers, mais que certaines des « sociétés mondiales affiliées à Kia [pouvaient] avoir une relation de travail avec [le courtier en données] Otonomo¹³¹ ». Ainsi, même en discutant directement avec les fabricants, il semble souvent difficile, voire impossible, de comprendre l'étendue exacte de leurs pratiques.

Les politiques mentionnent des tiers, mais ne divulguent pas leur identité ni ce que ceux-ci font des données. Les tiers sont rarement nommés dans la politique de confidentialité des fabricants et l'étendue du partage avec des tiers n'est pas claire¹³². Les faits démontrent qu'ils peuvent utiliser les données reçues du fabricant d'une manière qui n'est pas clairement prévue dans les éléments pour lesquels un consentement est demandé. Le consommateur n'a souvent pas la possibilité de consentir à ces utilisations de ses données ou de les refuser. Par exemple, comme nous l'avons vu plus haut, les fabricants automobiles vendent des données à des agrégateurs de données, qui en tirent des conclusions et les revendent. Si les consommateurs peuvent consentir au partage de certaines données, par exemple l'historique de leur localisation, leur consentement ne leur est pas demandé à l'agrégation de ces données avec des informations recueillies sur eux par d'autres parties, une opération qui permet à de tiers anonymes d'en tirer des conclusions et de les revendre.

Les concepts d'anonymisation et de dépersonnalisation et les risques de réidentification ne sont pas expliqués¹³³.

Les politiques de protection de la vie privée semblent généralement passer sous silence les risques que représentent pour les consommateurs la collecte et le partage de données. Il s'agit d'une grave lacune, car les recherches suggèrent que la décision d'une personne de consentir ou non à la collecte et au partage de données dépend de son

Mohit SETHI, *Questions de droit d'auteur liées aux consommateurs sur l'Internet des objets : Une étude sur les objets connectés offerts aux consommateurs canadiens*, Option consommateurs, 2019, p. 30, en ligne : <<https://option-consommateurs.org/publications/questions-de-droit-dauteur-liees-aux-consommateurs-sur-linternet-des-objets-une-etude-sur-les-objets-connectes-offerts-aux-consommateurs-canadiens/>>.

¹³¹ Notre traduction. Victoria SCOTT, « Your Car Is Tracking You Just as Much as Your Smartphone Is—and Your Data Is at Risk », *The Drive* (8 juin 2022), en ligne : <<https://www.thedrive.com/news/think-your-smartphone-is-tracking-you-your-cars-doing-it-too>> (consulté le 21 octobre 2024).

¹³² Voir section 3.1.1.

¹³³ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 92; BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 78, p. 22 constate que davantage d'entreprises expliquent désormais le concept d'anonymisation, mais qu'elles n'expliquent pas les risques de réidentification; voir aussi J. BELANGER, J. DE BEER et M. SETHI, préc., note 130, p. 31.

évaluation de la gravité et de la probabilité des risques liés à la collecte. Les consommateurs seront plus enclins à consentir à la collecte et au partage de données s'ils pensent que les conséquences sont sans importance ou que le risque d'un problème en découlant est faible¹³⁴.

Les politiques font parfois référence aux pratiques des tiers. Cette pratique oblige le lecteur à consulter les politiques de confidentialité d'une autre partie pour comprendre l'étendue de la collecte et de l'utilisation des données¹³⁵.

Les entreprises laissent également à désirer en ce qui concerne la forme de la divulgation :

Les politiques sont rédigées dans un langage compliqué. Le rapport du GAO a analysé le langage utilisé dans les politiques pour en vérifier la lisibilité et a constaté qu'aucune des politiques analysées ne répondait à ce critère¹³⁶.

Les fabricants ont plusieurs politiques qui se trouvent à plusieurs endroits. De nombreuses politiques de confidentialité des fabricants sont réparties sur plusieurs pages Web ou dans divers documents. Par exemple, la Fondation Mozilla a constaté que Toyota disposait de 12 politiques, avis et déclarations de confidentialité distincts, certains s'appliquant de manière générale à tous les services Toyota tandis que d'autres ne s'appliquaient qu'à des équipements spécifiques (tels que les caméras embarquées), à des modèles de voiture spécifiques ou à des services connectés¹³⁷. BC FIPA a également noté que les entreprises disposent généralement de plusieurs politiques de protection de la vie privée, dont au moins une politique générale s'appliquant à tous les services fournis par une entreprise et une autre traitant spécifiquement des services connectés. Ils notent « qu'il n'est pas toujours évident de savoir quelle politique s'applique ou s'il y en a plus d'une qui s'applique¹³⁸ ».

Cette pratique peut empêcher les consommateurs de comprendre quelle politique s'applique dans quelle circonstance ou même de savoir s'ils ont pris connaissance de

¹³⁴ Nils KOESTER, Patrick CICHY, David ANTONS et Torsten Oliver SALGE, *Privacy Risk Perceptions in the Connected Car Context*, Hawaii International Conference on System Sciences, 2021, p. 4414-4423, p. 4420, DOI : 10.24251/HICSS.2021.536. Il convient de noter que Scott Jones, chef adjoint du Centre canadien pour la cybersécurité au Centre de la sécurité des télécommunications a déclaré devant le Comité sénatorial permanent des transports et des communications que les Canadiens sous-estiment souvent les menaces qui pèsent sur la cybersécurité: LE COMITÉ SENATORIAL PERMANENT DES TRANSPORTS ET DES COMMUNICATIONS, préc., note 66, p. 39.

¹³⁵ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 78, p. 55, 95; Voir aussi J. BELANGER, J. DE BEER et M. SETHI, préc., note 130, p. 31.

¹³⁶ U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), préc., note 1, p. 16-17.

¹³⁷ MOZILLA FOUNDATION, « Toyota », **Privacy Not Included: A Buyer's Guide for Connected Products* (2023), en ligne : <<https://foundation.mozilla.org/en/privacynotincluded/toyota/>> (consulté le 31 octobre 2024); MOZILLA FOUNDATION, préc., note 101; voir aussi J. BÉLANGER, J. DE BEER et M. SETHI, préc., note 130, p. 29.

¹³⁸ Notre traduction. BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 78, p. 23.

toutes les politiques applicables, particulièrement si le fabricant n'en fournit pas une liste exhaustive et ne les rend pas facilement accessibles.

Les politiques peuvent ne pas être portées à l'attention des consommateurs de manière pratique ou opportune. Par exemple, « un fabricant automobile affiche désormais une politique de confidentialité de 15 pages sur l'écran d'une voiture de 20 cm/8¹³⁹ ». En outre, comme pour les objets connectés en général, les consommateurs ne peuvent voir les conditions de la collecte et du partage de leurs renseignements personnels qu'après l'achat du bien, par exemple, lors de l'installation de l'application mobile ou lorsqu'ils commencent à utiliser le service¹⁴⁰.

Il ressort de cette analyse que les pratiques de divulgation des fabricants ne contribuent guère à éclairer le consommateur. Les politiques de confidentialité manquent de clarté en raison de l'absence de spécificité concernant les renseignements collectés et la manière dont ils sont partagés et utilisés, ainsi qu'en raison de l'absence de mention des risques et de la difficulté de comprendre et d'accéder à ces informations.

La différence entre ce qui est écrit dans la politique de confidentialité et la réalité de la collecte et du partage des données est frappante. Par exemple, dans un reportage du Washington Post sur les voitures connectées, un journaliste et un technicien ont démonté un système d'infodivertissement et ont récupéré des données sur des historiques d'appels, des coordonnées des contacts de l'utilisateur (leurs noms, adresses et photos), des identifiants de téléphone uniques et l'historique de la localisation du véhicule. Il n'y avait aucune mention du fait que le système collecte cette information dans le manuel de l'automobile ou dans la politique de confidentialité du fabricant¹⁴¹. Pour citer un autre exemple, l'article du New York Times discuté ci-haut sur la vente de données à des courtiers en données et à des assureurs révèle que certains consommateurs ont « opté » pour ce partage de données en s'inscrivant à un programme appelé OnStar Smart Driver, qui est décrit comme un service qui fournit de rétroaction sur la conduite du consommateur et qui peut obtenir des devis d'assurance pour ce dernier. La journaliste a observé que la procédure d'inscription à ce service ne mentionne pas le partage des données avec des tiers¹⁴².

Nous pouvons supposer que l'imprécision des politiques de confidentialité est à l'avantage de ceux qui cherchent à collecter et à utiliser ces données. Par exemple, le fondateur de Berla, une entreprise spécialisée dans l'extraction de données à partir de véhicules, suggère que le travail de son entreprise est facilité par le fait que les consommateurs

¹³⁹ EUROPEAN DATA PROTECTION SUPERVISOR (dir.), « Connected cars », *TechDispatch* 2019.3.1-4, 2, DOI : 10.2804/35031.

¹⁴⁰ Alexandre PLOURDE, *Retour vers le futur : l'Internet des objets et la protection de la vie privée*, 465, coll. Développements récents en droit à la vie privée, Montréal, Y. Blais, 2019, p. 33-66 aux pages 53-55, en ligne : <<https://edoctrine.caij.qc.ca/developpements-recents/465/369051330>>.

¹⁴¹ Geoffrey A. FOWLER, « What does your car know about you? We hacked a Chevy to find out. », *Washington Post* (17 décembre 2019), en ligne : <<https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out/>> (consulté le 4 novembre 2024).

¹⁴² K. HILL, préc., note 82.

ignorent que les véhicules collectent des données à partir de leurs téléphones lorsqu'ils les branchent¹⁴³.

Compte tenu de ces lacunes, il n'est pas surprenant que le Commissariat à la protection de la vie privée du Canada ait déclaré au comité sénatorial qui étudiait la question des voitures connectées qu'il avait observé

l'insatisfaction des consommateurs à l'égard du manque de clarté et d'accessibilité de nombreuses politiques de confidentialité de l'industrie. Il [le commissaire] a insisté sur la lisibilité de ces politiques afin de renseigner les consommateurs sur les types de renseignements qui sont recueillis à leur sujet, sur ce qu'en font les entreprises, sur les entités auxquelles elles les communiquent et sur les risques de dommages matériels ou d'atteinte à la réputation pouvant résulter de la divulgation des données les concernant. Le commissaire a aussi affirmé qu'il fallait éviter que les entreprises submergent les consommateurs d'une quantité d'information telle que ceux-ci soient incapables de faire des choix éclairés et d'exercer un véritable contrôle sur leurs renseignements personnels¹⁴⁴.

En résumé, il est difficile de voir comment le consentement peut être éclairé lorsque l'information fournie est loin d'être claire.

Enfin, il faut observer que même si toute l'information requise était facilement accessible, il n'est pas clair que les consommateurs comprendraient suffisamment la technologie et ses risques pour être en mesure de donner un consentement éclairé. La recherche démontre que, même quand nous parlons des technologies moins complexes que la voiture connectée, les consommateurs ne font pas nécessairement des choix rationnels lorsqu'il s'agit de consentir à partager des renseignements personnels. La littérature est divisée sur le degré de rationalité des décisions des consommateurs lorsqu'ils prennent des décisions concernant leur vie privée ; il semble qu'ils sont souvent influencés par des préjugés ou des intuitions plutôt que par un raisonnement correct¹⁴⁵. Par exemple, les consommateurs semblent être indûment enclins à consentir à la collecte et au partage de données en échange d'avantages tels que des incitations monétaires¹⁴⁶. Le processus décisionnel est également compromis par le déséquilibre des pouvoirs entre les acteurs d'une transaction, l'épuisement et l'apathie des consommateurs qui sont constamment

¹⁴³ Sam BIDDLE, « Your Car Is Spying on You, and a CBP Contract Shows the Risks », *The Intercept* (3 mai 2021), en ligne : <<https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/>> (consulté le 19 mars 2025). La vidéo de l'entrevue avec le fondateur est disponible à *Infotainment system car data: Forensic Lunch Feb 2015 interview with Berla's Ben LeMere*, 18 juin 2019, en ligne : <<https://www.youtube.com/watch?v=ChRFhyNUavc>> (consulté le 19 mars 2025).

¹⁴⁴ Notre soulignement. LE COMITE SENATORIAL PERMANENT DES TRANSPORTS ET DES COMMUNICATIONS, préc., note 66, p. 57-58.

¹⁴⁵ D. CHOI et P. B. LOWRY, préc., note 50, p. 4. Voir aussi notre discussion du sujet dans UNION DES CONSOMMATEURS, *Protection de la vie privée en ligne : Les consommateurs comme acteurs*, 2021, p. 152-154, en ligne : <<https://uniondesconsommateurs.ca/vieprivee-outils-rapport/>>.

¹⁴⁶ D. CHOI et P. B. LOWRY, préc., note 50, p. 4.

sollicités pour donner leur consentement, et le fait que les consommateurs ont du mal à évaluer les risques et les conséquences à long terme de la divulgation des données¹⁴⁷.

3.1.3.2 Absence de consentement explicite

Les fabricants de voitures connectées ne demandent pas nécessairement aux consommateurs de donner leur consentement explicite à la collecte de renseignements personnels¹⁴⁸. Par exemple, moins de la moitié des politiques de confidentialité étudiées par le GAO exigeaient le consentement explicite du consommateur pour le partage des données de localisation et de leurs habitudes de conduite avec des tiers¹⁴⁹. Au lieu d'exiger un consentement explicite, les fabricants déclarent parfois que l'utilisation de la voiture ou du service connectés constitue une forme de consentement implicite. Par exemple,

la politique de confidentialité de Subaru indique que même les passagers d'une voiture qui utilise des services connectés ont « consenti » à ce que ces derniers utilisent - et peut-être même vendent - leurs informations personnelles du simple fait qu'ils se trouvent à l'intérieur du véhicule¹⁵⁰.

Nous rapportons des pratiques similaires dans la section 6 du présent rapport.

S'il est demandé au consommateur de consentir explicitement à la collecte, à l'utilisation et au partage de données avant l'achat d'un véhicule, c'est généralement dans l'un des nombreux documents qu'il signe lors de l'achat ou de la location d'une voiture¹⁵¹. Le consommateur peut également donner son consentement « explicite » aux pratiques de collecte de données après l'achat, par exemple en cliquant « oui » sur l'écran de la voiture lorsqu'il est demandé s'il accepte la politique de confidentialité du fabricant.

Il n'est donc pas surprenant que les consommateurs canadiens ne sachent généralement pas s'ils ont consenti à la collecte de données lorsqu'ils ont acheté un véhicule connecté¹⁵².

¹⁴⁷ Lee A. BYGRAVE et Dag Wiese SCHATUM, « Consent, Proportionality and Collective Power », dans *Reinventing Data Protection?*, p. 157-173 aux pages 3-4, en ligne :

<http://dx.doi.org/10.1007/978-1-4020-9498-9_9> (consulté le 22 novembre 2024); Teresa SCASSA et Anca SATTler, « Location-Based Services and Privacy », (2011) 9-1 *Can. J. Law Technol.*, 118, en ligne : <<https://digitalcommons.schulichlaw.dal.ca/cjlt/vol9/iss1/6>>.

¹⁴⁸ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 107-109.

¹⁴⁹ U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), préc., note 1, p. 19.

¹⁵⁰ Notre traduction. MOZILLA FOUNDATION, préc., note 101.

¹⁵¹ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 78, p. 9.

¹⁵² Voir la section 4.2.4 et BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, *2019 Update, The Connected Car: Who is in the Driver's Seat*, Vancouver, 2019, p. 5, en ligne : <<https://fipa.bc.ca/2019-update-to-the-connected-car/>> avec références aux CAA National Opinion Poll July 2018 4CAA National Opinion Poll December 2018, July 2018.

3.1.3.3 Absence de consentement libre

La littérature indique également que les consommateurs n'ont pas non plus la possibilité de donner un consentement libre aux pratiques de collecte de données.

Les fabricants de voitures connectées donnent rarement aux consommateurs la possibilité de refuser leur consentement à la collecte, à l'utilisation et au partage des données, même lorsque les fins ne sont pas spécifiées ou nécessaires pour le fonctionnement du véhicule¹⁵³. La littérature révèle que les fabricants procèdent de deux manières. D'abord, ils regroupent la collecte, l'utilisation et le partage des données nécessaires et non nécessaires, exigeant du consommateur qu'il consente à toutes les utilisations de données mentionnées, qu'elles soient nécessaires ou non. Par exemple, les politiques des fabricants automobiles étudiées par BC FIPA exigeaient que les consommateurs consentent à la collecte, à l'utilisation et au partage des données à des fins telles que les études de marché, l'amélioration des services, les objectifs commerciaux internes, ou même « à toute fin » ou « pour toute raison »¹⁵⁴. Les politiques ne faisaient pas de distinction claire entre les finalités pour lesquelles les renseignements personnels étaient collectés ou utilisés, « ainsi, les données nécessaires à une finalité (par exemple, les données de compte nécessaires à la fourniture de services) peuvent être utilisées pour une autre finalité spécifique (par exemple, le marketing), *même si elles ne sont pas nécessaires pour cette seconde finalité*¹⁵⁵ » puisque le consommateur y a « consenti ».

Deuxièmement, les fabricants offrent rarement aux consommateurs le choix de refuser une collecte ou une utilisation particulière de leurs données. L'analyse du BC FIPA a révélé que la plupart du temps, la seule option offerte à l'utilisateur pour refuser la collecte, l'utilisation ou le partage des données était de cesser complètement d'utiliser la voiture ou les services connectés¹⁵⁶. Le rapport 2017 du GAO a également noté que les fabricants ont déclaré avoir obtenu un consentement explicite pour la collecte, l'utilisation et le partage des données, mais qu'ils ont généralement offert peu d'options pour s'y soustraire. Les 13 fabricants automobiles interrogés ont indiqué que les consommateurs ne pouvaient refuser le partage de certaines données qu'au prix de la perte de toutes les fonctionnalités du véhicule connecté¹⁵⁷. En 2019, BC FIPA a constaté que certains fabricants avaient identifié et catégorisé plus précisément qu'auparavant les finalités pour lesquelles ils collectaient des données, et ceux-ci donnaient maintenant aux utilisateurs la possibilité de refuser certaines collectes et utilisations (par exemple, avec les témoins sur leur site Web), mais que la plupart des collectes et des partages de données restaient néanmoins non optionnels si la personne veut utiliser les services connectés du

¹⁵³ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 112. Le rapport conclut que cette pratique est en violation flagrante de la loi sur la protection des données au Canada.

¹⁵⁴ *Id.*, p. 100-102; BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 152, p. 26-28.

¹⁵⁵ Notre traduction. BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 12, p. 103.

¹⁵⁶ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 21, p. 110; voir aussi CONSUMER WATCHDOG, préc., note 101, p. 9.

¹⁵⁷ U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), préc., note 1, p. 17-21; voir aussi CONSUMER WATCHDOG, préc., note 101, p. 9.

véhicule¹⁵⁸. Cela correspond aux conclusions auxquelles nous en arrivons dans la section 6 du présent rapport. Nous avons également observé, comme la Fondation Mozilla, que même lorsque les consommateurs ont la possibilité de refuser la collecte de données, les fabricants les dissuadent parfois de le faire. Par exemple, la politique de confidentialité de Tesla exige que les consommateurs contactent Tesla pour refuser la collecte de données et indique que le véhicule peut souffrir de « fonctionnalités réduites, de dommages graves ou de défaillance » en cas de refus¹⁵⁹.

Enfin, la liberté au consentement à la collecte, à l'utilisation et au partage des données est compromise par l'absence de concurrence entre les fabricants au plan des politiques de confidentialité. Comme le souligne la Fondation Mozilla, les consommateurs ne comparent pas les voitures en matière de protection de la vie privée lorsqu'ils font leurs achats, mais s'ils le faisaient, ils constateraient qu'il n'y a pas de réelle différence entre les marques. Les 25 fabricants automobiles étudiés par la Fondation souffrent tous des mêmes défauts majeurs en matière de protection de la vie privée¹⁶⁰. L'absence de concurrence quant au recours à ces pratiques et l'impossibilité de refuser la collecte et l'utilisation des données ne laisse d'autre choix au consommateur que d'accepter ces pratiques.

3.1.3.4 Passagers et passants

L'idée que les consommateurs consentent à la collecte, à l'utilisation et au partage des données par les fabricants de voitures connectées et les fournisseurs de services s'effondre encore plus lorsque nous considérons la situation des passagers et des passants. En théorie, les consommateurs acceptent les politiques et conditions de confidentialité des fabricants lorsqu'ils achètent ou louent une voiture ou décident d'utiliser le véhicule ou ses services connectés. Cependant, les fabricants et les fournisseurs de services collectent également des données sur les passagers et les passants qui n'ont aucune occasion de donner ou de refuser leur consentement.

Certaines voitures connectées ont la capacité de recueillir des données sur les passants, tels que les piétons et les autres véhicules. Par exemple, des modèles de Tesla sont dotés d'un « mode sentinelle » qui permet à la voiture de surveiller son environnement extérieur et qui enregistre une vidéo lorsqu'elle perçoit une menace¹⁶¹. Les voitures capables de conduite automatisée surveillent également leur environnement afin de détecter d'autres voitures ou individus¹⁶². Comme indiqué plus haut, Ford a déposé une demande de brevet pour une technologie qui permettrait aux voitures de surveiller la vitesse des autres¹⁶³.

¹⁵⁸ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 152, p. 29-31.

¹⁵⁹ Notre traduction. MOZILLA FOUNDATION, préc., note 101.

¹⁶⁰ *Id.*

¹⁶¹ Par exemple, TESLA INC., « Model 3 Owner's Manual », en ligne :

<https://www.tesla.com/ownersmanual/model3/en_us/GUID-F311BBCA-2532-4D04-B88C-DBA784ADEE21.html> (consulté le 4 novembre 2024). Ces données ne sont pas collectées par Tesla et restent enregistrées dans la voiture, mais elles peuvent être extraites par l'utilisateur (ou la police ou toute autre personne qui y a accès).

¹⁶² S. K. KHAN, N. SHIWAKOTI, P. STASINOPOULOS et M. WARREN, préc., note 49, 59.

¹⁶³ S. EDELSTEIN, préc., note 91.

Dans tous ces cas, la personne concernée n'a pas la possibilité de consentir ou de refuser la collecte et l'utilisation de ses données.

Il en va de même pour les passagers, dont la présence et le poids peuvent être détectés, mais qui peuvent également partager des données avec le véhicule lorsqu'ils y connectent leur téléphone ou leur appareil. Lorsque les fabricants abordent cette question, ils précisent qu'il incombe au propriétaire ou au locataire du véhicule d'informer ses passagers du fait que leurs données seront collectées, utilisées et partagées, et d'obtenir leur consentement à ces pratiques¹⁶⁴. Étant donné que les propriétaires et les locataires de véhicules ne sont généralement pas au courant de l'ensemble des politiques et des pratiques des fabricants en matière de données, il semble irréaliste et inapproprié de leur confier cette responsabilité.

Cette collecte ne pose pas nécessairement de problème si les données ne sont pas des renseignements personnels. Cependant, nous pouvons facilement imaginer une situation où les données collectées sont liées à une personne identifiable, par exemple si les images capturées par une caméra de surveillance sont comparées à celles d'une base de données de personnes identifiées, ou si l'information sur le passager est liée au numéro de SIM de son téléphone.

3.1.4 Manque de contrôle des données par les consommateurs

Comme nous allons voir dans la section 5.1, la législation canadienne relative à la protection de la vie privée prévoit le droit pour les individus d'accéder à leurs données personnelles détenues par les entreprises et de les corriger. Dans certains cas, la personne a le droit d'exiger d'une entreprise qu'elle supprime ses données.

En réalité, les fabricants de voitures connectées ne donnent pas nécessairement aux utilisateurs l'accès à leurs données¹⁶⁵. Le rapport du GAO note que certains des fabricants automobiles étudiés ont déclaré que les consommateurs avaient accès à leurs renseignements personnels, mais que la plupart des politiques de confidentialité n'étaient pas claires quant à l'étendue de cet accès. Lorsqu'ils ont été contactés, la majorité des fabricants automobiles ont indiqué que les utilisateurs pouvaient corriger certaines de leurs informations sur le site Web du fabricant, comme leurs coordonnées, mais qu'autrement, les consommateurs n'avaient qu'un accès limité à leurs données détenues par l'entreprise¹⁶⁶. En outre, la Fondation Mozilla a constaté que la plupart des fabricants

¹⁶⁴ MOZILLA FOUNDATION, préc., note 101. PRIVACY INTERNATIONAL, préc., note 84, p. 6.

¹⁶⁵ Voir, par exemple, G. A. FOWLER, préc., note 141. L'utilisateur a demandé au fabricant à deux reprises, sans succès, l'identité de ceux avec qui l'entreprise a partagé ses renseignements. Voir aussi J. BELANGER, J. DE BEER et M. SETHI, préc., note 130, p. 32 : dans cette analyse des politiques de confidentialité des biens connectés, y compris des voitures connectées, leurs auteurs ont trouvé que les consommateurs ont un accès limité à leurs données, sauf s'ils communiquent avec les entreprises par des voies légales.

¹⁶⁶ U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), préc., note 1, p. 17-21.

automobiles qu'elle a analysés ne mentionnaient pas le droit du consommateur à la suppression de ses renseignements personnels collectés¹⁶⁷.

Comme nous le verrons à la section 3.3.2, les constructeurs se sont opposés à ce que les utilisateurs et les mécaniciens indépendants aient accès aux données diagnostiques ou à celles sur l'état du véhicule, au motif qu'il s'agit de données propriétaires et que le partage de ces données entraînerait des risques pour la sécurité¹⁶⁸.

Les limites imposées à la capacité d'une personne d'accéder, de corriger ou de supprimer ses données personnelles collectées et générées par sa voiture suggèrent fortement que le véritable propriétaire de ces données, dans un sens significatif, est le fabricant et non l'individu concerné¹⁶⁹. Lorsque les auteurs du rapport du GAO ont contacté les fabricants automobiles pour leur demander à qui appartenaient les données générées par ces voitures, ils ont reçu des réponses différentes : sept ont déclaré que la réponse à la question n'était pas juridiquement claire ou qu'ils ne savaient pas, trois ont déclaré que le propriétaire du véhicule était propriétaire des données, mais que le fabricant avait une licence pour les utiliser, deux ont déclaré que le fabricant était propriétaire des données, et un a déclaré que le fabricant automobile était propriétaire des données anonymisées et que le consommateur était propriétaire des renseignements personnels¹⁷⁰. Privacy International a également étudié la question, en demandant qui contrôlait les données (et était donc responsable de leur suppression) dans les voitures de location. Elle a constaté que les sociétés de location et les fabricants imposent aux particuliers de supprimer les données contenues dans les systèmes d'infodivertissement avant de rendre la voiture, mais qu'il n'existe pas de consensus sur la question de savoir qui contrôle ces données¹⁷¹. Comme le souligne le Conseil des académies canadiennes, les questions de propriété sont encore plus floues lorsque plusieurs acteurs sont impliqués dans la production des données (comme un fournisseur de services et un fabricant) et lorsque les données sont stockées dans différentes juridictions qui peuvent avoir des règles différentes en la matière¹⁷².

¹⁶⁷ MOZILLA FOUNDATION, préc., note 101.

¹⁶⁸ Bien que les règles relatives à la portabilité des données se trouvent souvent dans la législation sur la protection de la vie privée, la portabilité est généralement davantage liée à des questions de concurrence qu'à des questions de protection de la vie privée. Voir Inge GRAEF, Nadezhda PURTOVA et Martin HUSOVEC, « Data Portability and Data Control: Lessons for an Emerging Concept in EU Law », (2018) 19-6 *Ger. Law J.* 1359-1398, DOI : 10.1017/S2071832200023075.

¹⁶⁹ S. ZHANG, préc., note 107, 319. L'auteure explique que la notion de propriété des données n'est pas évidente et que les droits d'accès, de limitation de l'accès, d'utilisation et de destruction des données sont probablement les substituts les plus proches de la « propriété » dans le contexte de la voiture connectée.

¹⁷⁰ U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), préc., note 1, p. 13.

¹⁷¹ PRIVACY INTERNATIONAL, préc., note 84, p. 11.

¹⁷² THE COUNCIL OF CANADIAN ACADEMIES, préc., note 58, p. 86.

3.1.5 Risque de fuite ou de vol de données

Les questions de cybersécurité liées à la connectivité des voitures sortent généralement du cadre du présent rapport, mais elles seront brièvement abordées à la section 3.4. Pour la présente section, il suffit de dire que, comme les voitures connectées génèrent, collectent et transmettent de grandes quantités de renseignements personnels, il existe un risque de fuite ou de vol de ces données, soit à partir du véhicule lui-même, soit à partir de la base de données d'un fabricant ou d'une tierce partie. Il s'agit d'un risque important pour les consommateurs, compte tenu de la sensibilité des renseignements. Comme le souligne le BC FIPA, « plus il y a de données collectées et stockées, plus il y a de risques de violations potentielles »¹⁷³.

Le rapport du GAO note que tous les fabricants automobiles étudiés utilisent « des politiques et des technologies pour protéger les données »¹⁷⁴ et nous avons observé la présence des mêmes phrases dans les politiques que nous avons analysées dans la section 6 du rapport. Toutefois, la Fondation Mozilla a estimé qu'il était impossible de savoir si les fabricants automobiles cryptaient les données collectées dans une voiture, ce qui serait le « strict minimum » du point de vue de la cybersécurité¹⁷⁵. Comme nous le verrons à la section 3.4, certains fabricants, à tout le moins, ne cryptent pas leurs données.

3.2 Atteinte au droit de propriété

Lorsqu'un consommateur se procure un véhicule, il pense généralement qu'il en est le propriétaire et qu'il dispose à ce titre de certains droits : de pouvoir utiliser le véhicule, ainsi que toutes ses fonctionnalités et pièces, de le contrôler et de le réparer à son gré. Pourtant, la propriété dans l'ère numérique est complexe. L'intégration d'ordinateurs et de logiciels dans de nombreux biens de consommation, comme les voitures connectées, remet en question les fondements mêmes du droit de propriété du consommateur sur ces biens connectés.

Le droit accorde une place particulière aux biens immatériels, comme le logiciel. Les règles de droit qui encadrent les biens immatériels sont, à bien des égards, différentes de celles qui encadrent les biens corporels, et les deux peuvent s'appliquer au même objet, avec un ensemble de règles s'appliquant au bien physique et un autre à la composante immatérielle. Dans le cas des voitures connectées, le consommateur acquiert le bien matériel, la voiture, mais le fabricant conserve un droit de propriété sur l'élément immatériel du bien comme son logiciel par le biais du contrat de licence d'utilisation et du régime juridique de propriété intellectuelle. Comme le fabricant reste titulaire de droits de propriété sur les logiciels intégrés au bien, il continue de posséder des droits sur le bien, même après son acquisition par le consommateur. Ainsi, l'intégration des éléments

¹⁷³ Notre traduction. BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 21, p. 66.

¹⁷⁴ Notre traduction. U. S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), préc., note 1, p. 17-21.

¹⁷⁵ MOZILLA FOUNDATION, préc., note 101.

matériels et logiciels, tous deux nécessaires à l'usage d'un bien connecté, fait intervenir des notions de droit de propriété concurrentes.

Ce partage des droits de propriété du bien a pour effet de limiter les droits de propriété du consommateur en faveur du fabricant. Comme le dit un auteur, à l'ère numérique :

On a donc assisté à une sorte de phénomène de vases communicants : à mesure que la propriété intellectuelle se durcissait, la propriété matérielle paraissait se dissoudre, traduisant un déséquilibre croissant entre industriels – de la culture ou d'autres secteurs – et consommateurs¹⁷⁶.

Cette problématique est antérieure à la connectivité : les droits de propriété d'un bien peuvent être divisés pour les biens non connectés pour autant qu'ils contiennent une composante logicielle. Toutefois, les proportions respectives des droits changent en faveur du fabricant lorsque l'objet est connecté. Dans le cas des biens non connectés, le partage de la propriété est déterminé au moment de la vente. Si le fabricant d'un bien non connecté souhaite conserver et protéger ses droits sur le logiciel, il doit mettre en place les mesures pour le faire avant l'achat, notamment par le biais de la licence de l'utilisateur final et des verrous numériques qui contrôlent l'accès au logiciel et son utilisation par le consommateur. Ces derniers doivent être incorporés dans l'objet avant la vente, puisque le fabricant n'a plus accès au logiciel une fois que le consommateur possède le bien. Toutefois, dans le cas des objets connectés, le fabricant conserve un contrôle actif sur le logiciel, et donc sur le bien, après l'achat ; il peut ainsi modifier les conditions de l'utilisation du logiciel, voire même ses fonctionnalités, après que le consommateur ait acquis le bien.

Ownership is fragmented by the very nature of the IoT [Internet of Things] product. Even after the market exchange is complete and the good has been fully paid for, the vendor retains substantial power and jurisdiction over it. The buyer, the ostensible legal owner of the good, can do with it only what the vendor allows; she does not meaningfully own it in the orthodox sense¹⁷⁷.

Grâce à leur connectivité, les biens connectés sont soumis au contrôle direct de leurs fabricants, ce qui n'est jamais le cas des biens non connectés. Comme décrit dans la section 2, la connectivité permet au fabricant de recevoir en temps réel de l'information sur le véhicule et son utilisation, de contrôler certaines fonctionnalités du bien à distance, de le mettre à jour et de bloquer ou débloquer à distance des fonctionnalités du bien. Ainsi, la connectivité donne lieu à la possibilité d'une « surveillance continue des appareils intelligents et de leurs utilisateurs » ainsi qu'à la capacité du fabricant de modifier directement le logiciel du produit, ce qui lui permet de modifier les caractéristiques et les fonctionnalités du produit après la transaction initiale¹⁷⁸.

¹⁷⁶ Lionel MAUREL, « Que reste-t-il de la propriété dans l'environnement numérique ? », (2020) 2-10 *Délibérée* 19-26, 23, DOI : <https://doi.org/10.3917/delib.010.0019>.

¹⁷⁷ Ajay RAINA et M. PALANISWAMI, « The ownership challenge in the Internet of things world », (2021) 65 *Technol. Soc.*, 1-3.

¹⁷⁸ Notre traduction. N. TUSIKOV, préc., note 68 à la page 130.

Pour cette raison, une autre auteure réfère au concept de « droit de propriété précaire » pour décrire le déséquilibre en matière de droits de propriété, entre le consommateur et le fabricant du bien connecté :

Consumers are only entitled to a “precarious” form of ownership of smart products, which only entitles them to a licence to use—not to control and use as they see fit the goods they purchase—and companies can change the conditions of “ownership” after purchase¹⁷⁹.

Nous présenterons dans cette section les risques associés à ce droit de propriété précaire pour les propriétaires de voitures connectées. La littérature sur cette question réfère particulièrement à l'Internet des objets¹⁸⁰ dont fait partie la voiture connectée. Les risques présentés ne sont pas, pour la plupart, spécifiques à la voiture connectée, mais ils sont emblématiques d'une problématique plus large liée à l'incorporation de plus en plus de fonctionnalités connectées à des biens matériels.

3.2.1 Mise en œuvre et surveillance des contrats de licence

Comme expliqué ci-dessus, les fabricants conservent généralement la propriété des logiciels intégrés dans un produit par le biais d'un contrat de licence d'utilisateur final (CLUF). Les CLUF ne sont pas une nouveauté, mais leur mise en application et leur portée sont toutefois renforcées par la connectivité et l'intégration du logiciel dans les biens physiques. La connectivité permet de surveiller et de faire respecter à distance les conditions d'utilisation du logiciel. L'intégration du logiciel dans un objet physique connecté donne au fabricant un contrôle important sur le bien, qui renforce sa capacité de faire respecter ses conditions d'utilisation du logiciel, comme nous le verrons.

L'Organisation mondiale de la propriété intellectuelle (OMPI) définit le contrat de licence comme : « un contrat juridiquement contraignant en vertu duquel le titulaire de la propriété intellectuelle associée à une technologie recherchée (le donneur de licence) autorise un tiers (le preneur de licence) à utiliser cette propriété intellectuelle selon des modalités (conditions) définies dans le contrat¹⁸¹. » Lors de l'achat d'un bien numérisé assujéti à un tel contrat, le consommateur « accepte » le CLUF. Il ne devient donc pas propriétaire du

¹⁷⁹ *Id.* à la page 126.

¹⁸⁰ L'Internet des objets est un « ensemble des objets connectés à Internet capables de communiquer avec des humains, mais aussi entre eux, grâce à des systèmes d'identification électronique, pour collecter, transmettre et traiter des données avec ou sans intervention humaine » OFFICE QUEBECOIS DE LA LANGUE FRANÇAISE, « Internet des objets », *Grand dictionnaire terminologique* (2015), en ligne : <<https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26529845/internet-des-objets>> (consulté le 20 mars 2025).

¹⁸¹ L'ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE, « Accords de transfert de technologie », *OMPI*, en ligne : <<https://www.wipo.int/fr/web/technology-transfer/agreements>> (consulté le 27 novembre 2024).

composant immatériel, c'est-à-dire le logiciel : il dispose simplement d'une licence lui permettant de l'utiliser sous certaines conditions¹⁸².

Nous avons remis en question dans un rapport précédent la validité de la notion que les consommateurs consentent à ce type de contrat, d'autant plus que, dans de nombreux cas, les commerçants ne divulguent pas leurs contrats de licence avant l'achat¹⁸³. De plus, le contenu et la forme des contrats de licence d'utilisation sont particulièrement complexes et il est permis de douter de la compréhension de ces contrats par le consommateur moyen¹⁸⁴. Selon la *Federal Trade Commission* (FTC) aux États-Unis, le degré de compréhension des consommateurs sur ce qu'ils achètent et la différence entre les biens matériels et les logiciels qu'ils contiennent est, à tout le moins, incertain¹⁸⁵. En effet, la plupart des consommateurs s'attendent raisonnablement à pouvoir utiliser un bien connecté qu'ils achètent de la même façon qu'ils utilisent des biens qualifiés de « traditionnels »¹⁸⁶. De nombreux consommateurs reconsidéreraient l'achat d'un bien s'ils savaient qu'il existe des restrictions à son utilisation, par exemple des restrictions à sa réparation; on pourrait dans ce cas considérer que les commerçants passent ainsi sous silence un fait important¹⁸⁷.

À cela s'ajoute le fait que les consommateurs n'ont pas la possibilité de refuser certaines clauses spécifiques incluses aux contrats de licence d'utilisation ou d'en négocier la teneur. Dans un contexte lié à l'achat de biens de consommation, ces contrats sont identifiés comme des contrats d'adhésion qui obligent le consommateur à accepter ou refuser en bloc l'entièreté du contrat¹⁸⁸. Ainsi le refus d'accepter l'entièreté des conditions d'utilisation prévue à un contrat donné entraînerait l'impossibilité complète d'utiliser le logiciel¹⁸⁹.

Dans cette perspective, l'étendue des clauses qui peuvent se retrouver dans ses contrats et leur conflit avec les droits de propriété historiquement conférés aux propriétaires d'un bien matériel sont préoccupants. Perzanowski et Schultz rapportent des restrictions en

¹⁸² UNION DES CONSOMMATEURS, *Contrat de licence d'utilisateur final : acceptez-vous toutes les conditions?*, 2010, p. 9-10, en ligne : <<https://uniondesconsommateurs.ca/wp-content/uploads/2020/12/03-R10-CLUF-f.pdf#>>.

¹⁸³ *Id.*, p. 30-31.

¹⁸⁴ Daniel A. HANLEY, Claire KELLOWAY et Sandeep VAHEESAN, *Fixing America: Breaking Manufacturers' Aftermarket Monopoly and Restoring Consumers' Right to Repair*, Open Markets Institute, 2020, p. 14, en ligne : <<https://ssrn.com/abstract=4089852>>; Guido NOTO LA DIEGA et Ian WALDEN, « Contracting for the 'Internet of Things': Looking into the Nest », *Queen Mary Sch. Law Leg. Stud. Res. Pap.* 2016.219/2016.1-29, 5-11; J. BELANGER, J. DE BEER et M. SETHI, préc., note 130, p. 50.

¹⁸⁵ N. TUSIKOV, préc., note 68 à la page 139.

¹⁸⁶ *Id.* à la page 133.

¹⁸⁷ Aaron PERZANOWSKI, *The Right to Repair: Reclaiming the Things We Own*, Cambridge University Press, 2021, p. 202-203.

¹⁸⁸ Brian T. YEH, *Repair, Modification, or Resale of Software-Enabled Consumer Electronic Devices: Copyright Law Issues*, Congressional Research Service Report, R44590, Prepared for Members and Committees for the United States Congress, 2016, p. 19, en ligne : <<https://sgp.fas.org/crs/misc/R44590.pdf>>.

¹⁸⁹ N. TUSIKOV, préc., note 68 à la page 129.

matière de droits d'utiliser, de contrôler, de garder et de transférer le bien qui a fait l'objet d'une vente¹⁹⁰.

L'inclusion de clauses contractuelles limitant les droits des utilisateurs et donc corollairement les droits de propriété sur l'objet matériel dont les fonctions principales sont liées aux logiciels est une tendance présente dans le marché des véhicules. Par exemple, des limitations contractuelles ont été incluses dans des contrats de licence d'utilisation de logiciels intégrés aux véhicules afin d'imposer des limites en matière de réparation¹⁹¹. Un exemple célèbre est celui des tracteurs John Deere, dont la licence d'utilisation prétendait ne donner à l'acheteur que le droit d'utiliser le bien, et non celui de le réparer. La réparation non autorisée du bien était considérée comme une violation de l'accord pouvant entraîner sa résiliation ; en d'autres termes, l'entreprise pouvait supprimer l'accès de l'acheteur au logiciel, ce qui rendait le tracteur inutilisable¹⁹².

En outre, les CLUF des fabricants automobiles peuvent interdire d'accéder au logiciel du véhicule ou de le modifier, puisque le consommateur n'en est pas propriétaire:

General Motors, for example, argues that customers who wish to access or modify the vehicle's software in order to repair or tinker with the vehicle "incorrectly conflate ownership of a vehicle with ownership of the underlying computer software in a vehicle" (General Motors 2015, 10). According to General Motors, then, the customer purchased all non-software elements of the vehicle, not its software-enabled elements¹⁹³.

Les licences d'utilisation peuvent inclure des clauses qui prévoient des sanctions en cas de violations au contrat¹⁹⁴. Dans le cas d'un bien connecté, le fabricant inclut souvent une clause qui lui permet de mettre fin au service connecté, comme sanction ou même à tout moment et pour toute raison¹⁹⁵. La connectivité permet aux fabricants de surveiller l'utilisation à distance et de mettre en œuvre ces clauses. Si le consommateur ne respecte pas les conditions d'utilisation, le fabricant a le pouvoir et les moyens de désactiver le logiciel du bien, mettant ainsi fin à la capacité de l'utilisateur de s'en servir¹⁹⁶. De plus, les

¹⁹⁰ Aaron PERZANOWSKI et Jason SCHULTZ, *The End of Ownership : Personal Property in the Digital Economy*, The MIT Press, Cambridge, MA, 2016, p. 23.

¹⁹¹ Pamela SAMUELSON, « Freedom to Tinker », (2016) 17 *Theor. Inq. Law Forthcom.* 1-31, 588.

¹⁹² FEDERAL TRADE COMMISSION, *Nixing the Fix: An FTC Report to Congress on Repair Restrictions*, 2021, en ligne : <https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf>; D. A. HANLEY, C. KELLOWAY et S. VAHEESAN, préc., note 184, p. 12-13.

¹⁹³ N. TUSIKOV, préc., note 68 à la page 129. Voir aussi la section 6.

¹⁹⁴ *Id.* à la page 129.

¹⁹⁵ *Id.* aux pages 123, 130. Voir la section 6 de ce rapport.

¹⁹⁶ Pascale CHAPDELAIN, Anthony D. ROSBOROUGH, Aaron PERZANOWSKI, Bitā AMANI, Sara BANNERMAN, Carys CRAIG, Lucie GUILBAULT, Cameron J. HUTCHISON, Ariel KATZ, Alexandra MOGYOROS, Graham J. REYNOLDS, Teresa SCASSA et Myra TAWFIK, *A Modern Copyright Framework for the Internet of Things (IoT): Intellectual Property Scholars' Joint Submission to the Canadian Government Consultation*, Consultation on a Modern Copyright Framework for Artificial Intelligence and the Internet of Things to the Minister of Innovation, Science, Industry & the

contrats des fabricants de voitures connectées peuvent aussi indiquer qu'ils se réservent le droit de faire des mises à jour à distance sur les logiciels de l'automobile sans donner d'avis et sans demander le consentement du propriétaire de la voiture¹⁹⁷.

3.2.2 Désactivation et contrôle à distance de la voiture connectée

Un des risques pour le consommateur est donc le fait que le fabricant d'un bien connecté peut mettre fin à l'accès au logiciel du bien ou changer ses fonctionnalités, et ce, à distance et sans le consentement du consommateur. Cette désactivation à distance peut être exécutée par le fabricant qui veut mettre fin au service offert ou même en cas de violation de contrat par le consommateur¹⁹⁸. Cette pratique fait partie d'un phénomène plus large qui est connu sous le nom de « *bricking* » ; un bien connecté qui perd toute utilité parce que son logiciel ne fonctionne plus se transforme ainsi en objet inerte, ou en brique, pour ainsi dire, d'où le nom. Les objets connectés peuvent perdre leur fonctionnalité de cette manière, d'un seul coup ou progressivement, pour plusieurs raisons et non seulement en cas de désactivation du bien à distance pour violation du contrat. Par exemple, un bien peut être sujet au *bricking* si le fabricant cesse de mettre à jour le logiciel :

*Bricking is the remote destruction of [Internet of Things] products by manufacturers who strategically withhold software updates, which can contain essential security patches, or issue software updates designed to degrade the product's functionality. Depending on how products are bricked, they may cease to operate immediately or slowly lose functionality over time*¹⁹⁹.

La désactivation du bien peut également se produire involontairement, par exemple si l'entreprise rend le fonctionnement de son service dépendant de celui de ses serveurs, ces derniers pouvant tomber en panne²⁰⁰. Il y a aussi eu plusieurs cas où des biens intelligents sont devenus inutilisables lorsque l'entreprise a décidé de cesser d'offrir le service connecté ou a fait faillite²⁰¹.

Minister of Canadian Heritage, unpublished, archived at Schulich Law Scholars, Dalhousie University, 2021, p. 6, en ligne : <<https://digitalcommons.schulichlaw.dal.ca/reports/69>>.

¹⁹⁷ A. PERZANOWSKI et J. SCHULTZ, préc., note 190, p. 147.

¹⁹⁸ Voir la section 6 et voir Peter ROTT, « The Digitalisation Of Cars And The New Digital Consumer Contract Law », (2021) 12-2 *JIPITEC* 156-168, 163.

¹⁹⁹ N. TUSIKOV, préc., note 68 à la page 137.

²⁰⁰ Voir l'exemple des thermostats Netatmo cité dans Emmanuel NETTER, « Le droit de propriété dans l'univers numérique », (2022) 18 *Ann. Mines* 9-14, 13.

²⁰¹ Voir l'exemple des vélos électriques de VanMoof dans U.S. PUBLIC INTEREST RESEARCH GROUP EDUCATION FUND & IFIXIT, *Petition for Rulemaking to Protect Consumers' Right to Repair*, Before the United States Federal Trade Commission, Fairmark Partners LLP, 2023, p. 8, en ligne : <<https://pirg.org/edfund/resources/ftc-petition-for-rulemaking-to-protect-consumers-right-to-repair/>>. Pour les exemples de Jibo, Nest (Revolv), et Insignia, voir A. PERZANOWSKI, préc., note 187, p. 7-8.

Non seulement les voitures peuvent être mises à jour et désactivées à distance, elles peuvent également être contrôlées à distance²⁰². Une demande de brevet déposée par Ford illustre bien les défis au droit de propriété et d'usage d'un bien par son propriétaire dans ce contexte : dans le brevet de 2023, l'entreprise propose de couper la fonctionnalité de la radio, du régulateur de vitesse, des vitres, du déverrouillage des portes, voire du moteur du véhicule dans le cas d'un défaut de paiement de la voiture. En théorie, le véhicule pourrait également émettre un signal sonore en continu ou même se rendre lui-même à un autre endroit dans le cas d'un véhicule autonome²⁰³.

L'offre de services et de fonctionnalités connectés ébranle aussi l'idée de propriété sur un bien et constitue un modèle d'affaires qui peut être employé comme un moyen d'extraire davantage de revenus sur l'utilisation d'un bien même après sa vente. Dans ce cas, le consommateur paie pour le bien matériel et ce dernier peut devenir un vecteur permettant la proposition de services moyennant des frais supplémentaires.

We define “tethering” as the strategy of maintaining an ongoing connection between a consumer good and its seller that often renders that good in some way dependent on the seller for its ordinary operation. Such products present as physical goods but often function as vessels for the delivery of services²⁰⁴.

Il existe déjà des exemples dans l'industrie automotrice. Comme nous l'avons décrit ci-haut, dans la section 2.5.7 (déblocage de fonctionnalités à distance), plusieurs fabricants ont commencé à offrir des abonnements non seulement pour les services connectés, mais également pour débloquent certaines fonctionnalités physiques de la voiture, comme les sièges chauffants. On peut constater que les consommateurs sont parfois surpris de découvrir qu'une fonctionnalité pourtant intégrée dans la voiture achetée n'est disponible ou utilisable que sur paiement d'un abonnement supplémentaire. Par exemple, lorsque Mazda a annoncé que la fonctionnalité de démarrage à distance serait désormais un service payant, plusieurs consommateurs ont exprimé leur mécontentement et leur confusion. Mazda s'est défendue en indiquant que cette fonctionnalité avait été présentée aux consommateurs concernés comme un service exclu de la vente du véhicule et la raison pour laquelle les acheteurs de nouveaux modèles ont pu utiliser cette fonctionnalité gratuitement est qu'ils ont bénéficié d'un essai gratuit de 3 ans²⁰⁵.

En effet, il peut être difficile pour le consommateur de déterminer ce qu'il se procure lors de l'achat si certaines fonctionnalités, offertes sous forme de services, sont amenées à

²⁰² Voir aussi la section 3.4 sur la cybersécurité. A. RAINA et M. PALANISWAMI, préc., note 177, 3.

²⁰³ Paige SMITH et BLOOMBERG, « Ford wants to be able to shut down your air conditioner and radio if you miss a car payment—and the car could even drive away on its own », *Fortune* (2 mars 2023), en ligne : <<https://fortune.com/2023/03/02/ford-patent-late-payments-shut-off-air-conditioning-radio/>> (consulté le 20 mars 2025).

²⁰⁴ Aaron K. PERZANOWSKI, Chris Jay HOOFNAGLE et Aniket KESARI, « The Tethered Economy », (2019) 87-4 *George Wash. Law Rev.*, 785.

²⁰⁵ José RODRÍGUEZ JR, « Mazda Quietly Ditched Key Fob Remote Start for Subscription App (Updated) », *The Drive* (5 août 2024), en ligne : <<https://www.thedrive.com/news/mazda-quietly-ditched-key-fob-remote-start-for-subscription-app>>.

être modifiées avec le temps²⁰⁶. Ainsi, la nature de la transaction entre le consommateur et le vendeur se trouve altérée par la connectivité, et une transaction ressemblant en tout point à une vente de produit peut se transformer en une relation basée sur l'offre de services²⁰⁷.

*The shift to chipification is also facilitating a concerning shift toward subscription models of car ownership, in which a consumer buys the physical car but has to pay subscription fees for different services on the car, ranging from fuel efficiency boosts to heated seats to autonomous driving systems to adaptive cruise control*²⁰⁸.

Avec un modèle de transaction où plusieurs des fonctionnalités d'un bien sont liées à l'achat de services supplémentaires, les droits liés à l'usage et au transfert d'un bien qui étaient liés au transfert de propriété sont incertains et dépendent grandement de l'offre de service évolutive des entreprises.

*For tethered products, it is not the wear and tear of physical components, but the business decisions of the seller that often dictate whether a product continues to operate*²⁰⁹.

Il est ainsi démontré que le contrôle que conservent les fabricants sur les logiciels intégrés aux voitures connectées remet en question la notion de droit de propriété. La possibilité pour les fabricants de modifier, d'interrompre à distance ou même de contrôler les fonctionnalités de la voiture connectée peuvent interférer avec les droits conférés aux propriétaires d'une voiture connectée d'user, de jouir et de disposer librement de leur bien.

3.2.3 Obsolescence

Enfin, il faut noter que la connectivité des voitures peut avoir un impact sur leur durée de vie et leur obsolescence, notamment parce que les nouvelles technologies et les logiciels intégrés dans la voiture peuvent avoir une durée de vie utile plus courte que celle du véhicule. Ceci est un problème courant avec les systèmes d'infodivertissement et de navigation intégrés dans les véhicules connectés, qui deviennent obsolètes en quelques années et qui sont rapidement dépassés par rapport à des services comparables disponibles sur les nouveaux téléphones intelligents²¹⁰. Cette durée de vie est bien plus courte que celle d'une voiture, qui peut aisément aller jusqu'à 15 ans²¹¹.

Ce type d'obsolescence prématurée peut également se produire lorsqu'il y a des failles dans le logiciel du véhicule. Des millions de véhicules de plusieurs grands fabricants ont

²⁰⁶ A. K. PERZANOWSKI, C. J. HOOFNAGLE et A. KESARI, préc., note 204, 809-810.

²⁰⁷ *Id.*, 815.

²⁰⁸ M. FORELLE, préc., note 9, 8.

²⁰⁹ A. K. PERZANOWSKI, C. J. HOOFNAGLE et A. KESARI, préc., note 204, 811.

²¹⁰ L. DETERMANN et B. PERENS, préc., note 16, 923-924.

²¹¹ B. MARTENS et F. MUELLER-LANGER, préc., note 126, 116.

déjà été rappelés en raison de problèmes de logiciels²¹². En outre, certains types de logiciels, comme les systèmes d'exploitation, doivent régulièrement être mis à jour pour bénéficier de correctifs de sécurité. Les véhicules équipés de logiciels peuvent devenir prématurément obsolètes en raison de bogues ou de risques de sécurité s'ils ne sont pas mis à jour. Cette situation est problématique pour le consommateur qui se retrouve avec une voiture partiellement obsolète plusieurs années avant la fin de la durée de vie du bien physique. Par le passé, des fabricants ont fait payer ces mises à jour aux consommateurs ou n'ont mis à jour que la technologie des modèles de véhicules relativement récents, laissant les plus anciens devenir obsolètes²¹³. Les contrats analysés dans la section 6 de ce rapport limitent la responsabilité du fabricant en ce qui concerne la disponibilité des mises à jour.

Enfin, la technologie connectée peut elle-même devenir obsolète, rendant toutes les fonctions connectées connexes inutilisables, potentiellement avant la fin de la durée de vie normale du véhicule. Par exemple, dans les années 90 et au début des années 2000, GM utilisait le réseau sans fil de première génération (1G) pour son service connecté OnStar, et les systèmes télématiques installés lors de la fabrication de ses voitures sont uniquement analogiques²¹⁴. À cette époque, un réseau sans fil de deuxième génération (2G), plus performant et utilisant la technologie numérique, est déjà présent. De plus, au début des années 2000, l'introduction du réseau sans fil 3G permet l'accès plus rapide à Internet et améliore les capacités de transmission audio et vidéo²¹⁵. Ainsi, en quelques années, l'utilisation de la technologie analogique dans les véhicules équipés des services OnStar s'est révélée problématique. En 2002, une décision de la *Commission fédérale des communications* aux États-Unis (FCC) signait l'arrêt du système analogique dans un horizon de cinq ans²¹⁶. La décision a eu des conséquences directes sur approximativement 2 millions de consommateurs pour lesquels la technologie de leur voiture est devenue désuète pendant cette période et a cessé de donner accès aux services OnStar²¹⁷.

Toutefois, la connectivité peut également atténuer ce problème d'obsolescence grâce à la capacité du fabricant de mettre à jour le logiciel du véhicule à distance. Ces mises à jour permettent d'actualiser le logiciel (si le matériel physique le permet) et de prolonger la durée de vie de la technologie dans le véhicule. Par exemple, GM a annoncé que seul un petit nombre de véhicules sera affecté par la fin prévue du réseau 3G, puisque l'entreprise a effectué une mise à jour à distance afin de permettre à la plupart des véhicules

²¹² Sidi LU et Weisong SHI, « Vehicle Computing: Vision and challenges », (2023) 1 *J. Inf. Intell.*, 27-28.

²¹³ L. DETERMANN et B. PERENS, préc., note 16, 923-924.

²¹⁴ Jonathan LAWRENCE, « Automotive Telematics: Is it Time for a Renaissance or an Obituary? », dans *Mobile Media*, Routledge, 2005, p. 45-54 à la page 48.

²¹⁵ Ahmed Amin SOLYMAN et Khalid YAHYA, « Evolution of wireless communication networks: from 1G to 6G and future perspective », (2022) 12-4 *Int. J. Electr. Comput. Eng. IJECE* 3943-3950, 3944-3945, DOI : <http://doi.org/10.11591/ijece.v12i4.pp3943-3950>.

²¹⁶ J. LAWRENCE, préc., note 214 aux pages 47-48.

²¹⁷ Ken BELSON, « Mayday! Some Cars Will Lose OnStar Link », *The New York Times* (19 novembre 2006), en ligne :

<<https://www.nytimes.com/2006/11/19/automobiles/19ONSTAR.html>>.

concernés de fonctionner avec le réseau 4G ou la 5G²¹⁸. Toutefois, comme nous le verrons dans la section 6, les fabricants de véhicules connectés ne font généralement aucune promesse quant à la capacité de leurs véhicules à fonctionner sur les futures générations de réseaux cellulaires.

3.3 Atteinte au droit à la réparation

La notion de droit à la réparation est intimement liée au droit de propriété²¹⁹. L'une des premières formulations de ce droit se trouve dans l'arrêt *Wilson v. Simpson et al.*, rendu dès 1850 par la Cour suprême des États-Unis. Parmi d'autres questions, ce dossier a soulevé celle de savoir si la réparation et le remplacement d'une pièce essentielle pouvaient constituer une violation du brevet. La Cour a conclu que :

*It is the use of the whole of that which a purchaser buys, when the patentee sells to him a machine; and when he repairs the damages which may be done to it, it is no more than the exercise of that right of care which every one may use to give duration to that which he owns, or has a right to use as a whole*²²⁰.

Toutefois, les défenseurs du droit à la réparation plaident que cette notion va bien au-delà du principe qu'une personne a le droit d'effectuer des réparations sur son bien. Ils affirment qu'il existe également un droit positif à l'accès aux pièces de rechange, à l'information de diagnostic et à la formation pertinente pour effectuer des réparations. Ce droit positif peut être justifié non seulement par les droits de propriété, mais aussi par le fait que l'accès à la réparation indépendante présente des avantages indéniables tant pour la concurrence que pour l'environnement et l'innovation²²¹.

La connectivité des automobiles est susceptible de dresser des barrières pour les consommateurs en ce qui concerne leur droit à la réparation. Dans cette section, nous examinerons ces barrières.

3.3.1 Une réparation de plus en plus liée au numérique

Comme décrit dans la section 2, les véhicules comportent un nombre de composants numériques en constante augmentation. De plus en plus, les pièces sont équipées de contrôles numériques et de capteurs²²². Pour cette raison, même des actes d'entretien courants nécessitent désormais un accès au logiciel. Le calibrage correct d'un miroir

²¹⁸ ONSTAR, « 3G Network Sunset | Frequently Asked Questions », en ligne :

<<https://www.onstar.com/support/faq/3g-network-sunset>> (consulté le 14 janvier 2025).

²¹⁹ Leah CHAN GRINVALD et Ofer TUR-SINAI, « Smart Cars, Telematics and Repair », (2021) 54 *Univ. Mich. J. Law Reform* 283-329, 290, DOI : <https://doi.org/10.36646/mjlr.54.2.smart>.

²²⁰ U.S. REPORTS, *Wilson v. Simpson et al.*, 50 U.S. (9 How.) 109 (1850), p. 123 [U.S. Reports], en ligne : <<https://www.loc.gov/item/usrep050109/>> (consulté le 21 mars 2025).

²²¹ L. CHAN GRINVALD et O. TUR-SINAI, préc., note 219, 290-292; A. PERZANOWSKI, préc., note 187, p. i.

²²² M. FORELLE, préc., note 9, 7.

pourrait requérir l'accès aux données accumulées par le véhicule²²³. Même une manœuvre aussi simple qu'un changement de pneus pourrait être impossible ou risquée sans accès au logiciel. Comme les systèmes embarqués dépendent de plus en plus de techniques de co-vérification²²⁴, un propriétaire qui aurait changé ses pneus lui-même et qui ne disposerait pas des codes informatiques requis pourrait se retrouver avec un véhicule ou un système non fonctionnel²²⁵.

[...] In modern vehicles, software can thwart even the most benign forms of tinkering. Switching from summer to winter tires can require access to locked-down onboard computer codes just to make sure the transmission shifts properly²²⁶.

Le contrôle exclusif des fabricants sur les codes logiciels et les données diagnostiques permet de limiter ce que peuvent effectuer les consommateurs en matière de réparation et d'entretien. Ce contrôle est maintenu par les fabricants qui refusent de partager les logiciels de réparation ou les données diagnostiques, et aussi par les restrictions imposées sur l'accès aux logiciels et aux données par des clauses restrictives dans le CLUF ou des verrous numériques.

Dans la section 3.2.1, nous avons parlé du fait que des clauses des CLUF prévoient parfois des limites sur l'accès aux logiciels du véhicule. L'intégration de verrous numériques ou de mesures techniques de protection (MTP) est un autre moyen pour les fabricants automobiles de limiter l'accès au logiciel du véhicule, et ce, au-delà du cadre contractuel. Une MTP peut être définie comme étant « toute technologie ou tout dispositif qui contrôle efficacement l'accès à une œuvre [dans ce cas, un logiciel], ou qui restreint efficacement la reproduction d'une œuvre²²⁷ ». Au contraire des restrictions contractuelles et de la loi, les mesures techniques de protection intégrées aux logiciels permettent une mise en application des restrictions de manière technologique²²⁸. La définition est large : ce type de verrouillage numérique peut se produire, par exemple, lorsque le véhicule refuse l'installation d'une pièce dont le code n'est pas reconnu. Dans ce cas, il serait impossible de remplacer une composante matérielle défectueuse par une autre

²²³ LKQ CORPORATION, *Mémoire déposé dans le cadre de l'étude du Projet de loi no 29, Loi protégeant les consommateurs contre l'obsolescence programmée et favorisant la durabilité, la réparabilité et l'entretien des biens*, à la Commission de l'économie et du travail, 008M, 2022, p. 7, en ligne :

<https://www.assnat.qc.ca/Media/Process.aspx?MediaId=ANQ.Vigie.Bll.DocumentGenerique_191719>.

²²⁴ P. CHAPDELAINE et al., préc., note 196, p. 6. Voir aussi comme exemple Jack MONAHAN, « Ram's Restricting Truck Repair through Software Locks », *iFixit* (25 2023), en ligne : <<https://fr.ifixit.com/News/84923/rams-restricting-truck-repair-through-software-locks>> (consulté le 9 janvier 2025).

²²⁵ Voir l'exemple d'un système d'infodivertissement qui ne fonctionne pas sans activation par un concessionnaire autorisé dans L. DETERMANN et B. PERENS, préc., note 16, 927.

²²⁶ A. K. PERZANOWSKI, C. J. HOOFNAGLE et A. KESARI, préc., note 204, 831.

²²⁷ Jean-Sébastien RODRIGUEZ-PAQUETTE et Nicolas SAPP, « Les déboires des mesures techniques de protection dans l'industrie du divertissement ou le droit vs la technologie : un combat perdu d'avance ! », *Dév. Récents En Droit Propr. Intellect.* 2013.31-67, 31.

²²⁸ A. PERZANOWSKI et J. SCHULTZ, préc., note 190, p. 123.

composante standard, car les logiciels intégrés à leur véhicule sont configurés pour rejeter de telles modifications en ne reconnaissant que les composantes du propriétaire²²⁹.

L'entreprise LKQ, fournisseur de pièces de marché secondaire, a fait remarquer en 2023 que les restrictions sur la réparation ont augmenté d'une manière significative dans les dernières années :

Sur plus de 272 millions de véhicules légers aux États-Unis, 100 millions contiennent au moins un type de restriction qui empêche les réparateurs indépendants d'effectuer des réparations. Les restrictions en matière de réparation concernent généralement les véhicules récents équipés de nouvelles technologies, où l'accès aux données nécessaires à la réparation et à l'entretien se fait par l'intermédiaire d'un système de télématique.

[...]

*Aucune de ces restrictions n'existait il y a dix ans. En fait, la plupart des restrictions n'existaient même pas il y a cinq ans. **Ces restrictions découlent de la complexité technique croissante des véhicules, comme les systèmes logiciels, les systèmes télématiques et la cybersécurité***²³⁰.

La restriction sur la réparation par le biais d'un contrat de licence ou d'une MTP était possible avant l'introduction de la connectivité dans les véhicules, mais leur impact est amplifié dans le contexte d'une voiture connectée. La connectivité donne au fabricant un contrôle et une capacité de surveillance accrus sur ces restrictions, afin de détecter la nature des pièces de remplacement et les réparations par des réparateurs tiers et de communiquer cette information au fabricant, ce qui est déjà arrivé avec d'autres biens connectés²³¹. Elle permet aussi au fabricant de collecter et de garder un accès exclusif sur des données diagnostiques détaillées du véhicule, ce qui donne au fabricant un avantage important en matière de réparation.

3.3.2 Absence d'accès à l'information diagnostique

Comme nous l'avons vu précédemment (section 2.5.7), les fabricants de voitures connectées ont maintenant la capacité de collecter des données sur le fonctionnement du véhicule à distance, et ce, en temps réel, grâce au système télématique. Ces données sont particulièrement utiles pour les réparateurs, car elles fournissent en temps réel de l'information précise sur les différents systèmes du véhicule et sur les résultats des tests effectués par le réparateur²³².

²²⁹ A. RAINA et M. PALANISWAMI, préc., note 177, 3.

²³⁰ LKQ CORPORATION, préc., note 223, p. 3.

²³¹ A. PERZANOWSKI, préc., note 187, p. 87.

²³² W. KERBER et D. GILL, préc., note 53, 244; LKQ CORPORATION, *Research and Market Observations on Automotive Repair Restrictions: Research Prepared for the Federal Trade*

L'accès aux données diagnostiques est souvent protégé par les MTP²³³. De plus, ces données ne sont pas généralement stockées dans le véhicule ; elles sont plutôt envoyées directement aux serveurs privés du fabricant ou d'un tiers dans un format non standardisé²³⁴. Par conséquent, les données diagnostiques sont souvent inaccessibles aux réparateurs indépendants ou au consommateur.

Ainsi, le fabricant garde un monopole sur les données télématiques ; il peut soit conserver ce monopole en partageant l'accès seulement avec ses concessionnaires, soit choisir de partager les données avec les consommateurs ou les réparateurs indépendants à certaines conditions²³⁵. Par exemple, BMW vend les données d'entretien directement aux consommateurs ou à leurs mécaniciens indépendants²³⁶. Certains fabricants automobiles se limitent à rendre accessibles les seules données prévues par la législation en vigueur (voir la section 5) et limitent l'accès aux autres données en invoquant, entre autres, leur droit de propriété intellectuelle²³⁷. D'autres plaident que cette information ne peut pas être partagée pour des raisons de cybersécurité et de protection de données²³⁸.

Cependant, l'argument que le partage de données diagnostiques pose un risque pour la sécurité des véhicules est contesté. En fait, certains experts soulignent que le système actuel, qui consiste à conserver une base de données sur un serveur centralisé n'est pas sûr, et que des approches différentes pourraient être encore plus sécuritaires et, en même temps, susceptibles de contrer le monopole des fabricants sur les données de réparation. Par exemple, les données pourraient être stockées dans le véhicule et accessibles via le port OBD ou à courte distance : cela minimiserait les risques de fuites des données et permettrait aux mécaniciens indépendants et aux consommateurs d'y accéder, sans qu'elles passent obligatoirement entre les mains des fabricants²³⁹.

3.3.3 Recours à l'argument de sécurité

De manière plus générale, les fabricants automobiles affirment que toutes les restrictions à la réparation, y compris l'utilisation de verrous numériques, sont justifiées par des raisons de sécurité. Toutefois, la Federal Trade Commission (FTC) américaine a déclaré

Commission Nixing the Fix: A Workshop on Repair Restrictions, 2019, p. 18-19, en ligne : <https://downloads.regulations.gov/FTC-2019-0013-0020/attachment_1.pdf>.

²³³ Leah CHAN GRINVALD et Ofer TUR-SINAI, « The battle over right to repair is a fight over your car's data », *The Conversation* (13 novembre 2023), en ligne : <<http://theconversation.com/the-battle-over-right-to-repair-is-a-fight-over-your-cars-data-213052>> (consulté le 9 janvier 2025); L. CHAN GRINVALD et O. TUR-SINAI, préc., note 219, 296; Anthony D. ROSBOROUGH, « Unscrewing the Future: The Right to Repair and the Circumvention of Software TPMs in the EU », (2020) 26 *JIPITEC*, 28.

²³⁴ P. SAMUELSON, préc., note 191, 6.

²³⁵ W. KERBER et D. GILL, préc., note 53, 11-12.

²³⁶ B. MARTENS et F. MUELLER-LANGER, préc., note 126, 116.

²³⁷ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 21, p. 22.

²³⁸ B. MARTENS et F. MUELLER-LANGER, préc., note 126.

²³⁹ Thomas A. HEMPHILL, Phil LONGSTREET et Syagnik BANERJEE, « Automotive repairs, data accessibility, and privacy and security challenges: A stakeholder analysis and proposed policy solutions », (2022) 71 *Technol. Soc.* 1-9, 6-8, DOI : <https://doi.org/10.1016/j.techsoc.2022.102090>.

dans un rapport sur le droit à la réparation qu'elle n'avait vu que peu de preuves justifiant les restrictions imposées par les fabricants sur la réparation²⁴⁰. Selon le U.S. Public Interest Research Group Education Fund et iFixit, un organisme de réparation indépendant,

According to industry experts, there is “no cybersecurity risk in third-party repair.” Securely designed products cannot be undermined by repair technicians, whether manufacturer authorized, independent, or consumer. Manufacturers do not provide authorized repair technicians with information that would undermine security, because they know those secrets would not be kept by their broad service networks. If secrecy of repair information is the only thing keeping products secure, they are not secure. Cybersecurity professionals often state that “there is no security through obscurity”²⁴¹.

Des universitaires contestent également l'argument que les restrictions sur la réparation et sur l'accès aux données diagnostiques soient nécessaires pour des raisons de sécurité :

Although [manufacturers] are trying to frame the policy discussion as a trade off-problem between maximum security on the one hand and fair and undistorted competition on the other hand, the discussion among experts make it increasingly clear that such a trade off between more security and more competition does not exist. The main argument is that most IT experts think that an open interoperable telematics system with a multi-layered safety and security system (including certification) can achieve at least the same security levels than proprietary closed systems²⁴².

Dans la section 3.4 du rapport, nous abordons brièvement la question de cybersécurité. Nous pouvons constater que les voitures connectées présentent en effet des risques liés à la cybersécurité, mais que ces problèmes n'ont aucun lien évident avec la réparation indépendante ou le partage de données diagnostiques.

3.3.4 La parole aux experts en réparation

Les enjeux de réparation et d'entretien des automobiles sont complexes et en évolution constante. Les résultats de notre revue de littérature démontrent que plusieurs aspects techniques exercent une influence sur l'accès à la réparation et à l'entretien des automobiles connectées par les consommateurs. Afin d'avoir un point de vue plus technique sur les enjeux en matière de réparation, nous avons sollicité les commentaires des trois experts possédant des dizaines d'années d'expérience dans le domaine de la réparation automobile. Nous avons parlé aux trois experts à l'été 2024 lors des interviews orales d'une durée d'environ une heure. Cette section résume leurs observations les plus

²⁴⁰ FEDERAL TRADE COMMISSION, préc., note 192, p. 6.

²⁴¹ U.S. PUBLIC INTEREST RESEARCH GROUP EDUCATION FUND & IFIXIT, préc., note 201, p. 44-45.

²⁴² Wolfgang KERBER, « Data-Sharing in IoT Ecosystems from a Competition Law Perspective: The Example of Connected Cars », SSRN 2019.1-49, 12. Voir aussi les commentaires des professeurs Centivany, Diawara et Rosborough dans la section 7 du présent rapport.

pertinentes sur l'évolution du diagnostic et des réparations automobiles jusqu'à l'avènement de la voiture connectée, et les nouveaux enjeux pour les consommateurs et les réparateurs indépendants.

Les experts que nous avons interviewés sont :

- Eli Melnick, titulaire d'une maîtrise en génie électrique, il possède plus de 40 ans d'expérience dans le secteur automobile, avec une spécialisation dans les systèmes électroniques. Il a été propriétaire d'un atelier de réparation indépendant à Toronto et il agit maintenant à titre d'expert auprès des compagnies d'assurance pour enquêter sur les véhicules déclarés perte totale afin de déterminer la cause des défaillances.
- Patrick Darche est actuellement gestionnaire des opérations chez Communauto, un service de partage de voitures. Il a été technicien chez plusieurs concessionnaires automobiles pendant plus de 18 ans et responsable des ateliers mécaniques pendant 13 ans.
- Ron Green est technicien automobile depuis 1972 et propriétaire d'un atelier indépendant depuis 2010, avec une spécialisation dans les voitures de la marque Porsche.

3.3.3.1 Historique

Les trois experts ont évoqué l'importance du système OBD-II, qui a permis une généralisation et une standardisation des diagnostics, rendant les données plus accessibles et détaillées.

Tous trois ont également noté que depuis le développement de l'OBD, chaque fabricant a mis au point des systèmes de diagnostics embarqués qui fournissaient des renseignements au-delà des diagnostics disponibles via la norme OBD-II. Avec l'avènement des systèmes embarqués, les constructeurs ont intégré de plus en plus de capteurs dans le véhicule, de codes diagnostiques et de fonctionnalités à la connexion OBD. Eli Melnick observe :

*Onboard systems are so complex today and interconnected: a typical car today has between 20 and 40 processors or computers onboard, which talk to each other. It became a monster. **To do anything on a car today, you need to be able to monitor all those computers.***

In between 2000 and the 2010s, you'd get more and more advanced data ability, not only to read stuff, but to activate stuff. For example, if you're testing a radiator cooling fan, the electric fan, you can command that fan to come on through your scanner. (Notre soulignement)

Avant le *Memorandum of Understanding* (MOU) de 2014, ces données n'étaient accessibles qu'aux techniciens agréés du fabricant. Comme nous le verrons à la section 5.6.1, le MOU de 2014 est un accord non contraignant signé par les fabricants automobiles américains dans lequel ils acceptent de donner accès aux données et outils aux techniciens de réparation et aux particuliers, mais à un coût.

3.3.3.2 Accès aux outils et aux données

Les trois experts ont évoqué le fait que l'accès aux outils ou aux données nécessaires à la réparation n'est pas toujours simple et qu'il est souvent dispendieux.

M. Melnick explique que l'accès aux données et aux logiciels propriétaires se fait généralement par le biais d'un abonnement aux systèmes en ligne des fabricants. Les techniciens indépendants ont besoin non seulement d'un tel abonnement, mais aussi d'avoir accès aux appareils pour se connecter au véhicule, comme un lecteur de codes de véhicules. L'accès à ces outils peut être difficile ou cher. M. Melnick donne l'exemple du fait qu'il peut commander un lecteur de codes Mercedes, mais que celui-ci peut être en rupture de stock pendant six mois ou un an. De plus, le coût du lecteur de codes du fabricant est souvent prohibitif. Ron Green a donné l'exemple de Porsche : le lecteur de codes utilisé par les réparateurs autorisés de Porsche coûte environ 25 000 \$ et nécessite des mises à jour fréquentes au coût de 2 000 \$ chacune. De plus, il faut payer 25 \$ par accès ou 17 \$ par heure pour utiliser le système en ligne du fabricant.

M. Melnick indique qu'au lieu d'acheter un lecteur de codes du fabricant et de payer un abonnement pour avoir accès au système de chaque constructeur, les ateliers de réparation indépendants peuvent acheter des lecteurs de codes « après-vente », fabriqués par des tiers. Il indique qu'un lecteur de codes de base du marché secondaire peut coûter environ 700 \$. Un lecteur de codes plus haut de gamme, livré avec un an de mises à jour logicielles, peut coûter jusqu'à 5 500 \$, avec un supplément de 500 \$ à 1 500 \$ pour les mises à jour après la première année.

Les lecteurs de codes du marché secondaire peuvent lire des codes de diagnostic génériques pour une grande variété de modèles de voitures. **Toutefois, ils ne peuvent pas reprogrammer le véhicule ou mettre à jour ses logicielles.** En outre, les produits du marché secondaire ne sont pas toujours à jour en ce qui concerne les logiciels les plus récents, ce qui signifie que « le marché secondaire est exclu de certaines réparations, en particulier pour les véhicules plus récents », selon M. Melnick, qui affirme que ces outils sont essentiels à l'existence des garages indépendants. Il faut un abonnement au système du fabricant pour avoir un accès complet aux logiciels les plus récents et pour être capable de reprogrammer le véhicule.

Le coût de l'abonnement au système en ligne du fabricant, qui donne accès aux codes de diagnostic et aux logiciels de réparation, peut également être prohibitif, et les mécaniciens achètent parfois des abonnements courts. Selon M. Melnick :

For a specialist garage, because it only does one brand, they can probably buy an annual subscription, whereas a general repair garage couldn't possibly afford that. That makes it really difficult: say you need access to the vehicle data for a repair and you buy a 48-hour subscription. You plug in the part that you thought you needed and you do whatever you need to do with the scanner to facilitate the repair (it's called coding the part), and it doesn't work. Now you're under pressure. The 48 hours is expiring, and you haven't fixed the problem and now it becomes stressful.

M. Darche a constaté que les interfaces et les logiciels varient selon les marques, rendant parfois la gestion des outils complexe.

Eli Melnick et Ron Green ont expliqué que les grandes marques américaines (Ford, GM, Chrysler) et japonaises offrent le meilleur accès aux données de réparation, avec des lecteurs de codes de qualité disponibles auprès de fabricants indépendants. En revanche, l'accès aux informations techniques pour les voitures européennes est plus limité et parfois coûteux. M. Green donne l'exemple de Porsche : depuis 2014, Porsche ne fournit plus de mises à jour à un des principaux fabricants des lecteurs de codes de réparation du marché secondaire, en disant qu'ils sont en négociations avec ce dernier. Cela rend l'accès aux informations techniques difficile pour les ateliers indépendants. Certains fabricants d'automobiles rendent leurs outils et leurs données disponibles aux tiers, mais seulement sur leur plateforme et à un prix qui n'est pas abordable pour un réparateur indépendant. En en facturant des prix que M. Green considère exorbitants pour l'assistance technique, Porsche se conforme à la lettre de la MOU, mais pas à son esprit.

Bien que le MOU exige que les fabricants automobiles donnent accès à leurs systèmes et à leurs informations de diagnostic, M. Melnick note que les mécaniciens indépendants ne bénéficient pas toujours du même accès que les techniciens des concessionnaires du constructeur. Par exemple, M. Melnick dit qu'il voit souvent des commentaires d'autres techniciens indépendants indiquant que les services en ligne du fabricant sont en panne ou que leur abonnement au logiciel ne fonctionne pas.

M. Darche observe que l'accès aux données techniques s'améliore grâce à la législation et au lobbying aux États-Unis, mais que des défis subsistent, notamment pour les modèles spécifiques au marché canadien (qui ne sont pas vendus aux États-Unis). M. Melnick observe que les mécaniciens canadiens peuvent être soumis à davantage de restrictions en matière de réparation que les mécaniciens américains, parce que le marché canadien est plus petit. Si un véhicule n'est vendu qu'au Canada, les fabricants d'outils du marché secondaire ne sont guère incités à construire et à distribuer un lecteur de codes.

3.3.3.3 Complexification et numérisation de la réparation

Les trois experts s'accordent à dire que les réparations deviennent plus complexes et plus coûteuses avec l'introduction des ordinateurs partout dans le véhicule. Un problème majeur, souligné par les trois experts, est le besoin de logiciels pour la mise à jour, l'étalonnage ou la réinitialisation d'un véhicule après une réparation.

La technologie a complexifié des tâches qui étaient auparavant simples. M. Green donne l'exemple des nouveaux véhicules allemands qui ne disposent plus de jauge pour vérifier le niveau d'huile. Pour changer l'huile, le mécanicien doit vidanger, puis ajouter de l'huile, en se basant sur les données fournies par les capteurs numériques pour déterminer la quantité à verser. Les mécaniciens doivent ensuite utiliser le logiciel pour réinitialiser le rappel de service après un changement d'huile, et tout est enregistré dans le système du véhicule. Tout cela requiert un accès au système numérique du fabricant.

Tous les experts ont également donné l'exemple des modules de contrôle du corps du véhicule (*Body Control Module*), qui peuvent nécessiter une programmation spécifique pour les pièces de rechange. Selon M. Melnick :

If you install a module, let's say a body control module, it's not plug-and-play anymore. Most of the modules onboard are specific to the Vehicle Identification Number. So, you have to program the car's ID number into the module before it will be acknowledged by the other modules onboard.

Il explique que les constructeurs conçoivent les véhicules de cette manière en partie pour s'assurer que les consommateurs n'enfreignent pas la garantie en changeant des pièces avec des pièces de rechange génériques, mais une autre raison est prétendument la sécurité, car les véhicules connectés sont susceptibles de subir des cyberattaques.

M. Green a donné plusieurs exemples du fait que les éléments du corps du véhicule ont besoin d'une telle calibration. Les phares peuvent nécessiter un logiciel pour les calibrer en fonction du numéro d'identification du véhicule. Pour effectuer un réglage de la géométrie des roues, on doit maintenant calibrer le capteur d'angle de braquage monté sur la colonne de direction, qui communique avec le système de contrôle de la stabilité du véhicule. Même chose pour le remplacement des pneus, qui est devenu plus compliqué, nécessitant la calibration du système de surveillance de la pression d'air pour effectuer le travail, ainsi que des équipements spéciaux pour les systèmes de pneus avancés. Ces changements signifient qu'un logiciel est nécessaire pour effectuer la réparation, et rendent les réparations simples hors de portée d'un réparateur occasionnel ou d'un bricoleur.

Selon M. Darche :

On ne peut plus faire installer une pièce aussi simple qu'une « switch » [commande] de vitre parce que changer juste une commande peut nécessiter des calibrations pour que la voiture l'accepte. Dans les voitures d'il y a quelques années, les pièces sont pratiquement interchangeables.

Même la réinitialisation des voyants d'entretien nécessite parfois un logiciel. Un mécanicien indépendant peut être en mesure d'effectuer l'entretien, mais pas de réinitialiser le voyant (par exemple, après une vidange d'huile) s'il ne dispose pas des outils adéquats.

Pour cette raison, M. Darche dit qu'il est préoccupé de l'avenir de la réparation indépendante.

Ça pourrait prendre un spécialiste juste pour les mises à jour électroniques et réinitialiser les pièces à installer sur l'auto — un spécialiste en électronique pourrait devenir nécessaire pour s'assurer que les réparations et les pièces sont acceptées.

Il explique que ces changements exigent non seulement une plus grande spécialisation, mais aussi un coût plus élevé : par exemple, certains modèles de phares peuvent maintenant coûter entre 1 000 \$ et 3 000 \$. Avec le grand nombre de composantes électroniques et de dispositifs de sécurité à l'avant des véhicules, ceux-ci peuvent devenir une perte totale en cas de collision mineure.

D'autres limites existent en raison des restrictions de propriété et de la conception du véhicule ; M. Darche souligne que pour Tesla, le mécanicien doit respecter un certain

nombre de normes de réparation particulières établies par le fabricant (techniques de réparation et choix des matériaux, par exemple) :

Tu ne peux pas souder la structure. Les points de soudure, les matériaux... Tu ne peux pas les débosser. Réparer une Tesla c'est un autre monde. C'est un monopole, c'est comme tu as le « gun » à la tête, autant des assureurs que des usagers.

Enfin, M. Melnick souligne que les voitures modernes ont souvent besoin de mises à jour logicielles :

Almost every computer needs periodic software updates. It's the same with onboard computers: the manufacturers detect bugs, failures, things that don't work or they add additional features. They do it via software updates. Part of the repair protocol of today's vehicles is to look up Technical Service Bulletins (TSBs), before you do anything. Look up to see if there is a TSB for your issue and/or a software update -- a "reflash" as it's called in the industry.

Les ateliers de réparation indépendants peuvent effectuer ce service, mais, là encore, uniquement s'ils disposent de l'outil adéquat et de l'accès au logiciel propriétaire, ce qui implique des coûts.

M. Darche a mis en garde contre les risques associés aux mises à jour à distance, notamment les risques de « *bricking* » des ordinateurs de bord en cas de coupure de courant ou de surtension pendant la reprogrammation. Par exemple, une mise à jour à distance mal exécutée peut rendre un ordinateur de bord inutilisable, nécessitant son remplacement.

Selon M. Melnick, la télématique pourrait, en principe, remplacer complètement le port OBD, un jour. Les véhicules Tesla reçoivent déjà des mises à jour sans fil (sans port OBD); il connaît d'autres voitures qui reçoivent des mises à jour du système d'infodivertissement par Wi-Fi, mais pas des composants plus fondamentaux, comme les commandes du moteur. Bien que cela soit techniquement possible, cette pratique comporte des enjeux de sécurité.

3.3.5 Conséquences pour les consommateurs

Conserver le droit exclusif sur les données diagnostiques ou sur le logiciel requis pour effectuer des réparations a pour effet de limiter la capacité des consommateurs à réparer eux-mêmes leur véhicule ou à faire appel à un mécanicien indépendant. Ces pratiques donnent aux fabricants un avantage concurrentiel en matière de réparation²⁴³. En limitant l'utilisation de pièces génériques, la réinitialisation des codes de diagnostic, la calibration ou l'autorisation des réparations et de nouvelles pièces, les fabricants se placent dans une position avantageuse, voire monopolistique :

²⁴³ W. KERBER, préc., note 242; L. CHAN GRINVALD et O. TUR-SINAI, préc., note 219, 283. Voir aussi la section 7.3.2 du rapport.

From an economic perspective this can be seen also as a de facto bundling strategy, because the user of the device is not free to choose providers of aftermarket and other complementary services in the digital ecosystem but has to accept the entire bundle of the connected device and services offered by the manufacturer. [It is] important . . . that such a bundling strategy can be implemented either by denying access to necessary data, lack of interoperability, or also through a contractual bundling of these services²⁴⁴.

Le manque de concurrence aura deux effets principaux sur les consommateurs. Premièrement, les consommateurs auront un accès plus limité à la réparation, notamment s'ils habitent loin d'un concessionnaire ou d'un réparateur autorisé. Un nombre insuffisant de réparateurs peut également allonger les délais d'attente pour les pièces, l'entretien et les réparations²⁴⁵. La deuxième conséquence sera vraisemblablement l'augmentation des coûts pour les réparations et les pièces de rechange. Il est établi qu'en général, la réparation indépendante est moins chère que la réparation effectuée par les concessionnaires et que les pièces de rechange du marché secondaire sont moins chères que celles vendues par le fabricant :

Since the empirical experience in automobile aftermarkets is that the prices of repair and maintenance services as well as spare parts of OEMs [Original Equipment Manufacture ou fabricant] are much higher than those from independent service providers, the concerns of consumers that the elimination of competition on aftermarket and complementary markets would lead to higher prices and less consumer choice has to be taken very seriously. So far there are also no arguments (e.g., by the OEMs) that such closed ecosystems of connected cars would lead to efficiency advantages or more innovation with regard to aftermarket and complementary services²⁴⁶.

Les restrictions sur la réparation ne font qu'exacerber la tendance à l'augmentation du coût des réparations automobiles. Entre 2000 et 2017, le prix de la réparation de voitures a augmenté de plus de 60 % selon le United States Bureau of Labor Statistics²⁴⁷. Cette augmentation s'explique par plusieurs facteurs, y compris la complexification des voitures, mais on peut également constater que certaines des pratiques abordées précédemment coûtent cher au consommateur, comme le fait d'imposer des frais de réinitialisation pour des pièces installées par le propriétaire ou un réparateur indépendant²⁴⁸.

3.4 Risques liés à la sécurité du véhicule (vol, cybersécurité)

Les questions de cybersécurité dépassent le cadre de notre recherche, mais nous ne pouvons passer sous silence ce sujet, car notre analyse documentaire a révélé des manquements à cet égard qui posent un risque majeur pour les consommateurs. En gros,

²⁴⁴ W. KERBER, préc., note 242.

²⁴⁵ U.S. PUBLIC INTEREST RESEARCH GROUP EDUCATION FUND & IFIXIT, préc., note 201.

²⁴⁶ W. KERBER, préc., note 242, 11-13; voir aussi FEDERAL TRADE COMMISSION, préc., note 192, p. 22, 40.

²⁴⁷ A. PERZANOWSKI, préc., note 187, p. 23.

²⁴⁸ *Id.*, p. 94.

la collecte de données comporte des risques de fuites et de vols de données, alors que la connectivité ouvre la porte au piratage. Les voitures connectées présentent ainsi des risques pour les consommateurs sur ces deux fronts.

3.4.1 Risque de vol et de fuite de données

Les grandes quantités de données collectées par les fabricants automobiles sont généralement stockées dans un serveur central contrôlé par le fabricant ou par un tiers dont il a retenu les services. Bien que les fabricants affirment que cette solution est plus sûre que d'autres, comme le stockage des données de manière décentralisée, cela signifie que toute personne qui obtient un accès non autorisé au serveur central a accès aux données collectées sur les utilisateurs²⁴⁹.

D'importantes fuites de données se sont déjà produites dans ce secteur, plus souvent en raison d'une négligence que d'une attaque ciblée. Par exemple, Toyota a laissé accessibles, pendant plus de dix ans, des données provenant de ses services connectés, y compris des données sur le numéro d'identification et la localisation du véhicule à différents moments et des séquences vidéo prises par le véhicule. Bien qu'aucun incident d'utilisation inappropriée de ces renseignements n'ait été signalé, les données de véhicules appartenant à plus de deux millions de personnes ont été exposées²⁵⁰.

En 2024, Volkswagen a subi une fuite massive de données des voitures connectées, également causée par la négligence. Les données de localisation d'environ 800 000 clients de Volkswagen se sont avérées facilement accessibles, largement non protégées et non cryptées, sur un serveur infonuagique d'Amazon. De plus, l'entreprise a également divulgué des noms, des adresses courriel et parfois d'autres renseignements de contact, tels que l'adresse du domicile et les numéros de téléphone des utilisateurs qui s'étaient inscrits à l'une des applications mobiles de services connectés. Les données de localisation et les données d'identification ont pu être facilement mises ensemble, permettant la réidentification des données de localisation²⁵¹. Apparemment, la fuite aurait été le résultat d'une erreur technique et non d'un piratage. Selon le journal allemand Der Spiegel,

*Neither intelligence agencies nor snooping VW competitors, criminals or even bored teenagers would have found it particularly difficult to access the trove of information. Everything was there, you just had to know where to look. Nothing special was necessary beyond a couple of freely available computer programs that are part of the standard toolbox for criminal hackers and IT professionals alike*²⁵².

²⁴⁹ B. MARTENS et F. MUELLER-LANGER, préc., note 126.

²⁵⁰ Yuri KAGEYAMA, « Toyota: Data on more than 2 million vehicles in Japan were at risk in decade-long breach », *AP News* (12 mai 2023), en ligne : <<https://apnews.com/article/toyota-data-breach-connected-service-7f686c990daf3cd85b57d7ffaa27c81a>> (consulté le 21 mars 2025).

²⁵¹ P. B. FLÜPKE, M. HOPPENSTEDT, M. KREIL, M. ROSENBAACH et R. WILKIN, préc., note 106.

²⁵² *Id.*

Interrogée sur cette fuite et sur ses pratiques en matière de protection des données, la filiale de Volkswagen chargée de la collecte et du stockage de ces données a déclaré qu'elle recueillait des « données anonymes », qui étaient utilisées pour améliorer le logiciel des batteries dans les voitures électriques²⁵³.

De tels incidents témoignent des mauvaises pratiques de protection des données en vigueur dans le secteur. Non seulement des données très sensibles ont été exposées en ligne sans protection adéquate, mais elles n'étaient ni cryptées ni correctement anonymisées, car elles étaient facilement réidentifiables. Vu l'ampleur de la collecte de renseignements personnels et la difficulté de les rendre anonymes, nous croyons que ces pratiques représentent un risque important pour les utilisateurs de voitures connectées.

3.4.2 Risque de piratage informatique

Les véhicules connectés sont susceptibles d'être piratés. En 2011, des chercheurs avaient identifié la possibilité d'accéder à distance aux commandes d'un véhicule par le biais d'un piratage du matériel de la voiture ; après avoir introduit une vulnérabilité par une connexion physique (par exemple, par la connexion d'une clé USB ou d'un téléphone cellulaire), les chercheurs ont établi qu'il serait aussi possible de contrôler certaines fonctionnalités en utilisant les connexions sans fil du véhicule telles qu'OnStar ou Bluetooth²⁵⁴. En 2014, les chercheurs ont démontré leur capacité à pirater les véhicules connectés à distance en utilisant la connexion sans fil du réseau cellulaire²⁵⁵.

À la suite de ces révélations, le sénateur américain Ed Markey a publié en 2015 un rapport basé sur les informations qu'il a obtenues de seize grands fabricants automobiles sur leurs pratiques en matière de cybersécurité à la suite de l'ajout de technologies connectées à leurs véhicules. Le rapport a révélé que presque toutes les marques de voiture sur le marché étaient vulnérables au piratage, mais qu'aucun des fabricants n'avait sérieusement réfléchi aux implications de ces vulnérabilités ou à la manière de les mitiger²⁵⁶. En effet, le rapport a constaté que « les mesures de sécurité visant à empêcher l'accès à distance à l'électronique des véhicules sont incohérentes et aléatoires » dans l'ensemble du secteur, que les fabricants ne semblaient pas comprendre les questions posées par le sénateur sur les vulnérabilités en matière de cybersécurité²⁵⁷.

La même année, des chercheurs ont révélé une faille dans la cybersécurité de certains véhicules Chrysler via Uconnect, son système d'infodivertissement et de services connectés. Ils ont découvert que « la connexion cellulaire d'Uconnect permet également

²⁵³ *Id.*

²⁵⁴ John MARKOFF, « Researchers Show How a Car's Electronics Can Be Taken Over Remotely », *The New York Times*, sect. Business (10 mars 2011), en ligne : <<https://www.nytimes.com/2011/03/10/business/10hack.html>> (consulté le 15 janvier 2025).

²⁵⁵ Margo ANDERSON, « Black Hat 2014: Hacking the Smart Car - IEEE Spectrum », *IEEE Spectrum* (6 août 2014), en ligne : <<https://spectrum.ieee.org/black-hat-2014-hacking-the-smart-car>> (consulté le 15 janvier 2025).

²⁵⁶ Notre traduction. Ed MARKEY, *Tracking & Hacking : security & privacy gaps put American drivers at risk*, 2015, p. 1.

²⁵⁷ Notre traduction. *Id.*

à toute personne connaissant l'adresse IP du véhicule d'y accéder depuis n'importe quel endroit au pays²⁵⁸ ». En utilisant la vulnérabilité identifiée et l'adresse IP du véhicule, les pirates pouvaient envoyer des commandes au système de communication du véhicule et contrôler ses composants physiques et son système d'infodivertissement. Cela a été démontré de manière spectaculaire lors d'une expérience au cours de laquelle les chercheurs ont contrôlé le véhicule d'un journaliste à distance, le faisant s'arrêter sur l'autoroute, parmi d'autres manipulations. Au vu des résultats de ces recherches, Chrysler a rappelé 1,4 million de véhicules²⁵⁹.

À la suite de ces incidents et d'autres similaires, l'industrie et les gouvernements semblent désormais conscients de la nécessité de renforcer les protections en matière de cybersécurité dans l'industrie automobile²⁶⁰. Néanmoins, des vulnérabilités similaires continuent d'être découvertes, ce qui indique que la cybersécurité des voitures connectées reste insuffisante²⁶¹.

3.5 Faits saillants

Dans cette section, nous avons identifié plusieurs risques que les voitures connectées posent pour la vie privée des consommateurs :

- **La collecte massive et sans restriction de renseignements personnels, parfois sensibles.** Les fabricants de voitures connectées collectent des quantités massives de données, dont une grande partie est constituée de renseignements personnels, souvent sensibles.
 - Il est souvent difficile d'anonymiser ou de dépersonnaliser véritablement ces données.
 - L'objectif et l'étendue de la collecte ne sont pas toujours clairs.
 - Les données sont parfois conservées pour une durée indéterminée.
- **Le partage de données avec des tiers.** Les fabricants de voitures connectées n'expliquent pas clairement leurs pratiques de partage des données collectées avec des tiers. L'utilisation de données par les tiers pose des risques pour les consommateurs, notamment lorsqu'elles sont agrégées : profilage numérique, surveillance par les entreprises ou par l'État, etc.

²⁵⁸ Notre traduction. Andy GREENBERG, « Hackers Remotely Kill a Jeep on the Highway—With Me in It », *Wired* (21 juillet 2015), en ligne : <<https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>> (consulté le 15 janvier 2025).

²⁵⁹ *Id.*

²⁶⁰ Voir, par ex., MCKINSEY & COMPANY, préc., note 19; THE COUNCIL OF CANADIAN ACADEMIES, préc., note 58, p. 92 et seq.; S. K. KHAN, N. SHIWAKOTI, P. STASINOPOULOS et M. WARREN, préc., note 49.

²⁶¹ Andy GREENBERG, « Millions of Vehicles Could Be Hacked and Tracked Thanks to a Simple Website Bug », *WIRED* (26 septembre 2024), en ligne : <<https://www.wired.com/story/kia-web-vulnerability-vehicle-hack-track/>> (consulté le 15 janvier 2025).

- **L'absence de consentement valable à la collecte et au partage de renseignements personnels.** Les consommateurs donnent rarement un consentement explicite, libre et éclairé à la collecte ou à l'utilisation de leurs données.
 - Les politiques de protection de la vie privée sont difficiles, voire impossibles à comprendre pour les consommateurs. Elles sont rédigées d'une manière générale, utilisent des termes vagues et sont souvent incomplètes. Elles utilisent un vocabulaire complexe, en plus d'être fragmentées entre divers documents. Il apparaît ainsi impossible de donner un consentement éclairé sur la base de cette information.
 - Les consommateurs n'ont que peu de choix quant aux données collectées par le fabricant. Les fabricants refusent de fournir les services connectés si le consommateur ne consent pas à la collecte de données, même si la collecte n'est pas nécessaire au fonctionnement de la voiture ou du service. Ainsi, les consommateurs ne peuvent généralement pas se soustraire à cette collecte s'ils souhaitent utiliser leur voiture ou ses services connectés. Le consentement donné n'est donc pas libre.
 - Tous les grands fabricants se livrent à des pratiques similaires, ce qui signifie que les consommateurs ne peuvent pas choisir des marques de voitures plus respectueuses de leur vie privée.
 - Les voitures connectées collectent également des renseignements sur les personnes qui n'ont pas l'occasion de donner leur consentement, comme les passagers ou les passants.
- **Les consommateurs ont peu d'accès ou de contrôle sur leurs renseignements personnels collectés par les fabricants des voitures connectées.**
- **Les données des consommateurs ne sont pas nécessairement protégées de manière sûre et risquent d'être divulguées sans autorisation.**

En outre, nous avons constaté que la connectivité présentait des risques pour les droits de propriété des consommateurs. Par le biais des contrats de licence d'utilisateur, les fabricants conservent la propriété du logiciel dans les véhicules connectés, bien que le logiciel soit intrinsèquement lié au bien acheté par le consommateur (la voiture). Cette pratique n'est pas nouvelle, mais la connectivité donne maintenant au fabricant un contrôle considérable sur le logiciel et donc sur le véhicule après son acquisition par le consommateur.

En particulier, la connectivité permet au fabricant :

- **De surveiller à distance l'utilisation du bien connecté par le consommateur.**
- **De modifier à distance le logiciel du véhicule après son acquisition par le consommateur.** Ceci permet au fabricant de modifier les services offerts et les fonctionnalités du véhicule, ou même d'y mettre fin. La capacité du fabricant de priver le consommateur de l'accès au logiciel et de paralyser ainsi le bien connecté a déjà été démontrée avec d'autres produits connectés. Cette pratique permet au

fournisseur de mettre en œuvre des mesures prévues dans les clauses restrictives dans ses contrats de licence d'utilisateur final, par exemple, en mettant fin au service connecté si le consommateur ne respecte pas le contrat.

- **De contrôler le logiciel à distance**, par exemple, en verrouillant les portes si le consommateur n'effectue pas ses paiements de financement ou pour la location de véhicule.
- **De bloquer ou de débloquer des fonctionnalités du véhicule à distance**. Le fabricant peut placer certaines fonctionnalités du véhicule (accélération rapide, durée de vie de la batterie, etc.) derrière un mur payant, ce qui signifie que le fabricant peut vendre des abonnements pour débloquer les caractéristiques physiques existantes de la voiture.

Nous avons également constaté le risque que la voiture ou un service connecté cesse de fonctionner, notamment si le logiciel ou le service en question dépend du fabricant et qu'il cesse de le fournir ; certains biens connectés ont historiquement cessé de fonctionner lorsque l'entreprise a fait faillite ou a mis fin au projet.

Enfin, nous avons observé que certains systèmes connectés ont été confrontés à des problèmes d'obsolescence, notamment en raison de l'évolution de la technologie qui dépasse celle qui est intégrée dans les voitures, par exemple, en ce qui concerne les normes des réseaux de télécommunications.

En ce qui concerne le droit à la réparation, nous avons constaté les risques suivants :

- La réparation des voitures modernes devient de plus en plus complexe et difficile ; **de nombreuses réparations de base ne sont plus possibles sans l'accès à un logiciel**, à la fois pour diagnostiquer le problème et pour recalibrer le véhicule après le changement d'une pièce, réinitialiser les voyants d'entretien, mettre à jour le véhicule, etc.
- **Le droit à la réparation des voitures connectées peut être entravé si le fabricant limite l'accès aux logiciels ou aux données diagnostiques requises**. Ils le font en utilisant les clauses restrictives des contrats de licence d'utilisateur final et les mesures techniques de protection, mais aussi en rendant l'accès aux outils requis (données et logiciels) inabordable, lent, difficile, etc.
- Les restrictions sur l'accès aux logiciels et aux données diagnostiques mettent les réparateurs indépendants et les particuliers dans une situation défavorable face aux fabricants et à leurs concessionnaires, ce qui a pour effet de limiter l'accès à la réparation et d'en augmenter les coûts.

Enfin, nous avons observé que les voitures connectées présentent des **risques en matière de cybersécurité**. En particulier, le fait que les fabricants collectent et conservent une quantité massive de données de ces véhicules ouvre la porte aux **fuites de données**, et les véhicules connectés peuvent être **piratés et contrôlés à distance**.

4 La parole aux consommateurs

En juillet 2024, nous avons sondé 1 043 consommateurs canadiens afin de connaître leurs pratiques, connaissances, perspectives et inquiétudes relatives aux voitures dotées de composantes technologiques. Le sondage a été réalisé en ligne et a été mené par une firme spécialisée (Passages Marketing). Les résultats présentent une marge d'erreur de 3 % (19 fois sur 20).

Nous avons limité notre enquête aux adultes résidant au Canada qui sont propriétaires, copropriétaires ou locataires à long terme (12 mois ou plus) d'une voiture dont l'année de construction est plus récente que 2011 et possédant au moins une des technologies ou fonctionnalités suivantes :

- Écran intégré pour contrôler le GPS, la musique, etc. ;
- Capacité de connecter un téléphone cellulaire via une application comme Android Auto ou Apple CarPlay ;
- Capacité pour l'automobile de se connecter à Internet ou de générer un point d'accès sans fil ;
- Capacité de localiser la voiture à distance, par exemple, par une application mobile ;
- Capacité d'intégration des fonctionnalités de l'automobile avec une maison connectée ou d'autres objets connectés ;
- Capacité de transfert au fabricant, en temps réel, des données liées à la réparation et à l'entretien ;
- Possibilité pour le fabricant de diagnostiquer et de faire des mises à jour à distance des composantes informatiques de l'automobile.

Il est important de noter que ce ne sont pas toutes des technologies ou fonctionnalités connectées selon notre définition ; nous reviendrons sur ce point ci-dessous.

Nous avons par la suite effectué des entrevues semi-dirigées avec des répondants possédant une voiture dotée d'au moins un service connecté. Les entrevues avaient pour objectif de mieux comprendre la perspective des consommateurs, notamment en ce qui concerne leur connaissance de la technologie connectée et des risques qui y sont associés, de l'impact de la connectivité sur leurs droits, de leurs préoccupations concernant la voiture connectée, ainsi que de leur évaluation des avantages et des compromis inhérents à la technologie. Les résultats de ces entrevues se trouvent à la section 4.2.

4.1 Faits saillants du sondage

4.1.1 La présence et la connaissance des technologies dans la voiture

Tout d'abord, nous avons sondé les répondants sur leur connaissance de la présence des technologies dans leur voiture. Voir la *figure 1* pour les résultats. Dans ce tableau comme dans les autres, les grands nombres correspondent au pourcentage de répondants ayant répondu par oui ou par non, et les petits nombres en dessous de ce chiffre reflètent le pourcentage d'un sous-groupe de répondants qui a répondu par oui ou par non. Ces chiffres sont indiqués lorsqu'une catégorie particulière de répondants a répondu d'une manière qui diffère significativement de la moyenne.

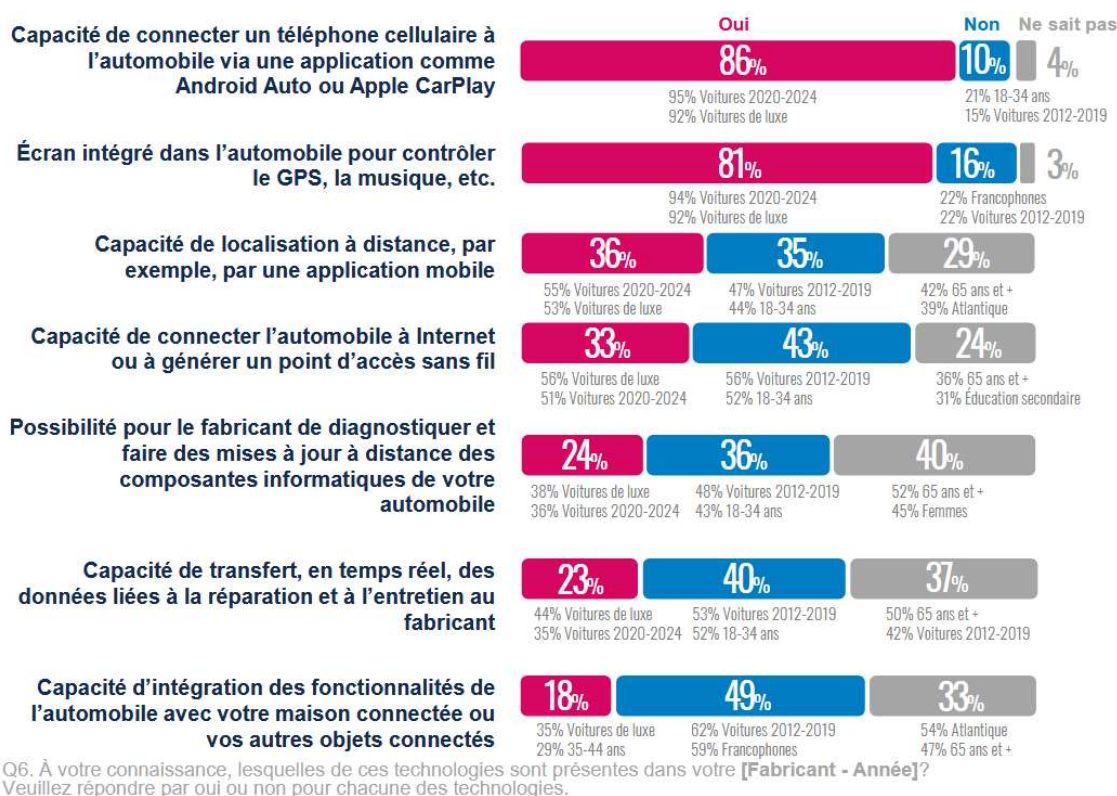


Figure 1

Il est important de noter que la présence d'une de ces technologies dans la voiture ne signifie pas nécessairement que le véhicule est « connecté » selon notre définition. Les deux premières technologies dans cette liste peuvent également se trouver dans des voitures non connectées à Internet ou à un réseau mobile. Toutes les autres fonctionnalités cependant ne sont présentes que dans des voitures connectées. Parmi les répondants, 52 % ont indiqué qu'ils ont connaissance d'au moins une des technologies connectées dans leur voiture. **On peut donc conclure qu'au moins cette proportion des répondants au sondage (52 %) possède une voiture connectée.**

De plus, nous pouvons constater que la proportion des conducteurs des voitures connectées est nettement plus élevée parmi les conducteurs des voitures plus

récentes (2020 à 2024). Parmi ce groupe, 72 % possèdent des voitures dotées des fonctionnalités connectées (312 sur 432).

De nombreux répondants possèdent une voiture qui a la capacité de connecter un téléphone cellulaire via une application comme Android Auto ou Apple CarPlay (86 %) ou qui possède un écran intégré (81 %). Ce résultat n'est pas surprenant, car ces applications sont maintenant disponibles depuis presque une décennie et l'écran est obligatoire depuis 2018. De plus, ces technologies sont très visibles et faciles à identifier, contrairement, peut-être, à certaines fonctionnalités connectées, telles que les diagnostics à distance.

Les fonctionnalités connectées sont moins présentes et moins connues. Pourtant, elles se trouvent beaucoup plus souvent dans les nouvelles voitures (2020 à 2024) et les voitures de luxe²⁶². Un grand pourcentage (de 24 à 40 %, selon les fonctionnalités) des répondants ignore si les technologies connectées sont présentes dans leur voiture. Nos entrevues ont semblé confirmer que les répondants ont souvent une mécompréhension de la technologie présente dans leur voiture.

Ceux qui ont indiqué que leur voiture est dotée d'une certaine technologie ont été questionnés sur l'utilisation qu'ils en faisaient (*figure 2*).

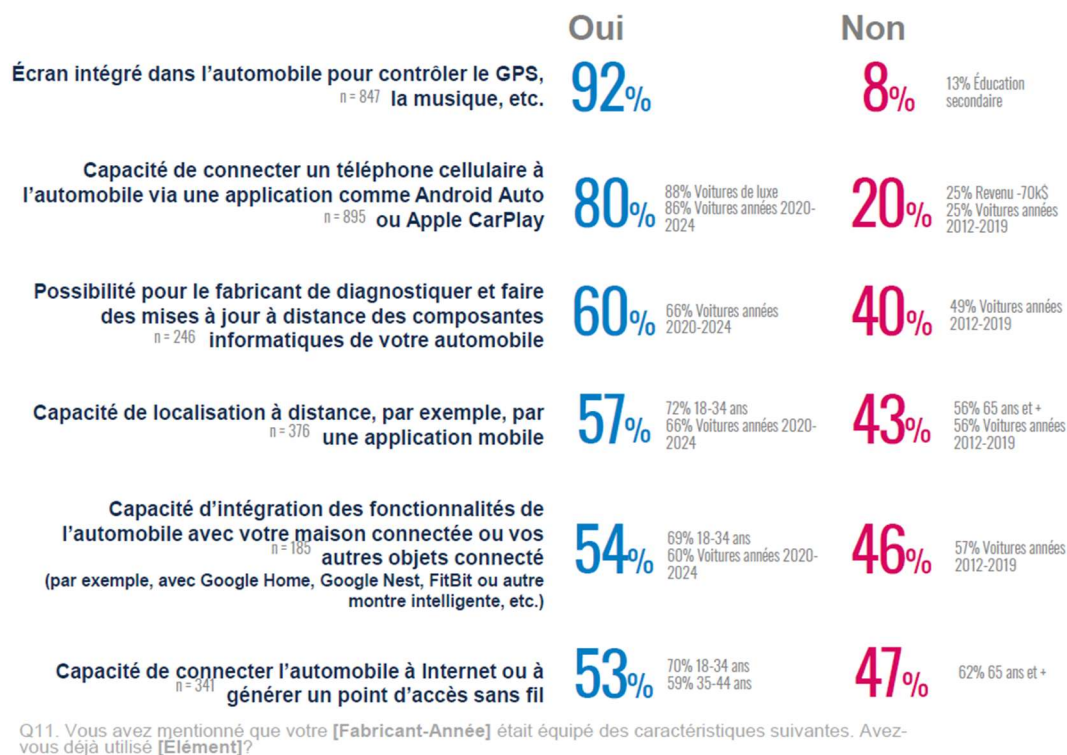


Figure 2

²⁶² La firme qui a mené le sondage a considéré comme « voitures de luxe » les Audi, BMW, Acura, Lexus, Cadillac et Mercedes-Benz. Ces véhicules comptent pour 11,8 % de l'échantillon total.

Les fonctionnalités les plus utilisées par ceux dont la voiture est dotée de fonctions technologiques sont l'écran et la connexion au téléphone cellulaire. Les taux d'utilisation sont plus bas en ce qui concerne les technologies connectées. En général, ces fonctionnalités sont plus souvent utilisées par les conducteurs des voitures plus récentes et par les personnes âgées de 18 à 34 ans.

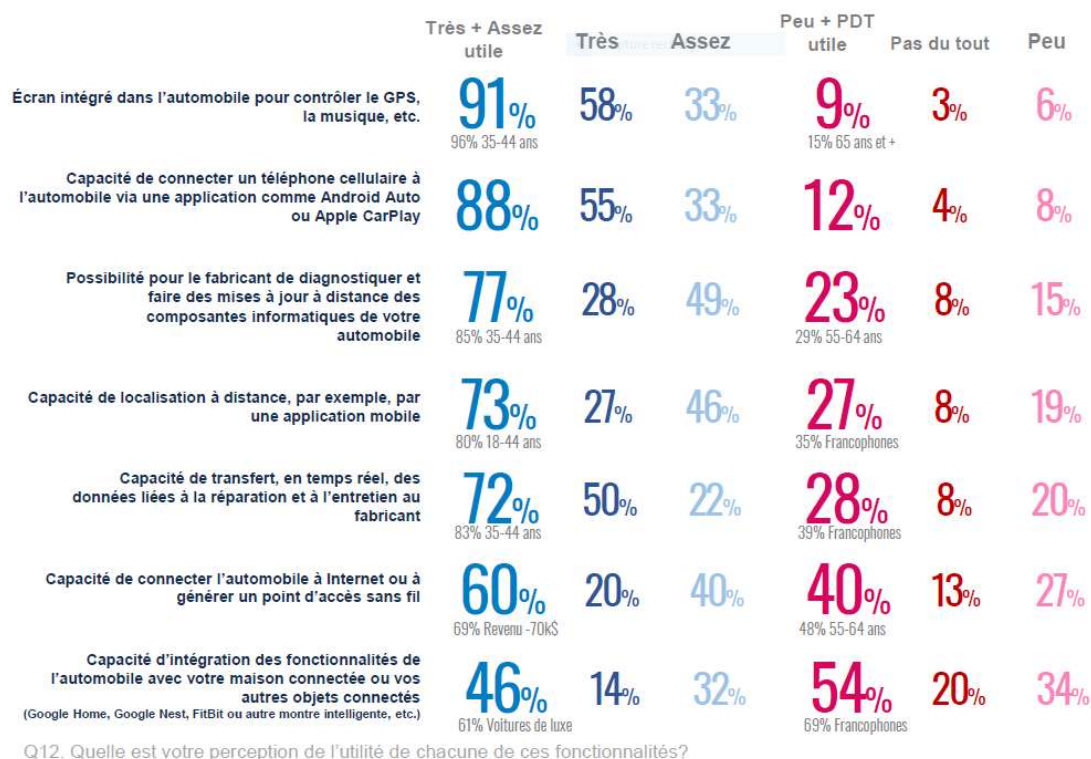


Figure 3

Figure 3 indique l'utilité perçue de diverses fonctionnalités chez tous les répondants. Le taux d'utilisation de ces fonctionnalités est plus bas que leur utilité perçue dans tous les cas, sauf la capacité d'intégrer la voiture avec une maison ou un objet connecté. Cette fonctionnalité a été perçue comme utile par seulement 46 % des répondants, bien qu'elle soit utilisée par 54 % des répondants qui ont cette technologie dans leur voiture. Toutefois, il semble en général que les personnes se montrent plus positives quant à l'utilité de la technologie lorsqu'elle n'est pas présente dans leur voiture.

Les personnes âgées de 35 à 44 semblent les plus convaincues quant à l'utilité des fonctionnalités connectées.

Enfin, en ce qui concerne la technologie dans le choix du véhicule, l'écran (85 %) et la capacité de connecter un cellulaire à la voiture sont de loin les technologies les plus importantes selon les consommateurs (82 %). En revanche, les répondants trouvent moins importants dans leur choix d'achat la capacité de localiser la voiture à distance (58 %), le transfert de données de réparation (52 %) ou la capacité pour la voiture de se connecter à Internet ou de créer un point d'accès sans fil (42 %).

4.1.2 Les abonnements et assurances connectés

Nous avons également sondé les consommateurs sur l'idée de payer un abonnement pour certaines fonctionnalités connectées.

Les répondants se montrent assez défavorables à cette idée. Seule la moitié se disent favorables à l'idée de payer un abonnement pour certains services (cartes virtuelles, système de navigation, système de diagnostic à distance, mises à jour à distance, localisation de l'automobile à distance, déblocage de fonctionnalités physiques). Ils sont particulièrement contre l'idée de payer un abonnement pour les services d'infodivertissement (37 % favorable) ou pour une connexion Internet dans la voiture (43 %). Nous pouvons émettre l'hypothèse que cette réticence pourrait être due au fait que les conducteurs ont déjà accès à ces services par le biais de leur téléphone cellulaire.

La grande majorité des répondants (88 % et plus, selon la fonctionnalité) n'ont jamais payé un abonnement pour des fonctionnalités connectées, bien que la pratique soit environ deux fois plus courante chez les jeunes et les conducteurs de voitures de luxe. Cependant, nous avons découvert lors des entrevues que le nombre de répondants qui ont réellement payé un abonnement pour un service connecté est encore plus faible, car plusieurs répondants parmi ceux qui ont indiqué avoir déjà payé un abonnement ont confié l'avoir fait par erreur. Beaucoup d'entre eux ont reçu ces services avec l'acquisition de la voiture pendant une période d'essai gratuite. D'autres faisaient référence lors du sondage à des abonnements sur leur téléphone cellulaire, soit un abonnement à un forfait de données mobiles, plutôt qu'à un point d'accès Wi-Fi dans la voiture.

Enfin, seuls 16 % des répondants ont indiqué d'avoir adhéré à des assurances où le calcul de la prime est basé sur les données issues de leur automobile ou de leur cellulaire. Ce chiffre est cependant bien plus élevé (29 %) chez les conducteurs de 18 à 34 ans. Un grand nombre de répondants ont indiqué qu'ils trouvent cette technologie trop intrusive (44 %) ou qu'ils craignent que l'assureur utilise à mauvais escient les données recueillies (33 %). Seuls 22 % trouvent que c'est une bonne façon d'économiser et 14 % trouvent que c'est utile, car ça permet de voir son historique de conduite et de recevoir des conseils.

4.1.3 La vie privée et les données liées à l'utilisation de la voiture

Nous avons sondé les consommateurs sur les pratiques des fabricants en ce qui concerne la collecte de données liées à l'utilisation de leur voiture.

Sur l'ensemble des répondants, 41 % croient que le fabricant de leur voiture est capable de collecter des données liées à l'utilisation de la voiture. Toutefois, ce chiffre monte à 53 % pour les répondants possédant une voiture plus récente (2020 à 2024). Ce dernier pourcentage correspond au nombre minimum de répondants possédant une voiture connectée (52 %), ce qui suggère que les conducteurs des voitures plus récentes sont, en général, au courant de cette capacité.

Quatre-vingt-cinq pour cent des répondants croient que le fabricant ne peut pas collecter ou utiliser ces données sans le consentement exprès de la personne. Comme nous allons

voir dans la section 5, la législation canadienne permet une collecte de renseignements personnels qui reposerait sur un consentement implicite, sauf dans des circonstances spéciales. On peut supposer que les consommateurs ne sont pas au courant, étant donné leur réponse.

Bien qu'ils croient que le consentement exprès est requis pour la collecte de données liées à l'utilisation de leur véhicule, seuls 13 % des répondants disent qu'ils ont eu une invitation à consentir à ce genre de collecte ; ce chiffre monte à 22 % pour les conducteurs des voitures connectées. Dans l'ensemble, environ un tiers d'entre eux ont refusé, mais parmi les conducteurs des voitures connectées, ce chiffre tombe à 13 %. Deux tiers (67 %) affirment qu'ils n'ont jamais eu ce type de demande et 20 % ont dit qu'ils ne le savent pas. Rappelons que 41 % des répondants croient que leur fabricant collecte ces données et qu'au moins 52 % des répondants ont des voitures connectées. **Cela veut dire que le nombre de consommateurs auxquels on a demandé de consentir à la collecte de leurs données (ou qui se souviennent de cette demande) est nettement plus bas que le nombre de personnes concernées par cette pratique.**

Quand nous avons demandé si le fabricant de leur automobile a une politique de confidentialité qui explique les modalités de la collecte et l'utilisation de ces données, 38 % des répondants ont dit oui. Parmi eux, seuls 35 % (environ 7 % de l'ensemble des répondants) ont indiqué qu'ils en ont pris connaissance. Les chiffres sont nettement plus élevés pour les répondants âgés de 18 à 34 ans et les conducteurs de voitures de luxe ou de nouvelles voitures (2020 à 2024). 80 % des répondants ont indiqué que, lors de l'acquisition du véhicule, les conditions de la collecte, de l'utilisation et du partage de données ne leur ont pas été clairement expliquées. Les jeunes et les conducteurs de nouvelles voitures ou de voitures de luxe se rappellent en plus grande proportion avoir obtenu des explications relativement à ces pratiques lors de l'acquisition de la voiture.

Les chiffres sont similaires lorsqu'il s'agit de la collecte de données par des tiers qui offrent des services pour les voitures connectées, tels que Google, Apple ou les assureurs. Seuls 16 % des répondants indiquent qu'ils ont reçu une invitation à consentir à la collecte ou l'utilisation des données liées à l'utilisation de leur véhicule par un de ces tiers ; 48 % affirment qu'ils n'ont jamais eu ce type de demande ; les autres ne savent pas, ne se souviennent pas ou n'ont jamais utilisé un service tiers. Pourtant, on sait qu'environ 16 % des répondants ont accepté de partager ces données avec leur assureur et que 69 % des répondants ont déjà utilisé Android Auto (Google) ou Apple CarPlay, qui peuvent collecter des données liées à l'utilisation de la voiture.

Ces constats sont frappants en ce qui concerne le consentement à la collecte et au partage de données. Nos résultats indiquent qu'un grand nombre de consommateurs ne savent pas si leur fabricant collecte des données liées à l'utilisation du véhicule, ne savent pas si le fabricant a une politique de confidentialité, et n'ont pas reçu d'explications relativement à ces politiques au moment de l'acquisition du véhicule. De plus, les répondants indiquent qu'ils ne se souviennent pas avoir donné un consentement exprès à cette collecte de données ou à la collecte par des tiers, même si les données montrent qu'ils y ont été soumis.

Quand on leur interroge sur leurs inquiétudes, 65 % des répondants se disent très ou assez préoccupés par la collecte de données liées à l'utilisation de leur voiture. Ce nombre

est encore plus élevé (76 %) quand on parle de la vente de ces données à des tiers pour des fins publicitaires. Les personnes plus âgées sont plus inquiètes, et les jeunes et les francophones et Québécois le sont moins.

Seuls 20 % des répondants croient avoir des recours adéquats en cas d'utilisation de leurs données par une personne non autorisée, par exemple, à la suite d'une fuite de données, alors que 40 % ne le savent pas. Encore une fois, les jeunes (18 à 34 ans) et les conducteurs de voitures de luxe se disent plus confiants que les autres groupes. Les femmes, les personnes âgées et les Québécois sont plus susceptibles d'avouer qu'ils ne savent pas s'ils ont des recours adéquats que les autres groupes.

Les répondants se montrent enthousiastes à l'idée d'un indice de vie privée, qui permettrait au consommateur, à partir d'une note globale, d'évaluer le niveau de protection de la vie privée offert par le fabricant d'une automobile. Une grande majorité (86 %) des répondants indiquent qu'un tel indice serait important ou très important dans leur prise de décision d'acquisition d'une voiture.

4.1.4 La réparation et les données de diagnostic

La longévité de la voiture est une qualité importante selon nos répondants : en moyenne, les répondants pensent que la durée de vie totale de leur voiture est de 13,7 ans et ils envisagent de la garder pendant une moyenne de 10,4 ans.

Nous avons présenté aux répondants le fait que les voitures connectées sont formées de dizaines d'unités électroniques de contrôle, plus communément appelées des ordinateurs, et contiennent des milliers de points de données et des millions de lignes de code. Face à ce constat, les répondants se montrent préoccupés quant aux enjeux de réparation.

Notamment, les répondants se montrent préoccupés par le risque de l'augmentation des coûts (88 %) et de la complexité (84 %) de réparation à cause de cette numérisation. On observe également des craintes en ce qui concerne le manque de mises à jour (76 % se disent préoccupés) ou d'accès aux pièces de réparation (76 %), ainsi que l'obsolescence des fonctionnalités connectées (73 %) et le manque d'accès aux données et logiciels de réparation (71 %). Pourtant, nous constatons que les Québécois sont moins inquiets que les autres répondants sur ce dernier point ; on peut supposer que certains sont rassurés par l'intégration de dispositions promouvant la réparation dans la loi québécoise en 2023 (voir la section 5.5).

Ensuite, nous avons présenté le fait que certaines automobiles qui disposent de fonctions connectées ont la capacité de générer et de collecter de l'information nécessaire à leur entretien et à leur réparation. Nous avons demandé aux répondants si cette information pouvait d'après eux être transmise au fabricant de leur automobile en temps réel grâce à la connexion Internet. Dans l'ensemble, 24 % des répondants ont dit oui, mais ce chiffre a été beaucoup plus élevé parmi les conducteurs des voitures de luxe (38 %) et des nouvelles voitures (36 %) et ainsi chez ceux pour qui il est plus probable que leur automobile dispose de fonctionnalités connectées. En revanche, seuls 11 % des répondants affirment avoir été invités à consentir à cette transmission de données (28 %

des conducteurs de voitures de luxe, 25 % pour les 18 à 34 ans). Encore une fois, on peut observer que même parmi ceux qui ont cette technologie dans leur voiture (ou parmi ceux qui ont connaissance de cette technologie), au moins la moitié ne se souviennent pas qu'on leur ait demandé leur consentement à la transmission de leurs données.

La grande majorité des répondants jugent qu'il est très (27 %) ou assez (54 %) facile de vérifier la fiabilité et la longévité d'une automobile avant de s'en procurer une, et qu'il est très (21 %) ou assez (53 %) facile de savoir si les pièces et les services de réparation seront aisément accessibles dans le temps. Cependant, les répondants sont très favorables à l'idée d'un indice de durabilité qui permettrait au consommateur, à partir d'une note globale, d'évaluer la réparabilité et la fiabilité des équipements. 40 % des répondants trouvent qu'un tel indice serait très important (40 %) ou assez important (49 %) dans le processus de la prise de décision d'acquisition d'une automobile (total de 89 %).

76 % des répondants se disent préoccupés par l'idée que les logiciels présents dans une voiture connectée pourraient limiter la possibilité de la personne de réparer son automobile ou de le faire réparer par un réparateur indépendant. Encore une fois, les Québécois sont moins préoccupés que les autres répondants à cet égard, peut-être grâce à une disposition adoptée récemment dans leur province, qui assure l'accès aux données diagnostiques des véhicules (section 5.5).

Enfin, nous voulions savoir si les répondants ont pris connaissance du contrat de licence d'utilisateur de leur véhicule, car ce document décrit les limites et les restrictions sur la manière dont le logiciel de la voiture peut être utilisé. 15 % des répondants disent l'avoir lu ; ce chiffre est plus élevé parmi les conducteurs de 18 à 34 ans (30 %), de 35 à 44 ans (20 %), les conducteurs des voitures de luxe (26 %) et ceux de nouvelles voitures (21 %). Ces chiffres sont similaires au nombre de répondants qui affirment qu'on leur a expliqué le contrat de licence lors de l'achat (17 % globalement). Toutefois, les entrevues suggèrent que le nombre réel est inférieur, car de nombreuses personnes interrogées à ce sujet semblent avoir mal compris au moment du sondage ce qu'est le contrat de licence.

4.2 Faits saillants des entrevues

4.2.1 Profils des répondants

Afin de mieux comprendre les réponses au sondage et la perspective des consommateurs possédant une voiture connectée, nous avons effectué 24²⁶³ entrevues parmi les répondants au sondage, entre le 28 août et le 25 septembre 2024. Au départ, nous avons

²⁶³ Notre objectif initial était de réaliser entre 30 et 40 entrevues, mais, après de nombreuses tentatives d'appels et l'exclusion de plusieurs participants, nous avons réussi à parler à 24 répondants. Plusieurs participants ont dû être exclus sur la base de leurs réponses, car ils ont indiqué qu'ils n'avaient pas répondu correctement au sondage et ne remplissaient donc pas les critères des entrevues. Par exemple, certains répondants avaient indiqué dans le sondage qu'ils possédaient un modèle de voiture qu'ils n'avaient pas en réalité ; interrogés à ce sujet, ils ont répondu qu'ils avaient rempli le sondage très rapidement et qu'ils n'avaient pas répondu avec précision.

tenté de ne mener des entrevues qu'avec des répondants qui ont payé au moins un abonnement pour avoir accès à un service connecté dans leur voiture : un point d'accès Wi-Fi, le déblocage de fonctionnalités physiques, la localisation de l'automobile à distance, un système de diagnostic à distance, et ainsi de suite. Nous avons sélectionné ces répondants, car nous voulions interroger uniquement les répondants possédant une voiture connectée et nous supposons qu'une personne ayant payé pour un service connecté dans sa voiture aurait une opinion plus développée sur le sujet que le répondant moyen.

Cependant, nous avons rapidement constaté une vaste mécompréhension des concepts de service connecté et d'abonnement à un service connecté parmi les répondants (voir la section suivante). Par la suite, nous avons ouvert la liste aux répondants possédant une voiture de 2018 et moins ayant une technologie ou une fonctionnalité connectée²⁶⁴, en présumant que le niveau de connectivité de leur véhicule serait plus élevé.

Autrement, nous avons constaté que quelques réponses données lors de l'entrevue différaient de celles qui avaient été données au sondage, notamment sur les questions concernant leur lecture de la documentation (politique de confidentialité et licence d'utilisation). Nous y reviendrons.

4.2.2 Expérience et compréhension des technologies

En parlant aux répondants qui ont indiqué qu'ils sont abonnés à un service connecté, il est devenu évident que les consommateurs ne sont pas familiarisés avec le fonctionnement de la technologie connectée dans leur voiture. Nombreux sont ceux qui ont indiqué dans le sondage avoir payé un abonnement pour un service connecté, alors que ce n'était pas le cas. Par exemple, certains ont déclaré avoir payé un abonnement pour un point d'accès Wi-Fi dans leur voiture, alors qu'en réalité, ils utilisaient les données mobiles de leur téléphone. D'autres ont des services connectés dans leur voiture, mais qui sont inclus par défaut, sans abonnement, malgré ce qu'ils semblent croire : plusieurs parlent d'une période d'essai des services connectés qui était incluse lors de l'acquisition du véhicule. D'autres encore n'ont pas bien compris ou n'ont pas bien répondu à la question: leur véhicule ne dispose tout simplement pas du service auquel réfère le sondage.

À quelques reprises, les répondants ont associé la notion de voiture connectée à la technologie hybride ou électrique, et ce, même après avoir reçu une explication de la notion de voiture connectée.

²⁶⁴ Nous avons aussi interviewé un répondant possédant une voiture d'avant 2018 dotée des fonctionnalités connectées.

4.2.3 La vie privée et les données collectées

Nous avons interrogé les répondants sur leurs réponses au sondage en ce qui concerne leurs niveaux de connaissance et de préoccupation quant à la collecte de données à partir de leur véhicule.

Nous avons d'abord posé des questions sur la politique de confidentialité : si la personne a indiqué lors du sondage l'avoir lu ou en avoir pris connaissance, qu'est-ce qu'ils ont retenu du document ?

En général, les répondants n'ont pas de souvenirs clairs de ce document. Ceux qui ont acheté des voitures auprès d'un particulier n'ont jamais eu cette information. Certains affirment avoir reçu l'information sur la collecte de données et la protection de la vie privée lors de l'achat, alors que d'autres ne s'en souviennent tout simplement pas. Une personne en particulier affirme qu'il est difficile de se souvenir d'informations qui datent de plusieurs années. La méthode de prise de connaissance de la politique de confidentialité varie également : certains ont eu des explications verbales du concessionnaire, d'autres l'ont lue et une personne l'aurait reçue par courriel. Une répondante a affirmé ne pas avoir lu la politique de confidentialité lors de la transaction, mais elle l'aurait fait ultérieurement, chez elle.

La quasi-totalité des répondants croit que les fabricants devraient avoir une politique de confidentialité et une répondante a mentionné que ces politiques seraient obligatoires, selon la nouvelle loi québécoise sur la protection de la vie privée.

Il est arrivé souvent que les réponses diffèrent de celles données lors du sondage en ligne. Si certains disent avoir lu la politique de confidentialité, mais en réalité c'est le concessionnaire qui la leur a expliquée. L'inverse est aussi vrai. Enfin, bien que plusieurs répondants affirment dans le sondage avoir lu les documents, on comprend que la plupart du temps, ils les ont simplement survolés avec le vendeur ou le concessionnaire.

En ce qui concerne le contenu, les interviewés ont peu de souvenirs ou de compréhension. Ceux qui ont dit en avoir pris connaissance réfèrent à la gestion de leurs données, aux aspects généraux de sécurité et de confidentialité (notamment, que les données ne seront pas partagées avec des tiers). Dans de nombreux cas, il est difficile d'obtenir des détails précis de la part des répondants comme « qui aura accès à vos données ? », « à quelles fins amasse-t-on vos données ? », etc. Beaucoup ne se rappellent plus. Parmi ceux qui s'en souviennent, ceux-ci identifient que les données et leur partage servent à assurer l'entretien ou la réparation du véhicule. Plusieurs personnes, mais non la majorité, affirment que leurs données ne seraient pas partagées avec des tiers ou pour des fins commerciales. Quelques personnes pouvaient identifier les personnes qui y auraient accès (une application, un centre de réparation, le fabricant, etc.). Deux personnes ont parlé des assureurs. Certains réfèrent au fait qu'il fallait télécharger une application mobile afin d'utiliser les services connectés.

Chez certains répondants, nous avons observé une insouciance relative face à la consultation et l'acceptation de la politique de confidentialité et un sentiment de confiance envers les vendeurs qui les réconforte dans le peu qu'ils savent.

Une autre personne, à qui le concessionnaire a expliqué la politique, exprime qu'il aurait souhaité avoir été plus adéquatement averti à ce moment et des risques concernant ses données.

En ce qui a trait aux inquiétudes concernant la collecte, nous avons constaté que les répondants craignent la fraude ou l'utilisation de données qu'ils considèrent comme sensibles. Plusieurs répondants racontent qu'ils appréhendent des fuites et du piratage. Les répondants reviennent souvent à la question des données financières ou des informations bancaires et médicales, qui les préoccupent davantage que leurs données liées à l'utilisation du véhicule. Une minorité de répondants appréhendaient qu'on puisse suivre leur localisation. Également, plusieurs répondants, mais pas la majorité, mentionnent l'analyse de leurs habitudes de conduites comme motif de préoccupation. Les données liées à la voiture leur semblent moins personnelles, bien que certains éprouvent un certain malaise à les partager.

Certains appréhendent la possibilité que leurs données soient vendues. Quelques répondants ont exprimé une réticence à ce que des entreprises tierces utilisent leurs données pour faire de la sollicitation pour leurs produits. Peu de répondants se disent inquiets du partage de données avec des compagnies d'assurance.

Quelques répondants ont également démontré une certaine indifférence envers la collecte et l'utilisation de leurs données. L'un a répondu que ça ne lui posait aucun problème de partager l'information selon laquelle il allait au Tim Hortons pour un café. Un répondant affirme que la collecte et l'utilisation de données ne le dérangent pas, mais cela dépend de l'usage qu'en font les entreprises.

La majorité des répondants croient qu'ils ont le droit de refuser la collecte de données. Une répondante dit qu'elle n'avait pas le choix d'accepter que ses données soient collectées vu qu'elle a choisi Tesla. Malgré cela, cette même répondante affirme avoir certaines inquiétudes par rapport à la collecte de données, mais, en même temps, elle avoue que de ne pas connaître la politique de confidentialité ne la dérange pas. Elle n'était pas la seule : plusieurs répondants qui se disent « vraiment préoccupés » ou « quelque peu préoccupés » par la collecte de données n'avaient pas lu la politique de confidentialité ou ne se sont pas informés.

En général, le niveau de préoccupation des répondants en entrevue correspond avec ce qu'ils avaient répondu lors du sondage, mais, pour certains, il y a eu de petites divergences. Une répondante en particulier dit qu'elle était préoccupée au départ, puis, après s'être informée auprès de gens qui s'y connaissent (on ne sait pas lesquels), qui lui ont dit qu'il existe des manières de protéger ses données, sa préoccupation s'est amenuisée. Une autre a même été inquiétée davantage par le fait qu'on lui a mentionné lors de l'entrevue qu'il pouvait y avoir une collecte de ses données et que celles-ci pouvaient être transférées aux fabricants.

Certains répondants sont préoccupés par la collecte de données par leur téléphone quand ils l'utilisent dans le véhicule. Par exemple, un répondant s'inquiète que le fabricant de son téléphone (Apple) puisse accéder à ses données de conduite.

Des répondants indiquent que le fait que la voiture soit louée réduisait leurs préoccupations face à la collecte des données.

4.2.4 La réparation et la connectivité

Ensuite, nous avons posé des questions sur les enjeux de la réparation et du droit de propriété. Les interviewés ont été interrogés sur leurs réponses au sondage quant à leur niveau de préoccupation concernant les obstacles à la réparation liés à la connectivité de leur voiture.

Il faut noter qu'une quantité appréciable de répondants avaient acquis leurs véhicules récemment et donc peu ont eu des problèmes nécessitant d'aller faire réparer leur véhicule. Ils n'avaient pas encore rencontré de problème avec le fait d'aller ou de ne pas aller chez le concessionnaire autorisé pour la réparation de leur véhicule.

On remarque que pour beaucoup de répondants, la réparation est une question de confiance et de relation avec le prestataire. Certains ont confiance en leur garagiste local et indépendant, d'autres ont développé une relation avec le concessionnaire. Certains évoquent le temps où l'on pouvait réparer soi-même ou avec l'aide d'amis, de parenté, de conjoints, ce qui n'est plus possible à cause de la complexité des voitures modernes, selon eux.

Il n'y avait pas de consensus sur le type de prestataire qui offre la meilleure qualité de réparations. Ce qui est important, c'est d'avoir l'option d'aller chez le prestataire de son choix. Plusieurs répondants parlent de la perte de la garantie comme étant le risque qu'ils courent s'ils ne font pas réparer leur voiture auprès du concessionnaire autorisé. Une répondante a affirmé qu'elle préférerait faire réparer son véhicule chez le concessionnaire autorisé, car elle craint que les garages locaux puissent subtiliser ses données.

De nombreux répondants sont préoccupés par la concurrence faussée entre le concessionnaire autorisé et les garages indépendants. Un répondant parle d'un monopole des fabricants, lesquels pourraient dicter leur prix, seraient supposément plus élevés qu'ailleurs. Avoir le choix permet de trouver la meilleure qualité de service et le meilleur prix. Plus d'une personne a rapporté que les prix étaient nettement plus élevés chez le concessionnaire.

En ce qui concerne la connectivité, un répondant partage ses préoccupations concernant les difficultés à faire réparer son véhicule sans avoir accès à un expert ou au logiciel requis. Cette personne s'est inquiétée de ce qui se passerait en cas d'urgence si le concessionnaire officiel n'était pas disponible ; serait-elle toujours en mesure de faire réparer son véhicule par un mécanicien indépendant ? Une répondante possédant un Tesla affirme qu'il peut s'avérer difficile de trouver un réparateur autorisé de Tesla dans des endroits un peu plus reculés, comme à l'Île-du-Prince-Édouard. Cela lui cause des inquiétudes.

Une autre répondante s'inquiète du risque que les concessionnaires accèdent eux-mêmes à distance à la voiture connectée afin de provoquer une défectuosité nécessitant un entretien. Un des répondants raconte que John Deere impose des restrictions sur ses véhicules et machineries de ferme connectés.

4.2.5 Contrat de licence d'utilisateur final (CLUF)

Lors du sondage, environ 15 % des répondants ont dit avoir lu leur contrat de licence d'utilisateur, qui explique les restrictions en lien avec le logiciel du véhicule. Nous avons ainsi posé des questions sur ce document lors des entrevues.

Les répondants qui ont acquis leur véhicule d'un particulier n'ont pas obtenu la documentation concernant les conditions d'usage.

Certaines personnes qui ont acheté directement du concessionnaire n'ont pas non plus reçu d'information ou ne s'en souviennent pas.

Ceux qui ont indiqué avoir lu le contrat de licence comprennent encore moins et se rappellent moins ce document que la politique de confidentialité. Beaucoup d'entre eux n'ont visiblement pas compris de quoi il s'agit. Environ le tiers des interviewés qui ont indiqué l'avoir lu croyaient que nous faisons référence aux documents relatifs au financement de l'automobile. Quand nous avons clarifié, beaucoup d'entre eux ont indiqué qu'ils n'ont pas lu le CLUF. Une personne répond : « *nobody reads that* » ; une autre indique que c'est peut-être son conjoint qui saurait ces détails, mais qu'elle ne sait pas de quoi il en retourne. De plus,

- quelques-uns croyaient que nous faisons référence à la politique de confidentialité ;
- Une répondante pensait qu'il était question du manuel d'instruction ;
- Une autre semble plutôt faire référence aux conditions pour la location et le retour du véhicule ;
- Une autre personne mentionne ne pas se rappeler du détail, outre qu'il pourrait recevoir de l'assistance directe si ses applications de base ne fonctionnent pas ;
- Un autre répondant réfère à des éléments que l'on retrouve typiquement dans un manuel d'utilisateur, et il mentionne que son représentant et lui ont discuté de comment maintenir son automobile en état, à quelle fréquence il devait faire des vérifications et des réparations ;
- Une personne exprime qu'il est ardu de se souvenir de toute l'information à travers toute la paperasse qu'on lui a soumise lors de l'achat ;

Quelques répondants ont parlé des restrictions liées à l'utilisation du véhicule. Un répondant énonce que ses préoccupations pour la collecte de données visent justement la restriction d'utilisation possible par le fabricant s'il fait mauvais usage du véhicule. Une deuxième parvient, après des explications supplémentaires de l'intervieweur, à parler des restrictions à l'usage de son véhicule, mais surtout en lien avec sa garantie.

Dans l'ensemble, nous avons constaté que le CLUF semble relayé à un statut de paperasse parmi tant d'autres reçues lors de l'acquisition du véhicule, que les répondants ont plus ou moins comprise. Il semble que le fait d'avoir reçu des explications ou d'avoir lu la politique ne change pas vraiment le détail de ce que les consommateurs ont compris ou retenu.

4.2.6 Balance des inconvénients

Enfin, nous avons demandé aux répondants quelle était la balance des avantages et inconvénients en ce qui concerne la technologie connectée dans leur véhicule, vu les préoccupations et les risques discutés lors du sondage et de l'entrevue.

On peut constater que plus le véhicule est récent (encore plus s'il s'agit du modèle « de l'année »), mieux les répondants semblent tolérer les risques associés aux voitures connectées. Cela est vrai, peu importe l'âge ou le genre des répondants interviewés. On sent une certaine résignation chez des répondants quant à l'état actuel des avancées technologiques : « on est rendu là, c'est comme ça, il faut s'y faire ». Sans rejeter tout danger, ils acceptent la technologie parce qu'ils y voient des avantages, tout de même. Une autre répondante, moins préoccupée par la collecte de données, a même répondu qu'il faudrait que ce soit obligatoire pour les fabricants de mettre cette technologie connectée. Cela réduirait, selon elle, le risque de vols, entre autres.

Les réponses sont assez variées, mais somme toute, la plupart des répondants jugent que les avantages l'emportent sur les inconvénients et qu'ils reprendraient une voiture connectée. Bien sûr, il y a des exceptions, et certains demandent plus d'encadrement et plus de sécurité pour leurs données.

Les personnes qui utilisent beaucoup leur voiture tendent à valoriser les avantages des technologies connectées ; ça leur est pratique et ils ne souhaitent pas revenir en arrière.

Une personne a répondu que l'atteinte à ses droits en tant que propriétaire était trop importante ; celle-ci veut notamment pouvoir faire ses réparations à l'atelier mécanique de son choix. Cette personne s'inquiétait également des données personnelles récoltées par la voiture et envoyées à la tierce partie CarFax. Cette personne n'avait d'ailleurs plus de voiture connectée au moment de l'entrevue.

Une répondante a exprimé son désir de pouvoir désactiver les fonctionnalités connectées lorsqu'elle ne les utilise pas, estimant qu'elle peut obtenir de l'assistance facilement en ville s'il y avait une urgence, mais moins facilement en région moins densément peuplée. Une répondante suggère d'ajouter des couches de sécurité supplémentaires afin d'amoindrir les risques, notamment en ce qui concerne la collecte, l'utilisation et la sécurité des données. Un autre répondant affirme que les risques d'atteinte à ses données personnelles outrepassent les avantages de la voiture connectée, à moins qu'on ne renforce les politiques publiques et la réglementation.

4.3 Analyse

En mettant ensemble les résultats du sondage et des entrevues, nous en arrivons à certains constats.

4.3.1 La technologie

Nous avons remarqué que les fonctions connectées étaient plus présentes dans les nouvelles voitures et les voitures de luxe. D'une manière générale, nous avons observé que les jeunes conducteurs semblent à la fois mieux informés sur la technologie et moins inquiets à ce sujet. Les conducteurs de voitures récentes sont également plus au courant des technologies connectées. Cela suggère tout d'abord qu'il existe une différence entre les générations et que les jeunes consommateurs sont plus habitués à la technologie connectée et à ses conséquences que leurs aînés. Les résultats suggèrent également que plus une voiture est connectée, plus le conducteur est conscient de la technologie.

Le sondage et les entrevues ont révélé que de nombreux consommateurs ne comprennent pas la technologie qui est dans leur voiture. Parfois, les consommateurs ne font pas la différence entre leur voiture ayant sa propre connectivité et leur voiture utilisant la connectivité de leur téléphone cellulaire, même si nous avons expliqué la différence.

L'écran et la connexion au cellulaire sont les fonctionnalités les plus connues et les plus importantes pour les consommateurs, même chez ceux qui ont d'autres fonctionnalités connectées dans leur voiture. Ceci n'est pas surprenant, car ces technologies sont présentes depuis plus longtemps et elles semblent répondre aux principaux besoins des consommateurs, en leur permettant d'accéder aux fonctions « connectées » dans leur voiture par le biais de leur téléphone cellulaire. C'est-à-dire que la connexion par le biais du téléphone cellulaire permet l'utilisation et l'affichage sur l'écran de leur voiture des applications connectées à Internet ou à un réseau cellulaire, telles que la navigation, l'infodivertissement, les textos, les appels téléphoniques, etc. Il nous semble que ce type de connectivité indirecte répond aux besoins de nombreux répondants, étant donné qu'ils ont déclaré que certaines fonctions connectées n'étaient pas les plus utiles ou intéressantes. Par exemple, la connexion à Internet ou la capacité de générer un point d'accès sans fil ne sont pas nécessairement perçues comme importantes dans le choix d'une voiture. Nous pouvons émettre l'hypothèse que cette fonctionnalité n'est pas perçue comme nécessaire tant que le téléphone cellulaire a déjà une connexion Internet via les données mobiles. Tant que la voiture est connectée d'une manière ou d'une autre, elle répond à ces besoins.

4.3.2 La collecte de données

Les réponses données au sondage et aux entrevues permettent de conclure que les consommateurs ne donnent généralement pas de consentement exprès, libre ou éclairé aux pratiques de collecte, d'utilisation ou de communication de leurs renseignements personnels. Ils ne comprennent pas bien les risques associés à ces pratiques non plus.

Alors que la plupart des répondants pensaient que leur consentement exprès était requis pour la collecte de données, très peu se souviennent qu'on leur ait demandé leur consentement. Le pourcentage de personnes ayant indiqué qu'elles utilisaient un service connecté était bien plus élevé que le nombre de personnes qui se souvenaient qu'on leur avait demandé de consentir à la collecte de données. Seuls 22 % des conducteurs des voitures dotées des fonctionnalités connectées se souviennent qu'on leur a demandé leur consentement à la collecte des données liées à leur véhicule, et sur ces 22 %, seuls 13 % ont refusé.

Il en va de même lorsque nous posons la question spécifique du partage des données de réparation par les voitures : le nombre de personnes qui déclarent que leur voiture peut transférer ces données est supérieur au nombre de personnes qui déclarent avoir été invitées à donner leur consentement à cet égard. Ceci est également vrai en ce qui concerne les applications tierces : beaucoup plus de personnes utilisent les services d'assurances basés sur l'utilisation du véhicule ou de Google ou d'Apple que le nombre de personnes qui se rappellent avoir été invitées par l'un de ces tiers (ou d'autres) à consentir à la collecte. Dans tous ces cas, il est possible que la personne ait donné son consentement sans toutefois s'en être rendu compte, par exemple si la demande se trouvait dans l'un des nombreux documents signés lors de la transaction ou si celle-ci s'est rapidement affichée sur l'écran de la voiture lors de la première utilisation. D'autres peuvent avoir oublié. Quoi qu'il en soit, la demande n'était manifestement pas expresse ou perceptible pour les répondants.

Comme nous le verrons à la section 5, la législation canadienne sur la protection de la vie privée n'exige généralement pas de consentement explicite si la collecte et l'utilisation des données sont raisonnables ou appropriées (et au Québec, si les données ne sont pas sensibles). Pourtant, la transparence est requise : la personne qui collecte les données doit aviser la personne de l'objectif de la collecte, de ses droits, etc. Or, nous avons constaté que presque aucune des personnes interrogées ne connaissait les informations pertinentes au moment où le consentement aurait (vraisemblablement) dû être donné. Beaucoup n'avaient pas lu la politique de confidentialité et n'en savaient rien à son sujet. Les personnes qui ont acheté une voiture d'occasion n'ont pas été informées de l'existence de ce document lors de l'acquisition de la voiture.

Même ceux qui ont indiqué avoir pris connaissance de la politique de confidentialité ont fait preuve d'un manque de compréhension lorsqu'elles ont été interrogées. Seule une poignée de personnes interviewées ont pu nous donner des précisions sur cette politique, en déclarant, par exemple, qu'elle indique que les données seront partagées avec le fabricant. De plus, bien que nous n'ayons pu vérifier l'exactitude de ces déclarations, certaines d'entre elles nous ont semblé douteuses (par exemple, que les données ne seraient pas partagées avec des tiers ou qu'elles ne seraient utilisées qu'à des fins d'entretien). La plupart des personnes qui en ont pris connaissance n'avaient que de vagues souvenirs et des suppositions quant au contenu de la politique de confidentialité. En général, les répondants qui ont lu la politique de protection de la vie privée ou à qui on l'a expliquée comprennent tout aussi mal les pratiques de collecte, d'utilisation et de partage de données que ceux qui ne l'ont pas lue ou à qui on l'a expliquée. Quelques répondants indiquent que le fait que la voiture soit louée réduisait leurs préoccupations

face à la collecte des données; cela démontre bien à quel point ces pratiques ne sont pas bien comprises.

Cela dit, les jeunes et les personnes dont les voitures possèdent plus de fonctionnalités connectées semblent plus conscients de l'existence de ces pratiques et se montrent plus insouciants quant à leur niveau de protection en matière de vie privée. Cela signifie-t-il que les pratiques changent ? Les voitures étant de plus en plus connectées, les gens sont-ils mieux informés ? Ou peut-être que les jeunes sont tout simplement plus conscients de ces risques ou y sont habitués ? Quoi qu'il en soit, ces répondants étaient tout aussi incapables que les autres conducteurs d'expliquer ce qu'est la politique de protection de la vie privée lors de l'entrevue. Les Québécois ont également indiqué lors du sondage qu'ils sont un peu moins inquiets, et plus optimistes quant à leurs recours en cas de problème. Nous nous demandons si les Québécois sont moins inquiets que les autres grâce à la réforme de la loi provinciale sur la protection des renseignements personnels en 2021 ; une personne a en effet mentionné la nouvelle loi lors de l'entrevue.

Même si les répondants se disent préoccupés, l'entrevue révèle que les inquiétudes des consommateurs ne sont pas précises. Quand nous avons demandé aux consommateurs de nous parler de leurs préoccupations, ils nous ont parlé de la fraude, du piratage et des fuites de données, de l'abus ou de la perte de contrôle sur l'utilisation de données financières et bancaires ou de leurs renseignements médicaux. Étonnamment, peu de répondants considèrent les données de localisation ou les données liées à l'automobile comme sensibles et leur utilisation ne les inquiète souvent pas. Comme nous l'avons vu plus haut, les données de localisation peuvent révéler d'énormes quantités d'informations sensibles sur une personne, telles que ses habitudes financières, ses traitements médicaux, etc. Ces données sont particulièrement révélatrices lorsqu'elles sont combinées avec les données relatives au véhicule, qui peuvent indiquer l'heure à laquelle la personne a visité un endroit, la durée de la visite, etc. Il apparaît donc que l'évaluation des risques par les personnes interrogées n'est pas approfondie. Elles s'inquiètent de l'utilisation illégale de leurs données bancaires ou médicales, mais se préoccupent beaucoup moins de l'utilisation dite légale d'autres données hautement sensibles pour des fins commerciales ou inconnues.

En outre, bien que les personnes se disent inquiètes dans le sondage, certains montrent des signes de complaisance lors de l'entrevue. Outre la méconnaissance des risques, nous pouvons supposer que cette insouciance est due au fait que certains consommateurs sont habitués à ces pratiques ou estiment qu'ils n'ont pas le choix.

Ces résultats jettent un doute sur l'idée que les consommateurs donnent un consentement libre et éclairé aux pratiques de collection de renseignements personnels, car la majorité des personnes ne se souviennent pas avoir consenti à la collecte de données et n'ont pas une connaissance ou une compréhension suffisante des pratiques pour donner un consentement éclairé. Et même s'ils ont compris ces pratiques, il est clair qu'ils n'en saisissent pas pleinement les risques.

4.3.3 La réparation et la propriété

Tant dans le sondage que dans les entrevues, les répondants ont indiqué qu'ils apprécient la réparabilité et que la longévité du véhicule est importante. Il n'y a pas eu de consensus quant à savoir qui serait le mieux placé pour réparer une voiture (concessionnaire, réparateur indépendant, un proche), mais il est clair que les personnes interrogées souhaitent avoir le choix en la matière. Ce qui les inquiète est la possibilité de ne pas avoir le choix du réparateur à cause des restrictions technologiques ou de la complexité du véhicule. Même s'ils ne comprennent pas la technologie ou le mécanisme, ou s'ils ont des opinions divergentes sur la personne la mieux placée pour réparer leur véhicule, les répondants tiennent à avoir le choix de leur prestataire.

Pratiquement aucun des répondants ne savait ce qu'était un contrat de licence d'utilisateur final. Une seule personne a indiqué qu'elle craignait que l'accès à son véhicule soit limité par le concessionnaire en raison de sa connectivité. La valeur du consentement des consommateurs aux restrictions quant à l'utilisation ou à la réparation de leur véhicule – imposées par la technologie, par la connectivité ou stipulées dans les CLUF – doit donc être remise en question.

4.3.4 La réglementation comme solution ?

Certaines réponses données au sondage et aux entrevues suggèrent qu'une plus grande protection réglementaire pourrait contribuer à atténuer certains des risques soulevés et certaines des inquiétudes des répondants.

En ce qui concerne la protection de la vie privée et la réparation, les Québécois sont moins inquiets que leurs homologues du reste du Canada. Nous émettons l'hypothèse que cela est dû au fait que le Québec a récemment légiféré pour mieux protéger les consommateurs dans ces deux domaines. Un meilleur encadrement dans le reste du pays peut apaiser les inquiétudes des consommateurs.

La grande majorité des répondants au sondage ont déclaré qu'ils souhaiteraient disposer d'un indice de réparabilité et d'un indice indiquant le niveau de la protection de la vie privée. Lors des entrevues, nous avons entendu plusieurs personnes faire une allusion positive à l'intervention réglementaire, en disant qu'elle pourrait être le seul moyen d'atténuer certains des risques identifiés. Quelques-uns ont déclaré que le gouvernement devrait intervenir pour mieux protéger la sécurité des données et pour s'assurer que les consommateurs ont le choix de refuser la collecte de données.

Comme nous le verrons dans la section suivante, le modèle actuel de protection de la vie privée repose en grande partie sur la transparence et sur le consentement des consommateurs aux pratiques de collecte et d'utilisation de données. Cependant, le sondage et les entrevues démontrent que les répondants n'ont qu'une vague compréhension de ces pratiques et des risques pour la vie privée qui y sont associés. Comme nous le verrons également, à l'exception du Québec, le droit à la réparation est

peu protégé au Canada. Il n'est donc pas surprenant que certains des répondants ressentent le besoin d'une plus grande protection législative.

4.4 Faits saillants

Nous avons mené un sondage auprès de plus de 1 000 consommateurs canadiens afin de connaître leurs pratiques, connaissances, perspectives et inquiétudes relatives aux voitures dotées de composantes technologiques. Ensuite, nous avons effectué des entrevues semi-dirigées avec 24 répondants possédant une voiture avec au moins une technologie connectée. Cette recherche nous amène aux conclusions suivantes concernant la technologie :

- D'une manière générale, nous avons observé que les jeunes conducteurs semblent à la fois mieux informés sur la technologie dans leur véhicule et moins inquiets à ce sujet. Les conducteurs de voitures récentes sont également plus au fait des technologies connectées.
- Cependant, de nombreux consommateurs ne comprennent pas la technologie dans leur voiture, au point qu'ils l'ont mal identifiée dans le sondage et dans les entrevues.

En ce qui concerne la collecte de leurs renseignements personnels :

- Très peu de personnes se souviennent qu'on leur a demandé leur consentement. Même ceux qui ont indiqué avoir pris connaissance de la politique de confidentialité ont fait preuve d'un manque de compréhension lorsqu'elles ont été interrogées. En général, les répondants qui ont lu la politique ou à qui on l'a expliquée sont généralement aussi ignorants que ceux qui ne l'ont pas lue ou à qui on ne l'a pas expliquée.
- Cela dit, les jeunes et les personnes possédant des voitures plus connectées semblent plus conscients de l'existence de ces pratiques et se montrent plus insouciantes quant à leur niveau de protection en matière de vie privée.
- Même si les répondants se disent préoccupés, l'entrevue révèle que les inquiétudes des consommateurs ne sont pas précises ou réfléchies.
- Les consommateurs craignent la fraude, le piratage et les fuites de données, l'abus ou la perte de contrôle sur l'utilisation de données financières, bancaires et médicales, mais sont plus ou moins ambivalents en ce qui concerne les utilisations « légales » de leurs données, même les données sensibles comme les données de localisation.

Ces résultats nous incitent à remettre en question le modèle de protection de la vie privée basé sur le consentement. 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.

Plusieurs consommateurs ont déclaré que le gouvernement devrait intervenir pour s'assurer que les consommateurs ont le choix de refuser la collecte de données et pour ajouter des couches de sécurité supplémentaires pour la collecte de données.

En ce qui concerne la réparation :

- Tant dans le sondage que dans les entrevues, les répondants ont indiqué qu'ils apprécient la réparabilité et qu'ils veulent garder le choix de leur réparateur. Ils critiquent l'idée d'un monopole des fabricants sur la réparation.
- Les consommateurs se disent inquiets des risques liés à la connectivité et la réparation.
- Les consommateurs ne savent pas ou ne comprennent pas ce que sont les contrats de licence d'utilisateur final (CLUF). La valeur du consentement des consommateurs aux restrictions quant à l'utilisation ou à la réparation de leur véhicule – imposées par la technologie, par la connectivité ou stipulées dans les CLUF – doit donc être remise en question.
- La grande majorité des personnes interrogées dans le cadre du sondage ont déclaré qu'elles souhaiteraient disposer d'un indice de réparabilité et d'un indice indiquant le niveau de la protection de la vie privée.

5 L'adéquation de la législation canadienne

Dans cette section, nous examinons l'adéquation du cadre législatif quant aux risques et préoccupations identifiés dans les sections précédentes. Notre analyse se concentra sur deux sujets : la protection de la vie privée et des renseignements personnels et le droit à la propriété, y compris le droit à la réparation. Pour chacun de ces sujets, nous survolerons l'encadrement juridique en place du point de vue du droit des consommateurs. Ensuite, nous procéderons à une analyse du cadre législatif afin d'évaluer s'il encadre les risques et répond aux préoccupations des consommateurs tels qu'identifiés dans la recherche. Enfin, nous examinerons le cadre réglementaire applicable aux États-Unis, en Union européenne et en Australie ; lorsque ces législations ont adopté des mesures ciblées concernant la voiture connectée, nous vérifierons leur adéquation.

5.1 La protection de la vie privée et des renseignements personnels : l'encadrement législatif

5.5.1 5.1.1 Survol des lois

Au Canada, la protection de la vie privée relève à la fois du gouvernement fédéral et des gouvernements provinciaux. Il existe de nombreuses lois canadiennes qui réglementent le traitement et la protection des renseignements personnels au Canada dans différents contextes et dans différents secteurs, par exemple, dans le secteur public, dans le domaine des soins de santé, et ainsi de suite. Cette section se concentre exclusivement sur les lois canadiennes qui réglementent la protection des renseignements personnels dans le secteur privé. Quatre lois de ce type sont actuellement en vigueur au Canada :

- **Au niveau fédéral :** La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE ou la loi fédérale)²⁶⁵. Pendant la rédaction de ce rapport, le gouvernement fédéral a examiné un projet de loi sur la protection des renseignements personnels dans le secteur privé, intitulée *Loi sur la protection de la vie privée des consommateurs* (LPVPC ou le projet de loi fédéral)²⁶⁶. Cette modification législative faisait partie du projet de loi C-27, déposé en 2022, puis mort au feuillet.
- **En Alberta :** La *Personal Information Protection Act* (APIPA)²⁶⁷.

²⁶⁵ Canada, *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5 [LPRPDE].

²⁶⁶ Chambre des communes du Canada, *Projet de loi C-27, Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*, première lecture, 70-71 Elizabeth II, 2021-2022, Partie 1, *Loi sur la protection de la vie privée des consommateurs* [LPVPC].

²⁶⁷ Alberta, *Personal Information Protection Act*, SA 2003, c P-6.5 [APIPA].

- **En Colombie-Britannique** : La *Personal Information Protection Act* (BCPIPA)²⁶⁸.
- **Au Québec** : La *Loi sur la protection des renseignements personnels dans le secteur privé* (LPRPSP)²⁶⁹.

Les sections suivantes présentent une vue d'ensemble des cadres établis par ces lois, en se concentrant sur les principes qui les sous-tendent plutôt que sur leurs dispositions spécifiques. Nous examinerons également les cadres, dans les domaines pertinents, qui proposaient d'établir le projet de loi C-27 dans cette section, même si le projet de loi est mort, car il est possible qu'un futur gouvernement relance ce projet de réforme²⁷⁰.

Toutes ces lois sont basées sur un ensemble de principes adoptés pour la première fois par l'OCDE en 1980 ; pour cette raison, les lois partagent plusieurs éléments²⁷¹. La législation québécoise a été adoptée à l'origine en 1993 et les autres ont été adoptés dans les années 2000. Seule la loi québécoise a été mise à jour de manière substantielle depuis son adoption, avec une réforme majeure en 2021. Pour cette raison, la législation québécoise est unique, à certains égards. Certaines parties de la loi fédérale ont été réformées au fil des ans pour ajouter des exceptions à l'obligation d'obtenir un consentement explicite, pour clarifier la notion de consentement dans certains cas, pour donner au Commissariat à la protection de la vie privée du Canada des pouvoirs plus étendus et pour ajouter des obligations de notification en cas de violation des données²⁷². Si une nouvelle version de la LPVPC – initialement proposée dans le projet de loi C-27 – est éventuellement adoptée, celle-ci pourrait constituer une révision en profondeur de la loi fédérale sur la protection de la vie privée.

Les lois fédérale et provinciales et le projet de loi s'appliquent à toute collecte, utilisation et communication de renseignements personnels par des organismes du secteur privé, par exemple, les fabricants des voitures connectées²⁷³.

²⁶⁸ Colombie-Britannique, *Personal Information Protection Act*, SBC 2003, c 63 [BCPIPIA].

²⁶⁹ Québec, *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1 [LPRPSP].

²⁷⁰ En effet, le projet de loi C-27 reprenait le contenu d'un projet de loi précédent, le projet de loi C-11, déposé en 2020 et également mort au feuillet.

²⁷¹ ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES (OCDE), *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, Paris, Organisation for Economic Co-operation and Development, 2002; BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 21, p. 76.

²⁷² Alexandra SAVOIE et Maxime-Olivier THIBODEAU, *Les lois fédérales du Canada sur la protection de la vie privée*, 2007-44-F, Ottawa, Bibliothèque du Parlement, 2020, en ligne : <https://lop.parl.ca/sites/PublicWebsite/default/fr_CA/ResearchPublications/200744E?> (consulté le 12 novembre 2024).

²⁷³ Le champ d'application de ces lois est parfois plus large ; par exemple, la LPRPDE s'applique également aux renseignements personnels concernant les employés d'une entreprise fédérale (LPRPDE, art. 4(1)); la LPRPSP s'applique aux renseignements personnels détenus par un ordre professionnel et à ceux détenus par un parti politique (LPRPSP, art.1). Dans cette section, nous n'examinons que les parties de ces lois qui s'appliquent à la collecte, etc., de renseignements personnels dans le secteur privé.

Pour alléger le texte, nous parlerons de la collecte (ou autre) de données lorsque nous ferons référence à la collecte, à l'utilisation et au partage des données dans cette section du rapport.

La LPRPDE s'applique aux organisations du secteur privé dans le cadre de leurs activités commerciales partout au Canada, sauf si l'organisme ne collecte, n'utilise ou ne partage pas des données qu'à l'intérieur d'une des trois provinces ayant adopté sa propre législation en cette matière²⁷⁴. Si, par exemple, une entreprise ne collecte, n'utilise ou ne partage des données qu'à l'intérieur du Québec, seule la LPRPSP québécoise s'applique à elle. Si les données traversent une frontière entre deux pays ou provinces, les deux législations s'appliquent²⁷⁵.

5.1.2 Les notions de base

Comme indiqué ci-dessus, chacune de ces lois s'applique à la collecte, etc., des renseignements personnels par des entités commerciales²⁷⁶. La notion de « **renseignement personnel** » est définie dans ces instruments juridiques comme étant tout renseignement concernant un individu identifiable²⁷⁷. Seule la loi québécoise ajoute qu'un renseignement qui, *directement ou indirectement, permet d'identifier la personne* est considéré comme un renseignement personnel²⁷⁸. Toutefois, cette notion large de renseignement personnel est celle qui a été adoptée par les tribunaux canadiens²⁷⁹. Cela signifie que toute collecte, etc., d'un renseignement qui peut être relié à une personne identifiée ou qui permet d'identifier une personne est visée par ces lois.

²⁷⁴ Les trois lois provinciales citées sont considérées comme « essentiellement similaires » en principe à la LPRPDE et les organismes de ces provinces sont donc exclus de l'application de cette loi, selon l'article 26(2) de la LPRPDE. La règle générale souffre de certaines exceptions pour les entreprises sous réglementation fédérale (banques, télécoms, etc.).

²⁷⁵ COMMISSARIAT A LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Lois provinciales qui peuvent s'appliquer au lieu de la LPRPDE » (29 mai 2017), en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/prov-lprpde/> (consulté le 6 novembre 2024).

²⁷⁶ LPRPSP, art. 1; BCPIPA art. 2; APIPA arts. 3 et 4; LPRPDE art. 3; LPVPC 5 et 6.

²⁷⁷ BCPIPA, art. 1; APIPA, art. 1(1)(k); LPRPDE, art. 2(1); LPVPC, art. 2(1).

²⁷⁸ LPRPSP, art. 2.

²⁷⁹ COMMISSARIAT A LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Bulletin d'interprétation : Renseignements personnels » (11 octobre 2013), en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/bulletins-sur-l-interpretation-de-la-lprpde/interpretations_02/> (consulté le 13 novembre 2024); BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 21, p. 81; BARBARA VON TIGERSTROM, *Information & Privacy Law in Canada*, Toronto, Irwin Law Inc., 2020, p. 301-303. Voir aussi COMMISSARIAT A LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « L'Internet des objets - Introduction aux enjeux relatifs à la protection de la vie privée dans le commerce de détail et à la maison » (17 février 2016), en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2016/iot_201602/> (consulté le 29 octobre 2024).

La loi québécoise et le projet de loi fédérale font également référence aux concepts de **dépersonnalisation** et **d'anonymisation**. Les autres lois passent sous silence ces notions. La loi québécoise stipule qu'un renseignement est anonymisé « lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne²⁸⁰ ». Un organisme peut procéder à l'anonymisation au lieu de détruire le renseignement personnel si c'est « pour l'utiliser à des fins sérieuses et légitimes²⁸¹ ». Un renseignement anonymisé n'est plus un renseignement personnel et n'est donc plus visé par la loi. L'anonymisation doit se faire en conformité avec les meilleures pratiques généralement reconnues et avec la réglementation gouvernementale²⁸². Bien que cette réglementation soit en vigueur²⁸³ et que l'anonymisation soit permise, la Commission d'accès à l'information du Québec, organisme responsable de surveiller l'application de la LPRPSP, considère qu'il est « quasi impossible de certifier que des renseignements anonymisés ne pourraient pas éventuellement être réidentifiés²⁸⁴ ». La LPVPC proposée par le gouvernement fédéral contient une définition similaire d'anonymisation et précise que les renseignements anonymisés sont exclus de l'application de la Loi²⁸⁵.

Quant aux données dépersonnalisées, la loi québécoise indique qu'un renseignement personnel est dépersonnalisé lorsqu'il « ne permet plus d'identifier directement la personne concernée²⁸⁶ ». Le projet de loi fédéral précise que l'acte de dépersonnaliser un renseignement personnel réduit le risque « sans pour autant l'éliminer, qu'un individu puisse être identifié directement²⁸⁷ ». Dans les deux cas, la dépersonnalisation rend plus difficile l'identification **directe** de la personne ; par exemple, les données sont dépersonnalisées si le nom ou autre méthode d'identification de la personne est effacé de l'ensemble des données collectées. La réidentification est pourtant possible et les renseignements dépersonnalisés sont donc considérés (dans la plupart des cas) comme des renseignements personnels protégés par les lois sur la protection de la vie privée²⁸⁸. Toutefois, les données dépersonnalisées peuvent être utilisées et partagées sans le consentement de la personne dans certains cas où ce consentement serait autrement nécessaire, n'eût été la dépersonnalisation desdites données²⁸⁹.

Tous ces instruments juridiques mentionnent la notion de renseignement **sensible**. En revanche, seule la loi québécoise en fournit une définition : un renseignement personnel est « sensible lorsque, de par sa nature notamment médicale, biométrique ou autrement

²⁸⁰ LPRPSP, art. 23.

²⁸¹ LPRPSP, art. 23.

²⁸² LPRPSP, art. 23.

²⁸³ Gouvernement du Québec, Décret 783-2024, 1er mai 2024.

²⁸⁴ « Conservation et destruction des renseignements personnels », *Commission d'accès à l'information du Québec*, en ligne : <<https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privées/conservation-destruction-renseignements-personnels>> (consulté le 13 novembre 2024).

²⁸⁵ LPVPC, arts. 2(1) et 6(5).

²⁸⁶ LPRPSP, art. 12.

²⁸⁷ LPVPC, art. 2(1).

²⁸⁸ Toutefois, la LPVPC indique que les renseignements dépersonnalisés ne sont considérés comme étant des renseignements personnels que dans certains articles de la loi : LPVPC, art. 2(3).

²⁸⁹ LPRPSP, art. 12. LPVPC, arts. 20, 21, 39.

intime, ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée²⁹⁰ ». La LPRPDE fédérale fournit des exemples plutôt qu'une définition :

Si certains renseignements sont presque toujours considérés comme sensibles, par exemple les dossiers médicaux et le revenu, tous les renseignements peuvent devenir sensibles suivant le contexte. Par exemple, les nom et adresse des abonnés d'une revue d'information ne seront généralement pas considérés comme des renseignements sensibles. Toutefois, les nom et adresse des abonnés de certains périodiques spécialisés pourront l'être²⁹¹.

L'absence de définition dans les autres lois et dans le projet de loi fédéral est étrange, puisque la notion de sensibilité apparaît à plusieurs reprises dans chaque instrument juridique. Souvent, la sensibilité doit être prise en compte pour déterminer si le consentement peut être implicite ou s'il doit être explicite²⁹². La notion est particulièrement présente dans le projet de loi, qui stipule que les renseignements concernant les mineurs sont considérés comme sensibles, que la sensibilité doit être prise en compte lors de l'analyse du caractère raisonnable de la collecte, etc., des données, lors de la détermination de la durée de conservation des informations, des mesures de sécurité appropriées, et ainsi de suite²⁹³.

Aucun de ces instruments, à l'exception de la loi québécoise, n'établit de règle stricte en matière de sensibilité ; ils obligent plutôt les entités privées à tenir compte de la sensibilité lorsqu'elles déterminent comment agir et ce qui est raisonnable. Au Québec, le fait qu'un renseignement personnel soit sensible crée l'obligation pour l'entité d'obtenir un consentement explicite avant de l'utiliser ou de le communiquer²⁹⁴.

5.1.3 La protection des renseignements personnels

5.1.3.1 Le consentement et la transparence

L'un des principaux mécanismes de protection de la vie privée prévus par ces lois est le principe selon lequel les personnes doivent consentir à toute collecte, utilisation ou communication de leurs renseignements personnels. Toutes les lois, incluant le projet de loi, sont basées sur ce principe ; en règle générale, aucune collecte (ou autre) de renseignements personnels ne peut avoir lieu, sauf si la personne concernée y donne son consentement²⁹⁵.

²⁹⁰ LPRPSP, art. 12.

²⁹¹ LPRPDE, annexe 1, art. 4.3.4.

²⁹² LPRPSP, art. 12 ; BCPIPA, art. 8 ; APIPA, art. 8(3) ; LPRPDE, annexe 1, arts. 4.3.4 et 4.3.6 ; LPVPC, art. 15(5).

²⁹³ LPVPC, arts. 2(2), 9, 12(2), 22, 53, 57, 74. La liste des obligations est similaire dans la législation québécoise.

²⁹⁴ LPRPSP, arts. 12 et 13.

²⁹⁵ Code civil du Québec, arts. 35-37 ; LPRPSP, arts. 12-13 ; BCPIPA, art. 6 ; APIPA, art. 7 ; LPRPDE, annexe 1, art. 4.3, LPVPC, art. 15(1).

Pour que le consentement soit valable, il faut que la personne ait une connaissance suffisante de ce à quoi elle consent. L'organisme doit ainsi fournir certaines informations à la personne concernée, comme l'objet et l'objectif de la collecte (ou autre), les droits de la personne en ce qui concerne leurs données, les coordonnées du responsable de la protection de la vie privée de l'organisme, etc.²⁹⁶. Certains de ces instruments juridiques précisent que l'information fournie ou la demande de consentement doivent être formulées en termes simples et clairs²⁹⁷ ou dans un langage « clair et raisonnablement compréhensible²⁹⁸ ». La législation fédérale actuelle et le projet de loi proposé, de même que la loi québécoise exigent que l'organisme rende accessibles ses politiques et pratiques de protection de la vie privée²⁹⁹.

Il y a pourtant plusieurs exceptions importantes à cette règle de base qui remettent en question la primauté du consentement. Le consentement n'est pas requis dans certaines situations spécifiques, nommées dans ces lois, comme : les urgences médicales, les enquêtes juridiques, la prévention de la fraude, etc.³⁰⁰; d'autres exceptions à cette notion sont plus générales et plus larges. Par exemple, la LPRPSP indique qu'un renseignement personnel peut, sans le consentement de la personne, être utilisé « au sein de l'entreprise » qui l'a collecté pour une fin autre que celle prévue « lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli³⁰¹ ». La LPVPC proposée indiquait qu'une entreprise peut collecter et utiliser des renseignements personnels sans le consentement de la personne et même à son insu si la collecte ou l'utilisation est faite en vue d'une activité d'affaires nommée dans la loi, par exemple, les activités nécessaires pour assurer la sécurité d'un produit, et si une personne raisonnable s'attendait à cette collecte ou utilisation³⁰².

L'importance du consentement comme mesure de protection est également remise en question par le fait qu'il peut souvent être déduit de manière implicite. Toutes les lois et le projet de loi indiquent que le consentement peut être implicite dans plusieurs cas, par exemple, s'il est « approprié » dans la situation³⁰³ ou si la personne fournit ses renseignements personnels à un organisme d'une façon volontaire et si « l'objectif [de la collecte ou autre] était considéré comme évident pour une personne raisonnable³⁰⁴ ». Le droit québécois établit comme règle générale que le consentement doit être manifeste,

²⁹⁶ LPRPSP, arts. 8, 8.1 et voir aussi 3.2 ; BCPIPA, arts. 7, 10 ; APIPA, art. 13, LPRPDE, annexe 1, arts 4.2.3, 4.3.2 ; LPVPC, art. 15(3).

²⁹⁷ LPRPSP, art. 14.

²⁹⁸ LPVPC, art. 15(4). LPRPDE, annexe 1, art. 4.3.2 prévoit que « les fins doivent être énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués ». Voir aussi BCPIPA, art. 7 et APIPA, art. 8(3) dans le contexte du consentement implicite. Voir aussi l'art. 6.1.

²⁹⁹ LPRPDE, annexe 1, art 4.8.1 ; LPVPC, art. 62; LPRPSP, art. 3.2.

³⁰⁰ Par exemple, LPRPSP, arts. 12 et 18; LPRPDE, art. 7 et annexe 1 art. 4.3; BCPIPA, arts. 12, 15, 18; APIPA, 14, 17, 20.

³⁰¹ LPRPSP, art. 12.

³⁰² LPVPC, art. 18. L'article proposé interdit cette collecte, etc., sans le consentement de la personne si c'est fait pour influencer la personne.

³⁰³ LPVPC, art. 15(5). Voir aussi LPRPDE, 4.3.6.

³⁰⁴ BCPIPA, art. 8 ; APIPA, art. 8.

libre, éclairé et donné à des fins spécifiques³⁰⁵, mais le consentement *exprès* est seulement exigé si les renseignements personnels en question sont sensibles³⁰⁶.

Est interdite par toutes les lois la pratique qui consiste à exiger le consentement à la collecte (ou autre) de renseignements personnels pour des fins non nécessaires ou non légitimes afin d'utiliser un bien ou un service³⁰⁷. Chacun de ces instruments prévoit également le droit de la personne concernée de retirer son consentement à la collecte (ou autre) de ses renseignements personnels³⁰⁸.

5.1.3.2 *Limites à la collecte, l'utilisation et la communication des renseignements personnels*

Les limites à la collecte de renseignements personnels sont prévues dans les instruments juridiques canadiens existants et proposés.

Tout organisme doit déterminer l'objectif de la collecte des renseignements personnels et limiter sa collecte à ce qui est nécessaire pour ces fins. En outre, ces objectifs sont souvent limités à ce qui serait considéré comme acceptable dans les circonstances par une personne raisonnable³⁰⁹.

Chacune de ces lois prévoit que les renseignements personnels collectés doivent être détruits lorsque les fins pour lesquelles ils ont été recueillis sont accomplies³¹⁰.

L'utilisation et la communication des renseignements personnels sont limitées par le même principe : en règle générale, l'entreprise ne peut utiliser ou transmettre le renseignement sauf pour la fin pour laquelle il a été collecté et si cela est raisonnable au vu des circonstances. Cependant, il y a plusieurs exceptions à ces règles, qui permettent l'utilisation et la communication de données pour d'autres fins, et ce, sans le consentement explicite de la personne dans plusieurs circonstances³¹¹. Seule la loi québécoise ne requiert pas que la communication soit en lien avec les fins de la collecte; cependant, toute communication est interdite à moins que la personne concernée n'y

³⁰⁵ LPRPSP, art. 14.

³⁰⁶ LPRPSP, arts. 12-13.

³⁰⁷ LPRPDE, annexe 1, art. 4.3.3 ; BCPIPA, art. 7(2); APIPA, art. 7(2); LPVPC, art. 15(7); LPRPSP, art. 9.

³⁰⁸ LPRPSP, art. 8 ; BCPIPA, art. 9 ; APIPA, art. 9; LPRPDE, annexe 1, art. 4.3.8, LPVPC, art. 17.

³⁰⁹ LPRPDE, art. 5(3) et annexe 1, arts 4.2.2 et 4.4 ; BCPIPA, art. 11 ; APIPA, art. 11 ; LPVPC, art. 12. Au Québec, la notion de la raisonnable nécessité est absente de la Loi qui parle plutôt d'un intérêt sérieux et légitime nécessaire afin de recueillir des renseignements personnels : LPRPSP, arts. 4 et 5.

³¹⁰ LPRPSP, art. 23 ; BCPIPA, art. 35 ; APIPA, art. 35 ; LPRPDE, annexe 1, art. 4.5.3 ; LPVPC, art. 53. La disposition dans la LPRPDE indique que l'organisme peut également dépersonnaliser les données.

³¹¹ En ce qui concerne l'utilisation: LPRPSP, art. 12 ; LPRPDE, annexe 1, art. 4.5 ; LPVPC, art. 12 ; BCPIPA, art. 14 ; APIPA, art. 16. En ce qui concerne la communication : BCPIPA, art. 17 ; APIPA, art. 19 ; LPRPDE, annexe 1, art. 4.5 ; LPVPC, art. 12.

consente ou que la loi ne le prévoi³¹². Encore une fois, le consentement peut être implicite sauf en cas de données sensibles.

5.1.3.3 *Le respect de la vie privée par défaut*

La loi québécoise comporte une disposition qui oblige les entreprises à respecter la vie privée par défaut :

Une personne qui exploite une entreprise et qui recueille des renseignements personnels en offrant au public un produit ou un service technologique disposant de paramètres de confidentialité doit s'assurer que, par défaut, ces paramètres assurent le plus haut niveau de confidentialité, sans aucune intervention de la personne concernée³¹³.

Sont exclus de cette obligation les paramètres de confidentialité d'un témoin de connexion.

Cette disposition a été ajoutée à la loi avec la réforme législative de 2021 et reste unique dans la législation canadienne sur la protection des renseignements personnels dans le secteur privé.

5.1.4 L'exactitude et l'accès aux renseignements personnels

Les entreprises ont l'obligation de veiller à ce que les renseignements personnels collectés soient exacts et à jour³¹⁴. Si ce n'est pas le cas, la personne concernée a le droit d'exiger que l'information soit rectifiée³¹⁵.

La personne a également le droit d'interroger l'organisme sur l'existence de renseignements personnels qui la concernent, de les consulter ou d'en obtenir une copie³¹⁶.

³¹² LPRPSP, art. 13, et voir les articles 18 et seq. pour les exceptions. Cette loi requiert également que les entreprises procèdent à une évaluation des facteurs relatifs à la vie privée avant de communiquer des données à l'extérieur du Québec, afin d'assurer que les renseignements bénéficieraient d'une protection adéquate : LPRPSP, art. 17.

³¹³ LPRPSP, art. 9.1.

³¹⁴ LPRPSP, art. 11 ; BCPIPA, art. 33 ; APIPA, art. 33 ; LPRPDE, annexe. 1, art. 4.6 ; LPVPC, art. 56.

³¹⁵ LPRPSP, art. 28 ; BCPIPA, art. 24 ; APIPA, art. 25 ; LPRPDE, annexe. 1, art. 4.9.5 ; LPVPC, art. 71.

³¹⁶ LPRPSP, art. 27 ; BCPIPA, art. 23 ; APIPA, art. 24 ; LPRPDE, annexe. 1, art. 4.9 ; LPVPC, art. 63.

5.1.5 Responsabilité et contrôle

L'organisme qui collecte, utilise ou partage des renseignements personnels en est responsable et il doit désigner une personne responsable de la mise en œuvre de ses obligations législatives³¹⁷.

Les organismes doivent prendre des mesures raisonnables pour assurer la sécurité et la protection des renseignements sous leur contrôle (ou sous le contrôle d'un tiers délégué, dans certains cas)³¹⁸. Toutes les lois sauf celle de la Colombie-Britannique prévoient des obligations en cas de fuite de données ou d'incident de confidentialité, notamment en requérant que l'organisme avise les personnes affectées ou l'organisme de contrôle pertinent³¹⁹.

Chaque loi donne également des pouvoirs à un organisme qui veille à l'application de la loi et qui a certains pouvoirs d'enquête, d'ordonnance, de traitement de plaintes et de contrôle de pratiques³²⁰. Certaines des lois prévoient également des sanctions pénales ou le paiement de dommages pécuniaires en cas de non-respect. Par exemple, la loi québécoise donne à la Commission d'accès à l'information du Québec le pouvoir d'intenter une poursuite pénale pour plusieurs infractions, notamment le fait de collecter, etc., les renseignements personnels en contravention de la loi ou de ne pas prendre des mesures de sécurité propres à assurer la protection de ces données³²¹.

En ce qui concerne les recours civils, toutes les lois fédérales et des provinces *common law* indiquent qu'une violation de la loi observée ou constatée par le commissaire pertinent donne à la personne concernée une cause d'action en dommages-intérêts contre l'organisme. Ainsi, la personne peut poursuivre l'organisme en justice pour la violation de ses droits, mais seulement après conclusion d'une enquête ou si une ordonnance est rendue par le commissaire contre l'organisation³²². En droit civil, la violation de la loi ou de la vie privée en général constitue une faute en soi et la législation québécoise prévoit

³¹⁷ LPRPSP, art. 3.1 ; BCPIPA, art. 4 ; APIPA, art. 5 ; LPRPDE, annexe. 1, art. 4.1 ; LPVPC, arts. 7, 8.

³¹⁸ LPRPSP, art. 10 ; BCPIPA, art. 34 ; APIPA, art. 34 ; LPRPDE, annexe. 1, art. 4.7 ; LPVPC, art. 57.

³¹⁹ LPRPSP, arts. 3.5 et seq. ; APIPA, art. 34.1 ; LPRPDE, arts. 10.1 et seq. ; LPVPC, art. 58 et seq.

³²⁰ Les organismes s'appellent : la Commission d'accès à l'information au Québec, the Information and Privacy Commissioner for BC, the Information and Privacy Commissioner of Alberta, et le Commissariat à la protection de la vie privée du Canada. Le projet de loi C-27 propose également la création d'un Tribunal de la protection des renseignements personnels et des données. Pour les pouvoirs, voir LPRPSP, arts. 42 et seq. ; BCPIPA, arts. 36 et seq. ; APIPA, arts. 36 et seq. ; LPRPDE, arts. 11 et seq. ; LPVPC, arts. 82 et seq.

³²¹ LPRPSP, arts. 90.1 et seq., 91 et seq. Voir aussi APIPA, art. 59. BCPIPA, art. 56 et la LPRPDE, art. 28, qui ne prévoient que des dispositions pénales assez restreintes. LPVPC, arts. 94 et 95 et seq. donneraient au Commissaire à la protection de la vie privée du Canada le pouvoir de recommander qu'une pénalité soit infligée à une organisation qui ne respecte pas certaines dispositions de la loi.

³²² BCPIPA, art. 57 ; APIPA, art. 60 ; LPRPDE, art. 14 ; LPVPC, art. 107.

des dommages-intérêts punitifs en cas de violation intentionnelle ou qui résulte d'une faute lourde³²³.

5.2 Analyse : adéquation de l'encadrement de la protection de la vie privée

Dans la section 3, nous avons identifié les risques pour la vie privée posés par les voitures connectées. En particulier, nous avons observé que les voitures connectées et leurs fabricants génèrent, collectent, utilisent et partagent des quantités massives de renseignements personnels concernant les conducteurs. Certaines de ces données sont très sensibles, et elles sont collectées, etc., souvent sans son consentement explicite, libre ou éclairé. Elles sont partagées avec des tiers, qui peuvent les utiliser pour des fins douteuses, comme leur agrégation et leur revente. Nous avons également constaté que les consommateurs n'avaient pas toujours accès aux données collectées sur eux et sur leurs véhicules, et qu'ils étaient exposés à des attaques de cybersécurité et des fuites de données.

Notre examen de la législation nous amène à deux conclusions principales. Premièrement, la législation actuelle semble peu adaptée pour faire face aux risques identifiés et deuxièmement, les fabricants automobiles semblent ne pas respecter certains éléments de la législation canadienne sur la protection de la vie privée.

5.2.1 Les limites à la collecte à l'utilisation et au partage des données sont inadéquates

Les lois canadiennes sur la protection de la vie privée exigent des organisations qu'elles identifient l'objectif de leur collecte, et qu'elles limitent leur collecte, etc., à ce qui est raisonnable ou nécessaire pour atteindre cet objectif. Les objectifs doivent également être raisonnables, acceptables ou légitimes et sérieux (selon la loi).

En théorie, ces encadrements peuvent limiter certains types de collectes de données dans le contexte de la voiture connectée. Toutefois, leur mise en application est limitée, et ils semblent inadéquats pour restreindre la collecte, l'utilisation et le partage massifs de renseignements personnels dans ce contexte.

En ce qui concerne la limite applicable aux objectifs mêmes, qui doivent être raisonnables, acceptables, légitimes ou sérieux, il s'agit d'une limitation essentielle, car sinon, les entreprises pourraient se fixer n'importe quel objectif, aussi intrusif soit-il (publicité ciblée, surveillance, etc.), et collecter tous les types de données pour le satisfaire. La limite est contextuelle et n'est donc pas spécifiquement définie dans la législation³²⁴. Il revient donc

³²³ LPRPSP, art. 93.1.

³²⁴ Même si l'évaluation du standard de la raisonnabilité est contextuelle, il s'agit d'une norme objective : *Canada (Commissaire à la protection de la vie privée) c. Facebook, Inc.*, 2024 CAF 140, par. 63.

aux entreprises, aux organismes chargés de l'application de la loi et aux tribunaux de les interpréter. Jusqu'ici, il y a eu peu de décisions en la matière, et peu d'objectifs commerciaux ont été jugés intrinsèquement déraisonnables³²⁵. Dans la décision de *Turner c. Telus Communications Inc.*, la Cour fédérale du Canada a pris en compte plusieurs éléments afin de déterminer le caractère raisonnable de la collecte : l'efficacité de l'utilisation de ces renseignements pour atteindre les objectifs, le caractère raisonnable de la collecte de cette information par rapport à une autre solution, et de la proportionnalité de l'atteinte à la vie privée par rapport aux coûts et aux avantages pour l'organisation³²⁶. Le Commissariat à la protection de la vie privée du Canada a tenté de clarifier cette norme en donnant des exemples de fins qu'il considère comme déraisonnables. Il indique notamment que la collecte, l'utilisation ou la communication seraient interdites si cela est fait dans un objectif qui autrement est illégal, s'il mène à un profilage ou une catégorisation donnant lieu à un traitement injuste, contraire à l'éthique ou discriminatoire, s'il cause ou est susceptible de causer un préjudice probable et grave, et s'il s'agit d'une surveillance exercée par une organisation au moyen des fonctions audio ou vidéo de l'appareil de l'individu lui-même³²⁷.

³²⁵ BARBARA VON TIGERSTROM, préc., note 279, p. 343-344.

³²⁶ *Turner c. Telus Communications Inc.*, 2005 CF 1601, par. 48.

³²⁷ Le CPVP donne d'autres exemples aussi. COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE DU CANADA, « Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3) » (24 mai 2018), en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gd_53_201805/> (consulté le 21 novembre 2024). Plus récemment, le CPVP a trouvé d'autres fins inacceptables dans des décisions contre Clearview AI et Tim Hortons. Dans la décision contre Clearview AI, le CPVP constat que « la collecte d'images et la création de dispositifs de reconnaissance faciale biométriques par Clearview, dans le but avoué de fournir un service au personnel des organismes d'application de la loi, et leur utilisation par d'autres personnes au moyen des comptes d'essai, représentent l'identification et la surveillance de masse de personnes par une entité privée dans le cadre d'une activité commerciale » et ne constitue pas une fin acceptable : COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE DU CANADA, « Conclusions en vertu de la LPRPDE no 2021-001 : Enquête conjointe sur Clearview AI, Inc. par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta » (3 février 2021), par. 72-73, en ligne : <<https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2021/lprpde-2021-001/#toc6-3>> (consulté le 26 mars 2025). Le dossier contre Tim Hortons concerne la collecte des données détaillées de localisation des utilisateurs de son application mobile et leur analyse pour déduire leur domicile, leur lieu de travail, savoir si le consommateur retournait chez lui, visitait un des concurrents de l'entreprise, etc. Le CPVP a conclu que « Tim Hortons n'avait pas un besoin légitime de recueillir de grandes quantités de renseignements de nature sensible concernant l'emplacement et l'entreprise n'a jamais utilisé les renseignements aux fins prévues; ii) l'incidence sur la vie privée associée à la collecte de renseignements personnels par l'application représente une atteinte à la vie privée qui n'est pas proportionnelle aux avantages que Tim Hortons aurait pu tirer d'une publicité ciblée optimisée pour mieux promouvoir son café et ses produits connexes » : COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE DU CANADA, « Conclusions en vertu de la LPRPDE no 2022-001 : Enquête conjointe sur le suivi de localisation par l'application de Tim

Ensuite, la loi exige que, lorsque l'organisation a établi l'objectif de la collecte de données, elle s'assure que la collecte (ou autre) est raisonnable ou nécessaire pour atteindre cet objectif. Cette exigence est également contextuelle. Pour référence, la CAI du Québec stipule que la collecte d'informations n'est pas « nécessaire » sauf si l'atteinte à la vie privée est proportionnelle à l'objectif, si la collecte des renseignements est rationnellement liée aux objectifs, si l'atteinte au droit à la vie privée est minimisée et si la collecte (ou autre) des données est « plus utile à l'entreprise que préjudiciable à la personne concernée³²⁸ ». Cette interprétation de la notion de nécessité correspond de manière significative à l'interprétation du caractère raisonnable qu'en a fait la Cour fédérale dans l'affaire *Turner*.

Ces critères démontrent que cette législation vise à établir un équilibre entre le droit des personnes à la vie privée et les intérêts des entreprises. La protection des droits des consommateurs ne l'emporte pas intrinsèquement sur les intérêts des entreprises et, ainsi, les critères contextuels comme la raisonnable ou la nécessité de la collecte sont interprétés de manière à trouver l'équilibre entre la protection de ces droits et les intérêts commerciaux³²⁹. Toutefois, une décision récente de la Cour d'appel fédérale a souligné que l'organisation n'a pas de droit inhérent aux données et que l'équilibre doit être trouvé entre les besoins d'une entreprise et les droits du consommateur. La distinction entre les concepts de droit (conférés seulement aux consommateurs) et des besoins constitue un « fondement conceptuel important³³⁰ ».

En appliquant ces règles au contexte de la voiture connectée, nous pouvons voir les limites de ces protections législatives. Nous avons vu que les fabricants ont tendance à utiliser des termes généraux et vagues pour décrire les objectifs de leur collecte de données. Les politiques de protection de la vie privée font référence à des fins telles que les « objectifs commerciaux légitimes », la « recherche et le développement » ou le « marketing ». Ces objectifs ne semblent pas déraisonnables ou illégitimes en soi, mais les notions sont tellement larges qu'il est impossible de trancher. Si la collecte de données audio ou vidéo à des fins de surveillance était déraisonnable selon les lignes directrices du CPVP, il n'est pas certain que la collecte de données de géolocalisation ou d'informations sur le véhicule à des fins de sécurité ou de recherche le soit. Dans l'exemple de la fuite de données de Volkswagen citée précédemment, le fabricant a déclaré que l'utilisation de données de géolocalisation dites anonymisées (et pourtant réidentifiées) avait pour but d'améliorer l'optimisation de la batterie et de son logiciel³³¹. Est-ce une collecte ou une utilisation déraisonnable ou illégitime ?

Hortons » (1 juin 2022), par. 36, en ligne : <<https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2022/lrpde-2022-001/>> (consulté le 26 mars 2025).

³²⁸ COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, « Collecte de renseignements personnels », en ligne : <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privées/collecte-renseignements-personnels_entreprises> (consulté le 21 novembre 2024).

³²⁹ T. SCASSA et A. SATTler, préc., note 147, 122.

³³⁰ *Canada (Commissaire à la protection de la vie privée) c. Facebook, Inc.*, 2024 CAF 140, par. 121.

³³¹ P. B. FLÜPKE, M. HOPPENSTEDT, M. KREIL, M. ROSENBAH et R. WILKIN, préc., note 106.

Bien que nous considérions les limites prévues dans ces lois comme importantes, le fait qu'elles doivent être interprétées de manière contextuelle les rend difficiles à appliquer, sauf dans les cas les plus flagrants. Étant donné qu'il existe peu de limites strictes, c'est l'entreprise qui collecte les données qui décide si la pratique est raisonnable ou non. Un tribunal ou un organisme qui veille à l'application de la loi peut contester cette décision après coup et la juger déraisonnable, mais ce n'est qu'après que la collecte, l'utilisation et parfois la divulgation des données aient déjà eu lieu. À ce stade, le mal que tentait d'éviter la loi est fait.

Enfin, ces règles nous semblent inadéquates pour mitiger les risques liés à l'agrégation des données par des entreprises tierces. Comme nous l'avons vu, les fabricants affirment qu'ils partagent les données des utilisateurs avec des partenaires et des tiers, parfois à des fins commerciales. Reprenons l'exemple décrit à la section 2, où GM a partagé des données de conduite avec LexisNexis Risk Solutions et à d'autres courtiers en données. LexisNexis Risk Solutions se décrit comme une société qui offre des « technologies sophistiquées d'analyse et de liaison de données » pour mieux prendre des décisions, gérer des risques et renforcer la sécurité et l'efficacité de l'entreprise³³². Ensuite, cette entreprise a partagé ces renseignements personnels avec d'autres tiers, comme les assureurs. Toutes les entreprises de cette chaîne peuvent affirmer que leur collecte, etc., des données étaient raisonnables ou légitimes considérant leur modèle d'affaires. Bien que nous puissions contester cette affirmation, il n'a pas été établi en droit que ce type d'activité est intrinsèquement déraisonnable et qu'il n'est donc pas autorisé par la loi canadienne sur la protection de la vie privée.

En ce sens, les limites à la collecte (ou autre) de données semblent inadéquates au contexte de la voiture connectée et insuffisante pour faire face aux risques encourus par les consommateurs. Les limites imposées par la loi sont difficilement applicables sauf dans les cas les plus flagrants et, dans tous les cas, seulement applicables après que la collecte (ou autre) de données ait eu lieu.

5.2.2 Manque de clarté sur la dépersonnalisation et l'anonymisation

L'absence d'encadrement des concepts de dépersonnalisation et d'anonymisation dans les instruments juridiques examinés (sauf au Québec) laisse place à l'ambiguïté dans le contexte de la voiture connectée. Cette ambiguïté permet malheureusement aux entreprises de plaider que certaines pratiques douteuses sont permises vu que les données ont été dépersonnalisées ou anonymisées.

Le Québec est la seule législation canadienne où la loi dit explicitement que les données qui peuvent permettre indirectement, et non seulement directement, d'identifier une personne sont des renseignements personnels. La loi québécoise est également la seule à définir et encadrer l'anonymisation (bien que le projet de loi fédéral contienne des concepts similaires). Les autres lois restent vagues sur ce point, ce qui laisse la porte ouverte aux fabricants d'automobiles de prétendre que les données qu'ils utilisent sont

³³² LEXISNEXIS RISK SOLUTIONS, « LexisNexis Risk Solutions », en ligne : <https://risk.lexisnexis.com/global/fr> (consulté le 26 mars 2025).

dépersonnalisées ou anonymes et qu'elles ne sont donc pas assujetties à la politique de confidentialité ou à la législation relative à la protection de la vie privée³³³.

Nous pouvons observer l'effet de cette pratique dans l'affaire Volkswagen évoquée précédemment (bien que ce cas se soit déroulé à l'extérieur du Canada). Dans cette affaire, la filiale de Volkswagen a prétendu qu'une base de données de géolocalisation était anonymisée. Cependant, les chercheurs ont démontré ce qui est déjà établi dans la littérature : les données de géolocalisation peuvent souvent être réidentifiées et ne sont presque jamais vraiment anonymes. Tant que les concepts de renseignements personnels, l'anonymisation et la dépersonnalisation ne seront pas des concepts clairement définis dans les autres lois canadiennes, les fabricants continueront à prétendre que certaines données ne sont pas des renseignements personnels, ou qu'elles sont anonymes et ne sont donc pas assujetties aux protections juridiques prévues dans ces lois, même quand ces données sont facilement ré-identifiables (voir la section 6 du rapport pour des exemples courants).

Sur ce point, on peut également se demander si les fabricants respectent la législation québécoise en matière d'anonymisation qui, rappelons-le, ne peut se faire que pour l'utilisation des renseignements à des fins sérieuses et légitimes et en conformité avec les meilleures pratiques et la réglementation en vigueur.

5.2.3 Les règles sur le consentement sont insuffisantes pour ce contexte

Tout d'abord, il convient de se demander si certaines des règles énoncées dans la législation et concernant le consentement sont respectées.

Comme nous l'avons observé ci-haut, les politiques de confidentialité des fabricants sont souvent larges, ouvertes et imprécises. Comme le consommateur ne peut généralement pas saisir les pratiques de la collecte, l'utilisation et le partage énoncées dans de tels documents, nous considérons qu'il ne lui est pas possible d'y consentir non plus. Pourtant, les lois exigent que les objectifs de la collecte soient divulgués avec un certain degré de spécificité. Nous ne sommes pas certains que les objectifs énumérés, tels que le marketing ou la recherche et développement (R et D), soient suffisamment clairs pour répondre à ces exigences.

Une autre règle semble trop souvent ignorée par les fabricants de voitures connectées : toutes les lois canadiennes indiquent que le consentement ne peut être exigé pour des fins qui ne sont pas nécessaires à l'accès au bien ou au service. De plus, le consommateur a le droit de retirer son consentement en tout temps. Au Québec, l'organisme doit assurer que les paramètres concernant la collecte, etc., de données non nécessaires sont au

³³³ Rajen AKALU, *Un code de pratique en matière de protection de la vie privée pour les véhicules connectés*, Faculté des affaires et des technologies de l'information, Institut universitaire de technologie de l'Ontario, 2019, p. 3, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/financement-pour-les-projets-de-recherche-et-d-application-des-connaissances/projets-menes-a-bien-dans-le-cadre-du-programme-des-contributions/2018-2019/p_201819_09/>. Voir aussi BARBARA VON TIGERSTROM, préc., note 279, p. 340.

niveau le plus respectueux de la vie privée par défaut. Toutefois, la littérature suggère que les fabricants automobiles n'offrent pas nécessairement la possibilité et l'occasion de refuser la collecte (ou autre) de données non nécessaires sans renonciation à l'accès au service en question, ou même à tous les services connectés.

Enfin, il faut observer que lorsque des renseignements personnels sont collectés au sujet de personnes qui n'ont jamais eu l'occasion de donner leur consentement, comme les passagers et les piétons qui interagiront avec la voiture connectée, le consentement de ces personnes ne peut pas même être considéré comme implicite. Ces personnes n'ont pas la possibilité de refuser la collecte (ou autre) de leurs données personnelles³³⁴. Si les fabricants collectent effectivement des renseignements personnels sur ces personnes, que ce soit directement ou indirectement, intentionnellement ou non, il s'agit vraisemblablement d'une violation de la loi.

Pourtant, même si la loi était strictement observée par les fabricants, les exigences en matière de consentement dans ces instruments juridiques nous semblent insuffisantes pour protéger adéquatement les consommateurs dans le contexte des voitures connectées. En premier lieu, les protections offertes par le consentement sont considérablement érodées par le fait que le consentement implicite est considéré comme acceptable dans la plupart des cas, et qu'aucun consentement n'est requis dans plusieurs autres. Les plus vieilles législations (APIPA, BCPIPA, LPRPDE) permettent aux organisations de considérer qu'il y a un consentement implicite lorsqu'il serait raisonnable ou approprié de le faire, ou lorsque la personne fournit des données à l'organisation et que l'utilisation en question peut être raisonnablement déduite. La nouvelle loi québécoise et la législation fédérale proposée sont particulièrement claires sur le fait qu'aucun consentement explicite n'est requis dans la plupart des cas. La législation québécoise n'exige un consentement explicite que lors de la collecte, etc., de données sensibles. Le consentement n'est pas du tout requis pour les utilisations secondaires des données de la personne qui ont déjà été collectées si les fins de l'utilisation sont compatibles avec celles pour lesquelles elles ont été collectées. La LPVPC proposée contient de nombreux articles qui indiquent les cas dans lesquels le consentement n'est pas requis, par exemple, si la collecte (ou autre) est faite en vue d'une des activités d'affaires nommées dans la Loi, si elle est faite pour des raisons d'intérêt public, pour les fins d'une enquête, etc.³³⁵. La liste est longue et la portée de certaines des dispositions, comme celle sur les activités d'affaires, est large. Dans ces cas, le projet de loi indique que l'organisation peut même collecter et utiliser des données à l'insu de la personne concernée.

En appliquant ces règles au contexte de la voiture connectée, nous constatons que de nombreuses pratiques douteuses identifiées dans la section 3 sont autorisées par le cadre législatif actuel. Selon la législation, le fabricant n'a pas besoin d'obtenir un consentement explicite pour collecter, par exemple, les données de géolocalisation du consommateur,

³³⁴ La seule disposition qui pourrait éventuellement traiter ce type de collecte de données serait l'article 18 de la LPVPC dans le projet de loi C-27. Cet article autorise les organisations à collecter des données à l'insu de la personne ou sans son consentement si la collecte ou l'utilisation est faite en vue d'une activité d'affaires, comme une activité nécessaire pour assurer la sécurité d'un produit ou d'un service fourni par l'entreprise.

³³⁵ LPVPC, arts. 18 à 52.

les données du véhicule et les informations de diagnostic³³⁶, si le consommateur fournit ces données, tant que cela semble raisonnable ou approprié, et si le fabricant a divulgué l'information relative à la collecte. La pratique est encore plus légitimée selon les lois applicables si le consommateur signe un consentement à un moment donné de la transaction, ou s'il clique sur « oui » sur l'écran du véhicule lorsqu'un pop-up lui demande l'autorisation de collecter ses données. Dans ce cas, le fabricant peut affirmer que le consentement était explicite. Il est important de noter que toutes les législations sur la protection de la vie privée examinées exigent seulement que l'organisation informe la personne de la collecte de données au moment de la collecte ou après ; dans le cas d'un véhicule, la collecte ne peut commencer qu'après l'acquisition du véhicule par le consommateur. À ce stade, le consommateur ne peut retirer son consentement sans perdre l'accès au bien acheté (ou à certaines de ses fonctionnalités).

Les données peuvent alors être utilisées, transmises et communiquées pour toutes les fins légitimes identifiées dans la politique de protection de la vie privée, ou pour toute autre fin conforme aux raisons pour lesquelles elles ont été collectées³³⁷.

La vie privée du consommateur est-elle protégée de manière significative par les règles élaborées sur la base de la notion de consentement ? Compte tenu de nos constats dans les sections 3 et 4 sur le manque de clarté des pratiques des fabricants, le fait que les consommateurs ne lisent que rarement les politiques de confidentialité et qu'ils ne les comprennent pas lorsqu'ils les lisent, et le fait qu'ils ne savent même pas si on leur a demandé leur consentement dans de nombreux cas, la réponse à cette question doit être « non »³³⁸.

Enfin, nous devons constater à quel point le modèle de consentement semble difficilement applicable à un contexte où plusieurs acteurs collectent et utilisent les données. Comme décrit ci-dessus, plusieurs acteurs ont accès aux données collectées par les voitures connectées : les fournisseurs de services (télécommunications, applications mobiles, etc.) ainsi que les partenaires ou sociétés affiliés des fabricants, y compris des agrégateurs et des courtiers. Même si la collecte, l'utilisation et le partage d'informations personnelles requièrent théoriquement le consentement de la personne concernée, nous constatons que le consommateur n'a pas de réelle possibilité de donner ou de refuser ce consentement, en dehors du consentement initial donné au fabricant. Plusieurs tierces semblent s'appuyer sur le consentement obtenu par le collecteur de données initial (c'est-à-dire le fabricant) ou sur un consentement entièrement implicite (voire imaginaire) plutôt que de chercher à obtenir un nouveau consentement avant d'utiliser ou de partager les données. Cette pratique nous semble juridiquement douteuse : même si une personne consent à ce que ses données soient partagées avec une autre personne, cela ne constitue certainement pas un consentement à l'utilisation ou le partage de ces données

³³⁶ Sauf au Québec, si ces données sont considérées comme sensibles.

³³⁷ Au Québec, il faut obtenir ou déduire le consentement (potentiellement implicite) pour la communication.

³³⁸ Rémi SLAMA, *Les véhicules autonomes et connectés à l'aune du droit des technologies de l'information au Québec*, Maîtrise en droit, Faculté de droit de l'Université de Montréal, 2023 analyse l'application des lois québécoise et fédérale aux voitures connectées et identifie également des lacunes en ce qui concerne le consentement et le partage de données avec des tiers.

par les tiers³³⁹. Néanmoins, la loi pourrait être plus claire sur ce point en interdisant ce type de « consentement » indirect ou en stipulant que certaines utilisations de données par des tiers, comme les courtiers en données, sont « déraisonnables » ou « illégitimes ».

Tous ces facteurs nous amènent à nous demander si l'obligation d'obtenir le consentement est une mesure de protection adaptée pour ce contexte. Le Commissariat à la protection de la vie privée du Canada a déclaré dans son évaluation 2016-2017 du modèle de consentement que, bien que le consentement soit toujours un principe important, il existe des situations potentiellement spécifiques où le consentement « peut être tout simplement impraticable » :

Il peut être pratiquement impossible (ou du moins très difficile) d'obtenir un consentement valable dans le cas d'initiatives de mégadonnées ou d'appareils de l'Internet des objets que les gens n'ont d'autre choix que d'utiliser. Il se pourrait que certains modes de fonctionnement de la technologie empêchent de comprendre comment les renseignements personnels sont traités ou quelles peuvent être les conséquences, ce qui affaiblit la pertinence et la validité du consentement éclairé³⁴⁰.

Nous partageons l'avis de BC FIPA que le contexte des voitures connectées est une des situations dans lesquelles il devient impossible d'obtenir un consentement valable :

There are too many players in the Connected Car ecosystem. Many of these players have their own terms of service and privacy policies that consumers are expected to read, understand and agree to (or else seek an alternative with a more acceptable policy). Meaningful consent in this context is virtually impossible. Even if OEMs competed on privacy and provided more privacy options in their terms of service, average consumers simply do not have the time, never mind the expertise, to review and take into account so many different terms of service and privacy policies³⁴¹.

En d'autres termes, même si les politiques de confidentialités étaient claires et partagées avec les consommateurs avant l'achat du bien, même si le consentement exprès a été requis en toute situation et même s'il n'y avait pas d'exception au principe de consentement, le principe de consentement resterait insuffisant pour protéger les droits à la vie privée des consommateurs dans ce contexte. Le simple consentement est

³³⁹ SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC, *Back on the Data Trail: The Evolution of Canada's Broker Industry (Draft Report)*, 2018, p. 35 semble partager notre avis.

³⁴⁰ COMMISSARIAT A LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Rapport annuel au Parlement 2016-2017 concernant la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur la protection des renseignements personnels » (21 septembre 2017), en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/201617/ar_201617/#heading-0-0-3-1> (consulté le 21 novembre 2024).

³⁴¹ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 21, p. 113-114; LE COMITÉ SENATORIAL PERMANENT DES TRANSPORTS ET DES COMMUNICATIONS, préc., note 66, p. 57-58; voir aussi Rajen AKALU, « Privacy, consent and vehicular ad hoc networks (VANETs) », (2018) 34-1 *Comput. Law Secur. Rev.* 37-46, DOI : 10.1016/j.clsr.2017.06.006.

insuffisant ici en raison de la complexité de la technologie, du nombre d'acteurs et de pratiques, du fait que les consommateurs n'ont pas de véritable choix, et de l'expertise requise pour comprendre les enjeux en matière de vie privée dans ce contexte.

Cela ne veut pas dire que le consentement doit être abandonné en tant que principe, mais simplement qu'il s'agit d'une protection insuffisante dans ce contexte³⁴². Le contexte des voitures connectées pose de sérieux défis à l'égard du consentement. La technologie et les risques qu'elle pose pour la vie privée sont complexes ; nos résultats au sondage et les entrevues menées avec les consommateurs démontrent que ni la technologie ni les risques ne sont bien saisis. Les fabricants de voitures connectées échangent des données avec trop de tiers et collectent des données pour trop de raisons. Une compréhension de ces pratiques et un consentement valable sont impossibles dans de tels cas.

Un auteur a observé que, pour des raisons similaires, les gouvernements ne s'appuient pas sur le consentement des consommateurs lorsqu'il s'agit de réglementer d'autres éléments des automobiles, comme la sécurité :

Governments recognize that consumers have neither the time nor resources to compare different car safety features when making a purchasing decision. This being the case, the government establishes detailed regulations in order to ensure that minimum safety standards are being maintained [...]

By contrast, decisions regarding the sharing of data by consumers are not prescribed in the same manner. As a general rule, in data protection law it is the individual that exercises control over their personal information³⁴³.

³⁴² Certains affirment que, dans certains contextes, le consentement individuel n'est plus du tout pertinent et qu'il devrait être remplacé par un autre mécanisme. Ce n'est pas l'argument que nous avançons ici. Pour ne citer que quelques exemples, le CPVP a fait valoir qu'un modèle serait de permettre, dans certains cas, les organisations de renoncer au consentement si la collecte était nécessaire, si des données pseudonymisées étaient utilisées dans la mesure du possible, si les avantages pour la société l'emportaient clairement sur les atteintes à la vie privée et si le CPVP était informé à l'avance de cette collecte : COMMISSARIAT A LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 340. Un autre modèle est celui du « consentement collectif », dans lequel un représentant de l'ensemble des personnes concernées par la collecte (ou autre) de données négocie les limites de celle-ci et les conditions du consentement : voir L. A. BYGRAVE et D. W. SCHATUM, préc., note 147. Dans le cas des voitures connectées, le nombre de parties concernées est vaste : utilisateurs du véhicule, passagers, piétons, passants, etc. L'organisme qui représente le mieux ce groupe massif de personnes serait sans doute l'État. Mark BURDON, *Digital data collection and information privacy law*, coll. Cambridge intellectual property and information law, n°54, Cambridge, Cambridge University Press, 2020 plaide que l'ensemble du modèle traditionnel de protection de la vie privée, basé sur le contrôle individuel et le consentement au partage des données, s'effondre lorsque des quantités massives de données sont non seulement collectées par des objets intelligents dotés de capteurs à tout moment, mais sont échangées, partagées et vendues par les entreprises. Dans un tel contexte, un modèle différent, qui tient compte des différentes structures de pouvoir entre les parties et de l'impossibilité du consentement, serait plus approprié.

³⁴³ R. AKALU, préc., note 341.

En effet, le législateur a imposé des limites et des obligations aux fabricants en ce qui concerne les dispositifs de sécurité, les émissions, la pollution, les caméras de recul, les enregistreurs de données d'événements, etc. Le gouvernement impose ces exigences aux fabricants automobiles plutôt que de confier au consommateur la responsabilité de choisir le produit le plus sûr et le plus performant. Il est logique que cette approche soit étendue à la collecte, à l'utilisation et au partage des données³⁴⁴. L'auteur propose ainsi la création de normes et propose même un code de conduite pour l'écosystème des voitures connectées, qui s'appliquerait non seulement aux fabricants, mais aussi à d'autres acteurs tels que les concessionnaires et les agences de location. Le code énonce des obligations visant à limiter la collecte de données et à fournir plus de transparence aux consommateurs lorsqu'on leur demande leur consentement³⁴⁵.

BC FIPA observe similairement que :

The most effective way to protect data is to not collect or retain it in the first place. This should be the starting point for data protection standards in the automobile industry: hard limits on purposes for which personal data may be collected and the collection of data, by type of data and approved purpose³⁴⁶.

Ainsi, l'organisme propose d'établir des règles de protection des données pour l'industrie des voitures connectées, d'impliquer des experts en protection de la vie privée dans la phase de conception et de recherche des systèmes de transport intelligents, y compris les véhicules connectés, et d'adopter des principes de protection de la vie privée dès la conception et des outils connexes³⁴⁷. La vie privée dès la conception (*privacy by design*) est un concept qui fait référence à la prise en compte de la vie privée dans la conception même d'un système. Cette approche nous semble fort pertinente dans le contexte des voitures connectées et il convient d'énumérer les sept principes sur lesquels elle repose :

- 1) « Principe proactif et non réactif; prévention plutôt que correction » : l'objectif de la protection de la vie privée dès la conception est d'agir de manière préventive en prenant des mesures visant à réduire le risque d'atteinte à la sécurité de renseignements personnels.
- 2) « Le respect de la vie privée comme paramètre par défaut » : les réglages par défaut de tout produit et services devraient favoriser la protection des renseignements personnels, de sorte que, sans intervention consciente de la part de l'utilisateur, sa vie privée sera protégée.
- 3) « Intégration du respect de la vie privée au niveau de la conception » : la protection des renseignements personnels doit être intégrée aux systèmes informatiques et aux pratiques d'affaires plutôt qu'un simple ajout périphérique
- 4) « Pleine fonctionnalité – somme positive au lieu de somme nulle » : la protection de la vie privée dès la conception devrait être considérée comme une plus-value;

³⁴⁴ *Id.*; BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 21, p. 113-114.

³⁴⁵ R. AKALU, préc., note 333.

³⁴⁶ BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION, préc., note 21, p. 114.

³⁴⁷ *Id.*

- il ne devrait pas être nécessaire de nuire à la mise en œuvre d'autres fonctionnalités afin de réaliser cet objectif.*
- 5) « *Sécurité de bout en bout – une protection complète pour le cycle de vie* » : La protection des renseignements personnels doit être intégrée à l'ensemble du cycle de vie d'un système
 - 6) « *Visibilité et transparence – assurer l'ouverture* » : la transparence est importante afin de s'assurer que les systèmes et pratiques en place sont réellement en mesure de protéger la vie privée des utilisateurs ; il doit toujours être possible de procéder à une vérification indépendante.
 - 7) *Respect de la vie privée de l'utilisateur – maintenir une démarche centrée sur l'utilisateur* » : Avant tout, la protection de la vie privée dès la conception doit prioriser les intérêts individuels³⁴⁸.

Il est clair que nous sommes loin du compte dans le contexte des voitures connectées, où nous avons observé que la collecte et le partage massifs de données sont la règle. Dans la mesure où des protections de la vie privée sont mises en place, elles semblent être une réflexion après coup. Il nous semble que la mise en œuvre de ces sept principes changerait radicalement la façon dont l'industrie fonctionne actuellement.

5.3 Le droit de propriété et le droit à la réparation dans le contexte numérique

Comme décrit ci-dessus, l'un des principaux risques posés aux consommateurs par les voitures connectées est l'érosion de leurs droits de propriété sur leurs véhicules, en raison de la capacité du fabricant d'exercer une surveillance et un contrôle de la voiture à distance.

La présente section examine le cadre juridique canadien relatif à ces enjeux et son adéquation pour répondre aux risques et préoccupations identifiées. Dans un premier temps, nous verrons que le droit de propriété au Canada permet de distinguer la propriété d'un bien physique et la propriété intellectuelle. Dans le cas des voitures connectées, les consommateurs achètent la voiture, mais les fabricants conservent les droits de propriété et le contrôle sur leurs logiciels, par le biais des contrats de licence et de mesures techniques de protection (MTP). Dans un deuxième temps, nous examinerons la *Loi sur le droit d'auteur* qui permet et soutient ces pratiques. Ce cadre législatif touche à la question du droit à la réparation, que nous examinerons plus en détail dans les sections suivantes.

³⁴⁸ Ce résumé provient de RAPPORT DU COMITE PERMANENT DE L'ACCES A L'INFORMATION, DES RENSEIGNEMENTS PERSONNELS ET DE L'ETHIQUE, *Vers la protection de la vie privée dès la conception : examen de la Loi sur la protection des renseignements personnels et les documents électroniques*, 42e législature, première session, 2018, p. 57-58 qui cite; Ann CAVOUKIAN, *Privacy by Design : The 7 Foundational Principles*, Information & Privacy Commissioner, Ontario, Canada.

5.5.2 5.3.1 Un droit divisé

Au Canada, les droits de propriété relèvent de la compétence exclusive des provinces³⁴⁹. Les notions fondamentales de propriété sont définies différemment en droit civil, applicable au Québec, et en *common law* qui s'applique dans les autres provinces canadiennes.

La notion juridique du droit de propriété en droit civil est définie dans le Code civil du Québec : « La propriété est le droit d'user, de jouir et de disposer librement et complètement d'un bien, sous réserve des limites et des conditions fixées par la loi³⁵⁰ ». Dans cette optique, le consommateur peut légitimement s'attendre à posséder ces droits sur le bien dont il acquiert la propriété, soit l'automobile connectée.

Pourtant, la définition de ce qui constitue un bien est plus complexe et le droit accorde une place particulière aux biens immatériels.

Le droit civil québécois distingue les biens corporels des biens incorporels :

Les biens corporels existent matériellement. Ces biens sont généralement perceptibles par les sens. Ainsi peut-on toucher et sentir la matière qui constitue les objets qui nous entourent (une maison, une automobile, un livre, etc.)³⁵¹.

En revanche, les biens incorporels sont des « choses sans corps et intangibles³⁵² », une catégorie vaste et disparate qui comprend notamment les biens sujets aux droits d'auteur, qui donnent à son titulaire des droits de nature patrimoniale et des droits moraux³⁵³. Dans le cas des voitures connectées, les biens incorporels qui nous intéressent sont les « œuvres littéraires », catégorie d'œuvres dont font partie les programmes d'ordinateur ou logiciels. Dans leurs accords de licence, les fabricants de voitures connectées affirment qu'ils ne vendent pas le logiciel de leurs véhicules, mais qu'ils permettent simplement au propriétaire ou locataire de la voiture de l'utiliser. Ainsi, un consommateur qui acquiert une voiture connectée peut être propriétaire d'un bien corporel – la voiture – et avoir le droit d'utiliser, de jouir et de disposer librement de la composante physique du bien, mais il n'a qu'une licence d'utilisation de la composante immatérielle, c'est-à-dire, du logiciel, et ce, sous de nombreuses conditions.

Quant à la *common law*, ce système envisage la propriété selon les relations s'opérant entre les personnes et les choses. La doctrine et la jurisprudence réfèrent aux ensembles des droits (*bundles of rights*) plutôt qu'un seul droit de propriété. Un propriétaire a un ensemble de droits envers les biens et envers d'autres personnes détenant d'autres droits (complémentaires ou concurrents) sur ces mêmes biens³⁵⁴. Ces droits comprennent notamment la possession, le contrôle, l'exclusion, la jouissance et la disposition du bien.

³⁴⁹ *Loi constitutionnelle de 1867*, 30 & 31 Victoria, c 3, art. 92(13).

³⁵⁰ *Code civil du Québec*, RLRQ, c. CCQ-1991, art. 947.

³⁵¹ Sylvio NORMAND, *Introduction au droit des biens*, 3e éd., Wilson & Lafleur, 2020, p. 60.

³⁵² Gaële GIDROL-MISTRAL, « Les biens immatériels en quête d'identité », (2016) 46 *Rev. Droit Univ. Sherbrooke*, 69-70.

³⁵³ S. NORMAND, préc., note 351, p. 64-65.

³⁵⁴ Mary Jane MOSSMAN et Philip GIRARD, *Property law: cases and commentary*, Third edition, Toronto, Canada, Emond Montgomery Publications, 2014, p. 2-3.

Il est possible qu'une personne ait certains de ces droits et qu'une autre en ait d'autres. La plupart des législations de *common law* ont des lois particulières relatives à la propriété, qui peuvent nuancer les principes généraux énoncés précédemment³⁵⁵.

La *common law* divise conceptuellement les types de propriété selon plusieurs aspects. Dans un premier temps, la notion de *real property* concerne les droits sur les biens immeubles ; à l'opposé, la *personal property* concerne les biens meubles comme des voitures. Tout comme en droit civil, la *common law* distingue les biens tangibles, c'est-à-dire les biens matériels, et les biens intangibles ou immatériels, comme la propriété intellectuelle.

Aux fins des présentes, nous pourrions qualifier le consommateur qui possède une voiture connectée selon sa relation directe (propriétaire, locataire) au bien personnel et tangible. Selon son statut, il pourra disposer de certains droits envers ce bien, par exemple, des droits de possession, de contrôle, de jouissance et de disposition. Toutefois, les fabricants n'étendent pas les droits liés au bien tangible aux biens intangibles, c'est-à-dire les logiciels. De cette manière, le fabricant garde un contrôle sur le logiciel de la voiture, qui n'est pas vendu ou loué avec la voiture, mais dont une licence d'utilisation est accordée au consommateur sous certaines conditions. Les logiciels font donc l'objet de droits distincts énoncés dans un contrat de licence ou dans la *Loi sur le droit d'auteur*.

Ainsi, les deux systèmes juridiques canadiens prévoient la division de la propriété d'un bien de la propriété de son logiciel. Cette division permet au fabricant de garder un contrôle important sur le bien après son acquisition par le consommateur. Même si le fabricant ne conserve que les droits sur le logiciel, l'exercice de ses droits affecte les droits du consommateur liés au bien acquis.

Examinons maintenant les règles relatives aux logiciels et aux droits de propriété immatérielle.

5.3.2 Propriété intellectuelle et *Loi sur le droit d'auteur*

La *Loi sur le droit d'auteur* (LDA, ou la Loi dans cette section du rapport) est le principal texte législatif au Canada qui énonce les droits de propriété sur les biens numériques. La section la plus pertinente de cette loi pour les fins de ce rapport concerne les verrous numériques, également connus sous le nom de mesures techniques de protection, ou MTP.

La LDA est une loi canadienne fédérale³⁵⁶, adoptée en 1921 et révisée à plusieurs reprises depuis les années 1980, qui vise à « protéger et récompenser les efforts intellectuels des

³⁵⁵ Bruce MACDOUGALL, *Halsbury's laws of Canada*, First edition, Markham, Ontario, LexisNexis, 2006, ch. 1.

³⁵⁶ La Constitution canadienne alloue le pouvoir législatif sur les droits d'auteur au Parlement fédéral : *Loi constitutionnelle de 1867*, 30 & 31 Victoria, c 3, art. 91 (23).

auteurs, pendant un certain temps³⁵⁷ ». La Loi énonce les droits de propriété de l'auteur ou du détenteur du droit d'auteur sur une œuvre, par exemple, ses droits exclusifs de produire ou reproduire l'œuvre, de contrôler sa distribution, sa reproduction et son utilisation par des tiers, et ainsi de suite. Les droits prévus dans la *LDA* permettent au titulaire du droit d'auteur de bénéficier financièrement de l'œuvre et encouragent ainsi, en théorie, l'innovation et la création. Toutefois, la jurisprudence indique que ces droits doivent être équilibrés avec les droits du public à jouir des œuvres et à utiliser leur copie de l'œuvre³⁵⁸.

Le logiciel, comme ce qui se trouve dans une voiture connectée, est protégé par la Loi, car un programme d'ordinateur est considéré comme une œuvre littéraire dans la *LDA*. Le titulaire du droit d'auteur d'un logiciel bénéficie ainsi des droits et protections prévus pour les œuvres dans cette loi³⁵⁹. Le détenteur des droits d'auteur sur un programme d'ordinateur contrôle donc sa publication, sa distribution, sa reproduction, etc.

En outre, la *LDA* permet aux titulaires de droits d'auteur de « concéder, par une licence, un intérêt quelconque dans ce droit³⁶⁰ ». Cependant, les contrats de licence sont plus restrictifs que permissifs ; tout en concédant le droit d'utilisation du logiciel au bien, la licence énonce souvent plusieurs limites restrictives, par exemple, en ce qui concerne le décodage du logiciel, sa revente, etc. Nous avons déjà abordé la question du droit d'auteur et des licences d'utilisation et de leur impact sur les consommateurs dans un rapport précédent et nous avons trouvé que les restrictions imposées par ces licences interdisent parfois aux utilisateurs d'accomplir des actes autrement autorisés par la *LDA*, comme la production d'une copie privée de sauvegarde de l'œuvre³⁶¹. En revanche, comme la *LDA* n'est pas une loi d'ordre public, le titulaire de droit d'auteur peut restreindre les actes autrement autorisés par cette loi dans un contrat de licence³⁶².

Les verrous numériques sont spécifiquement permis et protégés par la *LDA*. Dans les années 1990, le *Traité de l'OMPI sur le droit d'auteur* et le *Traité de l'OMPI sur les interprétations et exécutions et les phonogrammes* (« les Traités ») ont étendu la protection du droit d'auteur pour protéger les mesures techniques de protection (MTP). Ces traités invitent les États signataires à adopter une protection juridique « contre la neutralisation des mesures techniques efficaces qui sont mises en œuvre par les auteurs

³⁵⁷ *Télé-Direct (Publications) Inc. c. American Business Information, Inc. (C.A.)*, 1997 CanLII 6378 (CAF), [1998] 2 CF 22. Les objectifs de la *Loi sur le droit d'auteur* ne sont pas explicitement déclarés dans son texte et doivent être déduits des décisions judiciaires et des débats parlementaires.

Ysolde GENDREAU, « La civilisation du droit d'auteur au Canada », (2000) 52-1 *Rev. Int. Droit Comparé* 101-123, 112-114, DOI : 10.3406/ridc.2000.18139.

³⁵⁸ *Université York c. Canadian Copyright Licensing Agency (Access Copyright)*, 2021 CSC 32 (CanLII), [2021] 2 RCS 734, pars. 91-92. *Théberge c. Galerie d'Art du Petit Champlain inc.*, 2002 CSC 34 (CanLII), [2002] 2 RCS 336, pars. 30-31.

³⁵⁹ *Loi sur le droit d'auteur*, LRC 1985, c. C-42, art. 2 : Définition de « œuvre littéraire » et « programme d'ordinateur ».

³⁶⁰ *Loi sur le droit d'auteur*, LRC 1985, c. C-42, art. 13(4).

³⁶¹ UNION DES CONSOMMATEURS, préc., note 182, p. 59-64.

³⁶² *Id.*, p. 39-54. Nous avons plaidé que plusieurs de ces types de clauses vont à l'encontre des lois de protection des consommateurs, qui sont d'ordre public.

dans le cadre de l'exercice de leurs droits [...] et qui restreignent l'accomplissement » des actes interdits en vertu des lois et instruments internationaux sur le droit d'auteur³⁶³.

Le Canada, étant signataire des Traités, a modifié la *LDA* afin de se conformer à ces règles en 2012³⁶⁴. Des modifications importantes ont été introduites dans la *LDA* pour protéger les MTP en interdisant leur contournement, comme l'exigeaient les Traités. Cependant, les dispositions adoptées dans la réforme canadienne de la *LDA* sont allées bien au-delà de ce qui était requis par les Traités. L'approche choisie ne fait pas l'unanimité sur la scène internationale³⁶⁵, mais elle est en grande partie inspirée par l'approche américaine adoptée dans le *Digital Millenium Copyright Act*³⁶⁶.

L'article 41 de la *LDA*, adopté en 2012, définit une MTP comme toute technologie ou tout dispositif ou composant qui contrôle efficacement l'accès à une œuvre **ou** qui restreint efficacement l'accomplissement d'un acte non autorisé en ce qui concerne une œuvre³⁶⁷. Cette définition de MTP adoptée dans la législation canadienne est nettement plus large que celle prévue par les Traités, qui visent à protéger seulement des mesures techniques qui restreignent l'accomplissement d'actes non autorisés et qui n'offre aucune protection explicite pour les mesures qui contrôlent l'**accès** à l'œuvre³⁶⁸. Comme nous l'avons signalé lors de la consultation parlementaire sur cette modification législative,

En établissant une protection juridique pour les mesures techniques de protection qui contrôlent l'accès aux œuvres, l'article 41 va au-delà de la simple protection

³⁶³ ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE (OMPI), *Traité de l'OMPI sur le droit d'auteur (TRT/WCT/001)*, art. 18 [TRT/WCT/001], en ligne :

<https://www.wipo.int/wipolex/en/text/295168#P95_12573> (consulté le 28 janvier 2025).

³⁶⁴ *Loi sur la modernisation du droit d'auteur*, L.C. 2012, ch. 20, sanctionnée en 2012. Le pays a ratifié les traités en 2014 : ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE (OMPI),

« Parties contractantes : Traité de l'OMPI sur le droit d'auteur », *WIPO Lex*, en ligne :

<https://www.wipo.int/wipolex/fr/treaties/ShowResults?search_what=C&treaty_id=16> (consulté le 28 janvier 2025).

³⁶⁵ Par exemple, la *Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information*, Journal officiel n° L 167 du 22/06/2001 p. 0010 – 0019 ne contient pas de protection pour les MTP qui contrôlent l'accès à l'œuvre. Voir aussi Anthony HEMOND, « Mémoire de l'Union des consommateurs sur le projet de loi C-11 », (2012) 24-1 *Cah. Propr. Intellect.*, en ligne : <<https://www.lescp.ca/s/825>>; Séverine DUSOLLIER, « Les mesures techniques dans la directive sur le droit d'auteur dans la société de l'information : un délicat compromis », (2001) 25-2 *LEGICOM* 75-86, DOI : 10.3917/legi.025.0075.

³⁶⁶ UNION DES CONSOMMATEURS, « Mémoire de l'Union des consommateurs sur le projet de loi C-11 », (2012) 24-1 *Cah. Propr. Intellect.*, 117-118, en ligne : <<https://www.lescp.ca/s/825>> (consulté le 10 octobre 2024).

³⁶⁷ La notion d'efficacité fait partie de la définition d'une MTP dans la *LDA*, mais n'est pas définie dans la Loi. Les législations européenne, britannique et américaine incluent une définition d'efficacité. Ces définitions sont larges, mais la notion d'efficacité peut avoir pour effet de restreindre les MTP dans une certaine mesure. Voir l'affaire *Nintendo of America Inc. c. King* (infra) pars. 71-90 pour une discussion sur la notion dans la législation du Royaume-Uni et sur comment cette notion aurait pu restreindre la définition d'une MTP dans ce dossier. Voir aussi A. HEMOND, préc., note 365, 118.

³⁶⁸ *TRT/WCT/001*, préc., note 363, art. 11.

des droits dont disposent les auteurs, en permettant aux auteurs et aux titulaires de droit de limiter, par le biais de mesures techniques, les droits que la Loi confère aux utilisateurs³⁶⁹.

Ainsi, « le résultat est d'accorder aux fabricants de technologies (par opposition aux simples détenteurs de droits) un nouveau droit de facto de déterminer la conduite des utilisateurs et des consommateurs³⁷⁰ ».

En effet, l'accès à l'œuvre n'est pas limité ou contrôlé ailleurs dans la Loi : « à aucun moment le droit de contrôler l'accès à l'œuvre n'est identifié comme étant un droit conféré à l'auteur » dans la LDA³⁷¹. Normalement, le consommateur qui achète un support physique d'une œuvre ou qui obtient une licence d'utilisation d'une œuvre a d'emblée un droit d'accès à cette œuvre. En effet, la Loi précise que certains actes, comme la production d'une copie de sauvegarde, ne constituent pas une violation du droit d'auteur. Cependant, les MTP, dont la Loi interdit le contournement, peuvent restreindre l'accès autrement légitime au bien ; cette restriction peut avoir comme effet d'empêcher les utilisateurs d'effectuer des actes autorisés, tels que la réalisation d'une copie privée :

*Par exemple, certaines mesures de protection empêchent la lecture de CD de musique sur des ordinateurs afin d'empêcher la copie de son contenu – alors que le droit d'accès conféré à l'utilisateur se doit, logiquement, d'inclure le droit de cet utilisateur d'accéder à l'œuvre à partir de tout appareil compatible*³⁷².

En plus d'interdire le contournement³⁷³ d'une MTP, la Loi interdit également toute offre au public de contournement d'une MTP et déclare que nul ne peut fabriquer, importer ou fournir une technologie, un dispositif ou un composant pour contourner une MTP³⁷⁴. En cas de non-respect de ces règles, la LDA donne au titulaire du droit d'auteur le droit de poursuivre la personne qui contourne une MTP³⁷⁵ et elle prévoit des recours pénaux contre ceux qui contournent une MTP sciemment et à des fins commerciales³⁷⁶.

Ce faisant, le Canada a essentiellement adopté « un régime de responsabilité parallèle au droit d'auteur, selon lequel le contournement des MTP serait illégal, et ce,

³⁶⁹ Nous soulignons. A. HEMOND, préc., note 365, 115.

³⁷⁰ Notre traduction. P. CHAPDELAINE et al., préc., note 196, p. 11.

³⁷¹ UNION DES CONSOMMATEURS, préc., note 366, 115.

³⁷² *Id.*, 120.

³⁷³ « Contourner » a deux définitions dans la Loi, selon l'objet de la MTP en question. Si la personne contourne une MTP qui contrôle l'accès à une œuvre, contourner est défini comme « éviter, supprimer désactiver ou entraver la mesure — notamment décoder ou déchiffrer l'œuvre protégée par la mesure — sans l'autorisation du titulaire du droit d'auteur ». Si la MTP protège plutôt l'œuvre des actes non autorisés dans la Loi, comme sa reproduction illégale, contourner veut dire « éviter, supprimer, désactiver ou entraver la mesure ». *Loi sur le droit d'auteur*, LRC 1985, c. C-42, art. 41.

³⁷⁴ *Loi sur le droit d'auteur*, LRC 1985, c. C-42, art. 41.1

³⁷⁵ *Loi sur le droit d'auteur*, LRC 1985, c. C-42, art. 41.1.

³⁷⁶ *Loi sur le droit d'auteur*, LRC 1985, c. C-42, art. 42 (3.1).

indépendamment du droit d'auteur sous-jacent en cause³⁷⁷ ». C'est-à-dire que ces mesures confèrent aux détenteurs de droits d'auteur des protections et des droits allant au-delà de ce que prévoit la LDA ailleurs dans la législation. Le titulaire du droit d'auteur a le droit de faire respecter une MTP *même lorsque la MTP ne contrôle pas les utilisations de l'œuvre qui sont protégées par le droit d'auteur*. Cela a des conséquences majeures sur les droits de propriété : « si une MTP protège un logiciel qui, à son tour, contrôle la fonctionnalité complète d'un objet mécanique, la MTP peut alors protéger efficacement les aspects non protégés par le droit d'auteur de l'objet³⁷⁸ ».

La réforme législative de 2012 a introduit des exceptions qui visaient à permettre le contournement des MTP dans certaines circonstances (notamment, dans le but d'assurer l'interopérabilité entre différents programmes d'ordinateur). Ces exceptions, très strictes et difficilement utilisables, ont été revues et partiellement corrigées par le législateur en 2024 lors de l'adoption de deux projets de loi, C-244 et C-294 (voir ci-dessous). Pour nos fins, les exemptions les plus importantes sont celles qui permettent le contournement d'une MTP dans le but d'assurer l'interopérabilité entre différents programmes informatiques³⁷⁹. L'interopérabilité est une notion large qui n'est pas définie dans la Loi. Bien que la définition dépende du contexte, elle concerne en général « la capacité de deux ou plusieurs systèmes à échanger des informations et à comprendre les informations échangées³⁸⁰ ».

Les exceptions pour l'interopérabilité incluses dans la Loi en 2012 se sont avérées limitées. En premier lieu, les exceptions ne s'appliquent qu'aux programmes d'ordinateur ; c'est-à-dire que la Loi permet le contournement d'une MTP seulement pour rendre un programme d'ordinateur interopérable avec un autre. Cette formulation est ambiguë et il n'est pas clair si l'exemption s'applique aux biens intégrant des logiciels protégés par les MTP. Est-il autorisé de contourner une MTP dans un « programme d'ordinateur » d'une voiture connectée afin de rendre la voiture interopérable avec une pièce physique

³⁷⁷ Notre traduction. Anthony D ROSBOROUGH, « If a Machine Could Talk, We Would Not Understand It: Canadian Innovation and the Copyright Act's TPM Interoperability Framework », (2023) 19-1 *Can. J. Law Technol.* 141-171, 154. Rosborough parle ici des États-Unis, mais l'analyse est applicable à la législation canadienne. Pour une discussion sur l'effet similaire du mot « utilisation » dans la législation européenne, voir S. DUSOLIER, préc., note 365, 75-86.

³⁷⁸ A. D. ROSBOROUGH, préc., note 377, 154. Notre traduction.

³⁷⁹ *Loi sur le droit d'auteur*, LRC 1985, c. C-42, art. 41.12.

³⁸⁰ Notre traduction. Daniel HODAPP et André HANELT, « Interoperability in the era of digital innovation: An information systems research agenda », (2022) 37-5 *J. Inf. Technol.* 1-21, DOI : 10.1177/02683962211064304. A. D. ROSBOROUGH, préc., note 377, 163-164. Rosborough constate que le US DMCA contient une définition d'interopérabilité : « *the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged* » ; cette définition est ambiguë, car elle ne définit pas quelle partie du programme doit être mutuellement utilisable et dans quelle mesure les informations doivent être partagées de manière symétrique. Comme le note l'auteur, une étude des définitions du terme révèle qu'il dépend fortement du contexte et de la technologie ou du cas d'utilisation en question.

générique du véhicule ?³⁸¹ La réponse n'est pas claire, car il n'est pas question de rendre deux programmes d'ordinateur interopérables³⁸².

Deuxièmement, l'exemption s'applique lorsque le contournement d'une MTP est fait dans le **seul but** d'obtenir de l'information permettant de rendre un programme d'ordinateur et un autre interopérables. Elle permet également d'offrir au public ou de fournir des services ou une technologie en vue de contourner une MTP **uniquement** pour rendre le programme interopérable avec un autre³⁸³. Ces règles ont été utilisées pour refuser l'application de l'exception d'interopérabilité dans l'arrêt *Nintendo of America Inc. c. King* par la Cour fédérale en 2017.

La décision rendue dans cette affaire démontre à quel point les règles contre le contournement des MTP sont vastes et les exemptions sont limitées³⁸⁴. Dans cette affaire, la demanderesse a poursuivi une entreprise dirigée par le défendeur pour avoir vendu des dispositifs pour modifier les consoles de jeux Nintendo. La modification permettait aux utilisateurs de jouer des copies des jeux non autorisées sur leur console. La Cour a donné raison à Nintendo, qui a prétendu que cette distribution de dispositifs constituait une violation de la *LDA*, car la modification permettait à la console de jouer des jeux qui n'étaient pas autorisés par Nintendo, et constituait ainsi un contournement d'une MTP. Le Tribunal a rejeté l'argument selon lequel le défendeur ne contournait pas de MTP puisque le dispositif en question imitait simplement le logiciel de Nintendo afin d'inciter la console à accepter une cartouche de jeu non officiel, et ne contournait donc aucun obstacle ou verrou numérique. La Cour a conclu que cet acte constituait un contournement d'une MTP, même s'il n'avait pour effet que d'imiter le logiciel de Nintendo, car l'intention du législateur était de donner aux titulaires du droit d'auteur un pouvoir de contrôler l'accès à leurs œuvres. Elle a conclu que « les MTP de contrôle de l'accès ne doivent pas utiliser un obstacle quelconque à la copie pour être "efficaces" »³⁸⁵.

La Cour a également rejeté la défense de King voulant que la vente du dispositif relevait des exemptions d'interopérabilité. Ce dernier a plaidé que le contournement était légitime, car le dispositif permettait aux consommateurs de jouer aux jeux « *homebrew* » et donc rendait la console Nintendo interopérable avec les jeux non officiels. Selon la Cour, la preuve démontrait que l'objectif principal des dispositifs « est de permettre aux utilisateurs de jouer des copies pirates des jeux Nintendo » et donc le contournement n'avait pas comme seul but l'interopérabilité légitime avec les jeux *homebrew*³⁸⁶. De plus, la Cour a trouvé que le contournement n'était pas nécessaire pour permettre aux développeurs de distribuer des jeux *homebrew* et pour les consommateurs d'en jouer ; ainsi, il « ne faut

³⁸¹ Voir A. D. ROSBOROUGH, préc., note 377, 161-162.

³⁸² Michael GEIST, « 61 Reforms to C-61, Day 28: TPMs - Interoperability Exception, Linux and DVDs - Michael Geist » (30 juillet 2008), en ligne : <<https://www.michaelgeist.ca/2008/07/61-reforms-to-c-61-day-28/>> (consulté le 10 octobre 2024).

³⁸³ *Loi sur le droit d'auteur*, LRC 1985, c. C-42, art. 41.12. La *LDA* art. 30.61 permet aussi la reproduction d'un exemplaire d'un programme d'ordinateur pour le rendre interopérable avec un autre programme d'ordinateur.

³⁸⁴ *Nintendo of America Inc. c. King*, 2017 CF 246, [2018] 1 RCF 509, [*Nintendo c. King*].

³⁸⁵ *Nintendo c. King*, pars. 81-84.

³⁸⁶ *Nintendo c. King*, par. 120.

pas nécessairement contourner les MTP pour obtenir l'interopérabilité »³⁸⁷. Pour cette violation de droit d'auteur de logiciels de Nintendo, King a été condamné à payer plus de 12 millions de dollars en dommages-intérêts statutaires et punitifs³⁸⁸.

Cette décision donne une interprétation large de la définition de MTP et une interprétation restrictive d'interopérabilité. Elle suggère que tout contournement permettant l'utilisation des accessoires non officiels avec un logiciel peut constituer une violation de la LDA, même si aucun verrou ou obstacle numérique n'est contourné. Elle semble également indiquer que l'exemption d'interopérabilité ne s'applique pas s'il existe une possibilité de suivre la procédure préférée du titulaire du droit d'auteur pour faire fonctionner son logiciel avec un accessoire.

Taken together, these considerations suggest that circumvention of a TPM [MTP], for the purposes of interoperability requires some degree of necessity. It also suggests that where an OEM [Original equipment manufacturer ou fabricant] provides some internal process for accommodating third-party products or services, circumvention may not be 'legitimate'.³⁸⁹

Cette décision est le seul arrêt important concernant les règles du MTP et l'exemption de l'interopérabilité dans la LDA.

En 2024, deux projets de loi, C-244³⁹⁰ et C-294, ont été adoptés pour élargir ces exemptions. Ces lois ont été adoptées après de nombreuses années au cours desquelles les commentateurs ont souligné que les limites au contournement entravaient les réparations et après les initiatives américaines sur cette question. Elles suivent également les initiatives américaines sur ce point. Depuis les années 2010, le bibliothécaire du Congrès des États-Unis a pris une série de décisions autorisant le contournement des MTP contrôlant l'accès à certains œuvres si le contournement est nécessaire pour permettre le diagnostic, la réparation ou la modification d'un véhicule³⁹¹. L'adoption des exemptions reflète un effort pour trouver un juste milieu entre la protection des droits d'auteur et la promotion de l'utilisation légitime des œuvres protégées³⁹².

³⁸⁷ *Nintendo c. King*, par. 123.

³⁸⁸ *Nintendo c. King*, conclusions.

³⁸⁹ A. D. ROSBOROUGH, préc., note 377, 159.

³⁹⁰ Une version antérieure de ce projet de loi a été déposée en février 2021 comme le projet de Loi C-272. Ce dernier est « mort au feuillet » à cause des élections fédérales de l'automne 2021.

³⁹¹ Le bibliothécaire révise ces règles chaque 3 ans. Pour la décision la plus récente, voir « Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies », *Federal Register*, 28 octobre 2021, <https://www.federalregister.gov/documents/2021/10/28/2021-23311/exemption-to-prohibition-on-circumvention-of-copyright-protection-systems-for-access-control>. Il faut noter que l'exemption ne s'applique qu'à l'accès et pas à la distribution des dispositifs pour effectuer ce contournement. Voir aussi Justin Wm. MOYER, « Hacking your car is cool with us, says U.S. copyright authority - The Washington Post », *Washington Post* (28 octobre 2015).

³⁹² MC FORELLE, « Copyright and the modern car: Colliding visions of the public good in DMCA section 1201 anti-circumvention proceedings », (2023) 25-3 *New Media Soc.* 628-645, DOI : 10.1177/14614448211015235.

Les initiatives législatives autour du droit à la réparation ont commencé à prendre forme au Canada quelques années plus tard. En 2017, le Comité permanent de l'industrie, des sciences et de la technologie de la Chambre des communes fédérale a mené un examen de la *LDA*. Lors de cet examen, le Comité a entendu de nombreux intervenants qui ont « proposé d'autoriser le contournement des MTP à des fins d'utilisation licites du contenu » pour plusieurs raisons, y compris pour faciliter l'entretien et la réparation³⁹³. Le Comité a également reçu la recommandation de certains témoins « d'ajouter une disposition à la Loi pour prévenir l'application d'une clause contractuelle relativement aux activités qui ne constitueraient pas une violation aux termes de la Loi³⁹⁴ ». Le Comité a abondé dans ce sens et recommandé au gouvernement de moderniser les politiques « notamment pour faciliter l'entretien, la réparation ou l'adaptation d'un appareil acquis légalement à des fins qui ne portent pas atteinte au droit d'auteur³⁹⁵ ».

C'est dans ce contexte que les projets de loi nommés ci-haut ont été proposés et adoptés.

Le projet de loi C-294 modifie la *LDA* pour élargir l'exception d'interopérabilité afin de permettre le contournement pour rendre un programme d'ordinateur ou un dispositif dans lequel il est intégré interopérable avec un autre programme d'ordinateur, un dispositif ou composant³⁹⁶. Cela clarifie l'ambiguïté lorsqu'il s'agit de rendre les programmes d'ordinateur interopérables avec des biens physiques, tels les véhicules.

Le projet de loi C-244, quant à lui, prévoit une exemption aux règles de contournement des MTP en cas de réparation ou d'entretien d'un produit, y compris tout diagnostic connexe. Dans sa forme initiale, le projet de loi C-244 proposait de créer une exemption aux articles de la *LDA* qui interdisent d'offrir au public ou de fabriquer, importer, fournir, offrir ou mettre en circulation toute technologie pour contourner une MTP, si le contournement avait pour objectif de rendre possible tout diagnostic, entretien ou toute réparation du produit³⁹⁷. Cependant, des amendements apportés au projet de loi ont retiré cette exemption³⁹⁸. Cela signifie que les individus doivent compter sur leurs propres

³⁹³ COMITE PERMANENT DE L'INDUSTRIE, DES SCIENCES ET DE LA TECHNOLOGIE, *Examen prévu par la loi de la Loi sur le droit d'auteur*, 2019, p. 76.

³⁹⁴ COMITE PERMANENT DE L'INDUSTRIE, DES SCIENCES ET DE LA TECHNOLOGIE, *Examen prévu par la loi de la Loi sur le droit d'auteur*, 2019, p. 78.

³⁹⁵ COMITE PERMANENT DE L'INDUSTRIE, DES SCIENCES ET DE LA TECHNOLOGIE, préc., note 393, p. 79.

³⁹⁶ *Troisième lecture, Projet de loi C-294 (44-1) : Loi modifiant la Loi sur le droit d'auteur (interopérabilité)*, 70-71 Elizabeth II – 1 Charles III, 2021-2022-2023.

³⁹⁷ *Première lecture, Projet de loi C-244 (44-1) : Loi modifiant la Loi sur le droit d'auteur (diagnostic, entretien et réparation)*, 70-71 Elizabeth II, 2021-2022.

³⁹⁸ *Troisième lecture, Projet de loi C-244 (44-1) : Loi modifiant la Loi sur le droit d'auteur (diagnostic, entretien et réparation)*, 70-71 Elizabeth II — 1-2 Charles III, 2021-2022-2023 §, consulté le 17 octobre 2024. Le projet de loi a été également modifié pour préciser que l'exemption ne s'applique pas aux programmes d'ordinateur, mais plutôt à un produit « duquel fait partie une œuvre, une prestation fixée au moyen d'un enregistrement sonore ou un enregistrement sonore dont l'accès est contrôlé par la mesure technique de protection ». L'effet de cette modification n'est pas clair ; voir Anthony D. ROSBOROUGH et Alissa CENTIVANY, « The empty success of recent amendments to Canada's right-to-repair bill », *Policy Options* (2023), en ligne : <<https://policyoptions.irpp.org/magazines/may-2023/right-to-repair-fail/>> (consulté le 17 octobre 2024); Anthony D. ROSBOROUGH et Alissa CENTIVANY, « Le droit à la réparation se

compétences pour effectuer un contournement, étant donné que l'offre de la technologie ou des services à cet effet n'est pas autorisée³⁹⁹.

5.4 Analyse : adéquation de l'encadrement du droit de propriété

Dans la section 3 du rapport, nous avons identifié des risques posés par la connectivité des voitures au droit de propriété du consommateur. Les contrats de licence et les verrous numériques permettent aux fabricants de garder, après la vente, le contrôle sur l'utilisation du véhicule. Nous avons également vu que la connectivité permet aux fabricants de surveiller l'utilisation du bien et le respect des restrictions qu'ils imposent. De plus, la connectivité donne aux fabricants la capacité de mettre en œuvre ces restrictions avec un contrôle direct sur le bien, par exemple, en leur permettant d'empêcher l'utilisation du bien à distance en cas de non-respect des conditions de service. Dans la section 4, nous avons également identifié des préoccupations des consommateurs en ce qui concerne l'accès à la réparation, vu la complexification des biens et les restrictions possibles sur la réparation.

L'encadrement juridique canadien du droit de propriété n'apaise pas les préoccupations identifiées en ce qui concerne les véhicules connectés. Au contraire, les lois permettent la division d'un bien entre éléments corporels et incorporels et la *LDA* énonce un large éventail de droits pour le propriétaire des droits de propriété intellectuelle. Cette division des droits de propriété peut avoir un sens dans certains contextes, par exemple lorsqu'un logiciel est utilisé sur un ordinateur et que la désactivation ou le contrôle de ce logiciel n'aurait pas d'impact au-delà de son utilisation. Toutefois, lorsque le logiciel est intégré dans un bien, tel qu'un véhicule, cette division devient plus problématique, car elle permet au fabricant d'exercer un contrôle sur le bien physique qui dépend du logiciel.

L'encadrement législatif ne prévoit aucune protection pour le consommateur contre le contrôle à distance exercé par les fabricants des biens connectés. Rien n'empêche l'utilisation des contrats de licence d'utilisateur final restrictifs. Dans notre rapport sur les contrats de licence de 2010, nous avons plaidé que les CLUF devraient être reconnus comme des contrats de consommation et devraient être assujettis aux lois sur la

précise au Canada, mais des incertitudes demeurent », *Policy Options* (2023), en ligne : <<https://policyoptions.irpp.org/fr/magazines/decembre-2023/droit-de-reparer/>> (consulté le 17 octobre 2024).

³⁹⁹ Cette prudence dans la formulation du projet de loi pourrait être attribuée aux obligations commerciales internationales du Canada, notamment dans le cadre de l'Accord Canada-États-Unis-Mexique (ACEUM) : Anthony D ROSBOROUGH et Alissa CENTIVANY, « Le droit à la réparation se précise au Canada, mais des incertitudes demeurent », *Policy Options*, en ligne : <<https://policyoptions.irpp.org/fr/magazines/decembre-2023/droit-de-reparer/>> (consulté le 17 octobre 2024). Cependant, l'Accord prévoit que les États signataires peuvent prévoir des exceptions aux règles de contournement des MTP, si c'est pour une utilisation non attentatoire d'une catégorie particulière d'œuvres et « lorsque l'effet néfaste réel ou probable de cette utilisation non attentatoire est démontré par des éléments de preuve substantiels » : *Accord Canada-États-Unis-Mexique (ACEUM)* 30 novembre 2018, Chapitre 20, Droits de propriété intellectuelle, art. 20.66 (4)(a) et (h). Voir aussi A. D. ROSBOROUGH, préc., note 377, 166.

protection des consommateurs⁴⁰⁰. Les clauses abusives devraient être traitées comme telles dans le cadre de la législation sur la protection des consommateurs ; toutefois, à ce jour, la législation sur la protection des consommateurs ne protège guère les consommateurs à cet égard. Les contrats de licence d'utilisation imposent actuellement des limites importantes et préjudiciables à l'utilisation par les consommateurs des biens qu'ils ont achetés, et cette situation devrait être mieux réglementée, tant dans la LDA que dans les lois sur la protection des consommateurs.

De plus, nous constatons que l'encadrement juridique de la LDA protège les droits de propriété intellectuelle des fabricants d'une manière préjudiciable aux consommateurs, en protégeant l'utilisation des MTP, sous réserve de quelques exemptions, fort limitées.

Historiquement, ce contrôle direct du bien acheté par un consommateur n'a jamais été l'objectif de la LDA⁴⁰¹. Comme nous l'avons vu plus haut, la Loi était à l'origine destinée à protéger les détenteurs de droits contre d'autres acteurs commerciaux, et l'introduction des MTP dans la LDA a étendu, d'une manière sans précédent, les droits des titulaires de droits d'auteur, puisqu'elle permet l'exercice d'un contrôle et l'imposition de restrictions à des utilisations privées et autrement autorisées de l'œuvre. La justification pour cette intrusion sur les droits des consommateurs était que les MTP étaient nécessaires pour empêcher le piratage, si facile à l'ère numérique, et la commercialisation illégale des œuvres⁴⁰². Cependant, la littérature démontre que ce type de mesure de contrôle a été utilisé, non seulement pour protéger les droits des titulaires de droits d'auteur de publier ou de reproduire leur œuvre, mais aussi pour conserver un « droit de regard » sur la façon dont les consommateurs utilisent leurs biens⁴⁰³. En effet, ce qui fait l'objet d'un contrôle par les fabricants automobiles va bien au-delà de l'interdiction de la copie de logiciels intégrés à l'automobile :

TPMs [MTP] typically bar access to both copyrighted components (like the entertainment portion of the data) and uncopyrightable elements (like the car's diagnostic data). Thus, unlike scan tool data, diagnostic telematics data is not accessible to everyone⁴⁰⁴.

Les restrictions imposées par les MTP n'ont fait que s'aggraver dans l'ère des biens connectés et de l'Internet des objets. Les MTP ont été incorporées au départ aux composants physiques des œuvres protégées, tels que les CD et DVD contenant la musique, les logiciels ou les vidéos. Maintenant, les MTP sont intégrées aux biens physiques qui ne contiennent aucune autre œuvre protégée que le logiciel requis pour faire fonctionner l'objet (la voiture, le thermostat, la porte, etc.)⁴⁰⁵. Alors que la LDA visait à l'origine à protéger les œuvres telles que les jeux, la musique et les films contre la

⁴⁰⁰ UNION DES CONSOMMATEURS, préc., note 182, p. 19.

⁴⁰¹ Michelle M. Wu, *Defeating the Economic Theory of Copyright: How the Natural Right to Seek Knowledge is the Only Theory Able to Explain the Entirety of Copyright's Balance*, Georgetown Law Faculty Publications and Other Works, 2023, p. 16, en ligne : <https://scholarship.law.georgetown.edu/facpub/2495>.

⁴⁰² L. MAUREL, préc., note 176, 22.

⁴⁰³ *Id.*

⁴⁰⁴ L. CHAN GRINVALD et O. TUR-SINAI, préc., note 219, 296.

⁴⁰⁵ P. CHAPDELAINE et al., préc., note 196, p. 4.

reproduction et la distribution illégales, elle est désormais utilisée pour justifier les limites aux droits des consommateurs à utiliser leurs objets quotidiens. Les MTP, qui constituaient déjà une intrusion sans précédent dans l'utilisation par le consommateur d'un bien qu'il avait acheté, sont devenus considérablement plus intrusifs avec l'avènement des biens connectés. Ils peuvent désormais être utilisés avec les contrats de licence pour restreindre la réparation ou d'autres utilisations essentielles d'un bien physique, et leur application peut être surveillée et contrôlée par le fabricant grâce à la connectivité.

Pour ces raisons, certains auteurs plaident que les règles sur les MTP sont contraires à l'objectif de la LDA :

*The use of TPMs [MTP] by manufacturers to control and protect uncopyrightable features of physical devices in no way furthers the objectives of copyright and the delicate balance to preserve between competing interests, and significantly narrows the scope of the property rights and uses of such physical devices*⁴⁰⁶.

En effet, certains plaident que l'objectif de la promotion de l'innovation dans les lois sur la propriété intellectuelle justifie l'approche inverse : encourager l'interopérabilité et l'utilisation des standards et rendre les codes sources des véhicules plus ouverts⁴⁰⁷.

*Many of the current standard setting organizations (SSOs) in the automotive field champion open interoperability standards. In fact, at least one industry SSO has adopted open-source software policies, and seemingly every major auto manufacturer works with Android Auto to support an open development model for infotainment apps*⁴⁰⁸.

*However, economic theory has shown that firms often have too many incentives for choosing systems with a too low level of interoperability, leading to too closed systems with a too low level of openness and interoperability. This problem also seems to be very relevant with regard to IoT [Internet of Things] applications, where many complaints about too many firm-specific proprietary solutions can be found, leading to the demand for more interoperability and standardization*⁴⁰⁹.

Bien que la Loi prévoie des exemptions au contournement des MTP, ces exemptions ne semblent pas répondre aux besoins des consommateurs. L'adoption du projet de loi C-294 semble désormais permettre de contourner une MTP afin de s'assurer qu'une voiture connectée peut fonctionner avec une pièce générique plutôt qu'une pièce d'origine (ou « propriétaire »). Cependant, la décision dans l'affaire *Nintendo c. King* peut limiter cette règle. Si le détenteur d'un droit d'auteur permet d'une manière ou d'une autre d'atteindre le résultat visé par le contournement, le jugement suggère que ce contournement n'est pas sujet à l'exemption d'interopérabilité. Si le fabricant fournit donc des pièces de remplacement officielles, est-ce que le contournement d'une MTP pour permettre l'utilisation d'une pièce du marché secondaire constitue une violation de la LDA ? La décision de *Nintendo c. King* semble dire que ça l'est, car le contournement n'est pas

⁴⁰⁶ *Id.*, p. 10.

⁴⁰⁷ L. DETERMANN et B. PERENS, préc., note 16, 945.

⁴⁰⁸ *Id.*, 970.

⁴⁰⁹ W. KERBER, préc., note 242, 6.

nécessaire pour effectuer le remplacement : le consommateur aurait pu simplement utiliser la pièce autorisée⁴¹⁰. Même si ce n'est pas le cas, l'incertitude et la crainte de litiges ne manqueront pas d'empêcher quiconque de contourner une MTP à cette fin ou d'offrir un tel service.

De plus, nous avons des doutes sur l'utilité du nouvel article 41.121 de la LDA, introduit par le projet de loi C-244, qui ne permet pas d'offrir au public des outils pour contourner des MTP pour des fins de réparation ou de diagnostic, étant donné que le consommateur moyen ne peut pas contourner ces verrous numériques sans recourir à un service à un outil spécialisé⁴¹¹.

En outre, rien dans ces dispositions ne permet aux consommateurs de contourner des MTP pour des raisons autres que la réparation, le diagnostic ou l'interopérabilité. Cela veut dire que le consommateur est toujours limité dans son utilisation du bien ; par exemple, il est interdit de contourner une MTP pour mettre fin à un contrôle à distance non souhaité de son bien, pour changer le logiciel du véhicule pour un logiciel ouvert, etc.

Une façon de résoudre tous ces problèmes serait de revenir à une recommandation entre autres faite par Union des consommateurs, au moment de la réforme législative de la LDA de 2012 : éliminer la protection des MTP qui contrôlent l'accès à une œuvre⁴¹². C'est-à-dire que la LDA ne devrait seulement protéger une MTP qui a pour effet de restreindre une utilisation de l'œuvre déjà interdite par la Loi, par exemple sa reproduction ou sa distribution illicite.

En résumé, l'encadrement actuel permet aux fabricants de conserver un contrôle important sur le bien auquel est attaché le logiciel. En effet, le cadre législatif examiné ici ne prévoit aucune protection pour les consommateurs en ce qui concerne ce contrôle. En ce sens, il n'atténue en rien les risques et les préoccupations identifiés, et aggrave même certains problèmes tels que le droit à la réparation. Dans la section suivante, nous examinerons une approche différente, qui définit un droit à la réparation plus positif.

5.5 Vers un droit à la réparation canadien ? Le droit à la réparation au Québec

Rappelons que l'un des risques des voitures connectées identifiés dans ce rapport est l'atteinte au droit à la réparation : sans accès aux données de diagnostic et aux logiciels de réparation, les mécaniciens indépendants et les consommateurs sont fortement

⁴¹⁰ Graham J. REYNOLDS, « Of Lock-Breaking and Stock Taking - IP, Climate Change, and the Right to Repair in Canada », (2023) 101-1 *Can. Bar Rev.* 32-60, 53-54.

⁴¹¹ Voir A. D. ROSBOROUGH et A. CENTIVANY, préc., note 399.

⁴¹² UNION DES CONSOMMATEURS, préc., note 366. Voir aussi P. CHAPDELAINE et al., préc., note 196, p. 14.

désavantagés. En examinant le cadre législatif au Canada, nous n'avons trouvé qu'une seule législation qui tente de traiter cette question d'une façon directe⁴¹³.

Au Québec, en 2023, des modifications ont été apportées à la *Loi sur la protection du consommateur* (LPC) afin de renforcer le droit à la réparation pour les consommateurs québécois. À la suite du dépôt du projet de loi n° 29, Loi protégeant les consommateurs contre l'obsolescence programmée et favorisant la durabilité, la réparabilité et l'entretien des biens (PL 29), des dispositions spécifiques à la réparation d'automobiles ont été adoptées. Les nouvelles dispositions de la LPC concernent plus largement le droit à la réparation, mais nous nous concentrerons sur celles qui ont un lien direct avec les automobiles connectées et la connectivité des biens de consommation.

En prenant en compte la réalité de la réparation des voitures connectées, le législateur québécois a ainsi voulu faciliter l'accès aux données automobiles nécessaires à des fins de diagnostic, d'entretien ou de réparation. Cette initiative a été bien accueillie par des groupes de défenses de droits des consommateurs et par des représentants des réparateurs automobiles indépendants. Selon LKQ, une entreprise qui distribue des pièces de réparation automobile en Amérique du Nord et qui fait affaire au Québec :

*L'angle du contrôle des données par les grands fabricants automobiles est l'angle le plus saillant qui contribue à l'érosion de la participation des joueurs indépendants de l'après-marché de l'automobile*⁴¹⁴.

Le nouvel article 39.4 de la LPC impose aux fabricants automobiles de :

*donner accès, dans un format lisible, aux données de cette automobile à son propriétaire, à son locataire à long terme ou au mandataire de ceux-ci ou à toute autre personne déterminée par règlement, à des fins de diagnostic, d'entretien ou de réparation*⁴¹⁵.

Au moment d'écrire ces lignes, l'article n'a pas encore fait l'objet d'interprétation devant les tribunaux et nous ne sommes pas en mesure d'évaluer, à ce stade, le degré de

⁴¹³ Il existe au Canada un accord volontaire signé par les membres de l'industrie automobile, connu sous le nom de *The Canadian Automotive Service Information Standard* ou « CASIS ». L'objectif de l'accord, qui est toujours en vigueur, est de garantir au marché secondaire automobile un accès similaire à celui qui est fourni aux concessionnaires aux renseignements relatifs à l'entretien, aux outils de diagnostic et aux informations sur la formation. Tout comme le MOU américain (voir la section 5.6.1), les principales dispositions de l'accord exigent des fabricants automobiles qu'ils fournissent aux réparateurs professionnels des renseignements sur les services et les outils de la même manière et dans la même mesure qu'aux concessionnaires. En outre, les fabricants doivent permettre aux réparateurs d'accéder aux informations sur l'entretien à des « prix commercialement raisonnables » et par le biais d'un abonnement à court terme. L'accord présente des lacunes importantes : il ne garantit pas aux consommateurs le droit d'obtenir des informations de diagnostic concernant leurs véhicules, il ne prévoit pas de mécanisme d'application rigoureux et il ne prévoit pas l'utilisation des données télématiques. *An Agreement Respecting The Canadian Automotive Service Information Standard* (« CASIS »), 2009, en ligne : <https://www.oemrepairinfo.ca/wp-content/uploads/2024/06/CASIS_EN.pdf>.

⁴¹⁴ LKQ CORPORATION, préc., note 223, p. 7.

⁴¹⁵ *Loi sur la protection du consommateur*, RLRQ, c. P-40.1, art. 39.4.

coopération des fabricants face à cette obligation⁴¹⁶. Pour l'Association pour la protection des automobilistes (APA), qui a présenté un mémoire dans le cadre des consultations sur le PL 29, cette disposition est nécessaire dans le contexte de la voiture connectée. En effet, l'APA a souligné qu'il est difficile pour les ateliers indépendants d'accéder aux données de l'automobile pour les véhicules connectés qui ne sont pas équipés de port OBD-II et qui transmettent des données diagnostiques purement par une connexion sans fil. L'Association se réfère à l'exemple du fabricant Tesla qui limite l'accès aux données de réparation et d'entretien :

Les Tesla ne sont donc pas équipées de port OBD II et l'accès à leurs données est laborieux. Tesla bloque cette communication et force les ateliers indépendants à pirater les véhicules pour être en mesure d'obtenir les données nécessaires aux réparations. Le PL 29 pourrait empêcher un dérapage où d'autres fabricants pourraient s'inspirer de l'exemple de Tesla⁴¹⁷.

Soulignons qu'entre la présentation du projet de loi et l'adoption finale de cette disposition, le législateur a retiré l'obligation de fournir gratuitement cet accès aux données⁴¹⁸. Cela constitue, selon nous, un recul pour les droits des consommateurs. La Loi prévoit un encadrement général du prix auquel doivent être fournis les renseignements nécessaires à l'entretien et la réparation, dont font partie les données de réparation. Selon l'article 39.3 de la LPC, les données doivent être disponibles à un prix raisonnable. La définition de « prix raisonnable » est prévue au deuxième alinéa, soit un prix qui ne décourage pas l'accès par le consommateur ou son mandataire⁴¹⁹. Un règlement pourra déterminer des cas dans lesquels le prix d'un renseignement nécessaire à l'entretien et à la réparation est présumé décourager l'accès⁴²⁰.

Le coût de ces données reste donc un enjeu à surveiller et l'application de la disposition qui oblige le fabricant à les fournir à un prix raisonnable devra faire l'objet d'une analyse future afin de déterminer son efficacité pour mitiger les difficultés des consommateurs en matière de réparation et d'entretien de leur voiture connectée. À l'heure actuelle, le coût des données de réparation et d'entretien est un enjeu de taille et la notion de la raisonnable de ce coût peut laisser présager des difficultés d'application sans la mise en place de balises plus claires par les tribunaux ou par voie réglementaire.

⁴¹⁶ L'article entrera en vigueur le 5 octobre 2025.

⁴¹⁷ L'ASSOCIATION POUR LA PROTECTION DES AUTOMOBILISTES, *Mémoire : Consultations particulières et auditions publiques sur le projet de loi n° 29, Loi protégeant les consommateurs contre l'obsolescence programmée et favorisant la durabilité, la réparabilité et l'entretien des biens*, à la Commission de l'économie et du travail, 009M, 2023, p. 6, en ligne : https://www.assnat.qc.ca/Media/Process.aspx?MediaId=ANQ.Vigie.BII.DocumentGenerique_191735&process=Default&token=ZyMoxNwUn8ikQ+TRKYwPCjWrKwg+vIv9rjj7p3xLGTZDmLVSmJLoqe/vG7/YWzz.

⁴¹⁸ *Loi protégeant les consommateurs contre l'obsolescence programmée et favorisant la durabilité, la réparabilité et l'entretien des biens*, Projet de loi 29 (Présentation - 1 juin 2023), en ligne : <https://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-29-43-1.html>, art. 4.

⁴¹⁹ *Loi sur la protection du consommateur*, RLRQ, c. P-40.1, art. 39.3. al. 2.

⁴²⁰ *Loi sur la protection du consommateur*, RLRQ, c. P-40.1, art. 39.3. al. 3.

D'un autre côté, le législateur a amendé le projet de loi pour ajouter l'obligation de donner accès aux données dans un format lisible. Cet ajout fait écho à certaines demandes transmises par des représentants de l'industrie des réparateurs automobiles lors de consultation sur le PL 29. LKQ a notamment indiqué au législateur que le manque d'accès aux données de réparation et d'entretien ne passe pas nécessairement par un refus clair du fabricant. Des réparateurs indépendants peuvent aussi être privés de ces données du fait que certains fabricants peuvent rendre les transferts de données coûteux ou transmettre des données qui sont difficilement lisibles pour les réparateurs indépendants⁴²¹. La disposition adoptée fait ainsi explicitement référence à l'obligation de fournir des données dans un format lisible tout en mettant de côté l'obligation de fournir ces données gratuitement.

L'obligation du fabricant de fournir les données de diagnostic, de réparation et d'entretien est une obligation envers le consommateur et non pas directement envers les réparateurs indépendants. En effet, la LPC encadre les relations contractuelles et précontractuelles entre les commerçants et les consommateurs et n'encadre pas les obligations que pourraient avoir les fabricants envers d'autres commerçants. Le libellé de la disposition laisse supposer cependant que le consommateur pourra désigner le réparateur de son choix comme étant son mandataire et que ce dernier pourra, de cette manière, accéder aux données de l'automobile. En revanche, un flou demeure autour de la notion de mandataire et de la facilité avec laquelle les consommateurs pourront permettre à un réparateur de leur choix d'obtenir les données de leur automobile. Dans le cadre des consultations sur le PL 29, l'Association des industries de l'automobile du Canada, qui représente le secteur canadien de l'entretien et de la réparation automobile, a indiqué sa crainte « qu'une définition trop vague de mandataire ne permette à des fabricants automobiles de multiplier les exigences et les délais avant d'accéder à une requête de partage de données de conduite et ainsi se soustraire à cette disposition cruciale de la Loi⁴²² ».

Le législateur québécois a aussi adopté une disposition qui interdit formellement au fabricant automobile l'utilisation de techniques ayant pour effet de rendre plus difficile la réparation ou l'entretien d'une automobile, notamment en rendant l'accès aux données diagnostiques plus difficile :

227.0.3 Sous réserve de ce qui peut être prévu par règlement, aucun commerçant ou fabricant ne peut recourir à une technique ayant pour effet de rendre plus difficile pour le consommateur ou son mandataire d'entretenir ou de réparer un bien.

Est notamment une technique visée au premier alinéa le recours, par un fabricant d'une automobile, à une technique ayant pour effet de rendre plus difficile pour son propriétaire, son locataire à long terme ou le mandataire de ceux-ci d'avoir accès

⁴²¹ LKQ CORPORATION, préc., note 223, p. 8.

⁴²² L'ASSOCIATION POUR LA PROTECTION DES AUTOMOBILISTES, préc., note 417, p. 12.

*aux données de l'automobile à des fins de diagnostic, d'entretien ou de réparation*⁴²³.

Cette disposition nous semble particulièrement intéressante, car elle suggère qu'une MTP qui rend la réparation plus difficile pourrait être illégale. Reste à savoir ce qui constituerait une « technique ayant pour effet de rendre plus difficile pour le consommateur [...] de réparer un bien ». Les pratiques que nous avons identifiées, telles que l'exigence d'un logiciel spécial pour autoriser une réparation ou pour utiliser une pièce de rechange, seraient-elles considérées comme le recours à une telle technique ? Cette disposition pourrait cependant permettre à l'organisme chargé de la surveillance de l'application de la LPC, l'Office de la protection du consommateur (OPC), d'agir plus largement sur les techniques mises en place par les fabricants, afin de garantir le plus efficacement possible le droit à la réparabilité.

Un autre élément lié à la connectivité a été intégré au PL 29 : l'obligation pour les commerçants et les fabricants qui les utilisent de rendre disponibles les logiciels de diagnostic et leurs mises à jour, pendant une durée raisonnable après la conclusion d'un contrat⁴²⁴. Toutefois, la LPC permet aux commerçants et aux fabricants de se dégager de cette obligation en avertissant le consommateur par écrit, avant la conclusion du contrat, qu'ils ne fournissent pas de tels renseignements⁴²⁵. Dans l'éventualité où les fabricants automobiles devaient garantir la disponibilité des logiciels de diagnostic et leurs mises à jour, ils devraient aussi, en vertu de l'article 39.3 de la LPC, les rendre disponibles gratuitement lorsqu'ils sont accessibles sur un support technologique⁴²⁶. Une lacune importante : le législateur n'oblige pas les commerçants et les fabricants de rendre disponibles les logiciels nécessaires à la réparation et l'entretien (l'obligation ne s'applique qu'aux logiciels de diagnostic). Cela pourrait avoir un effet néfaste sur le droit à la réparation ; par exemple, le logiciel nécessaire pour réinitialiser un véhicule après sa réparation est un logiciel nécessaire à la réparation, mais il n'est pas un logiciel de diagnostic, et n'est donc pas expressément visé dans l'article 39 de la LPC. On peut donc se demander si ce choix sera un frein à l'accès à certains logiciels nécessaires pour procéder à l'entretien et la réparation d'une automobile par un réparateur indépendant.

En cas de défaut des commerçants et des fabricants de respecter les obligations prévues à la Loi, les consommateurs ont les recours généraux de la Loi, par exemple, l'exécution de l'obligation de fournir les données ou logiciels requis⁴²⁷. Le législateur a aussi prévu des recours spécifiques, notamment lorsque le fabricant ou le commerçant se trouvent en défaut de rendre disponibles les renseignements nécessaires à la réparation pendant une durée raisonnable et qu'ils ne se sont pas dégagés de cette obligation conformément à la Loi⁴²⁸. Dans certaines circonstances, le consommateur pourrait notamment obtenir que le

⁴²³ *Loi sur la protection du consommateur*, RLRQ, c. P-40.1, art. 227.0.3.

⁴²⁴ *Loi sur la protection du consommateur*, RLRQ, c. P-40.1, art. 39 al.1.

⁴²⁵ *Loi sur la protection du consommateur*, RLRQ, c. P-40.1, art. 39 al.3.

⁴²⁶ *Loi sur la protection du consommateur*, RLRQ, c. P-40.1, art. 39.3 al.1.

⁴²⁷ *Loi sur la protection du consommateur*, RLRQ, c. P-40.1, art. 272.

⁴²⁸ *Loi sur la protection du consommateur*, RLRQ, c. P-40.1, art. 39.

fabricant assume les frais raisonnables de réparation⁴²⁹. Il faudra faire le suivi de la mise en œuvre de ces dispositions pour évaluer de quelle façon ses recours seront applicables dans les cas de réparation et d'entretien des automobiles connectées.

L'OPC dispose aussi du pouvoir d'imposer, dans certaines situations, des sanctions administratives pécuniaires pour le non-respect de ces dispositions⁴³⁰. De plus, un fabricant ou un commerçant qui contreviendrait à l'une des dispositions présentées précédemment pourraient faire l'objet de sanctions pénales. De plus, un fabricant qui aurait recours à une technique ayant pour effet de rendre plus difficile pour le consommateur ou son mandataire d'entretenir ou de réparer un bien, pourrait se voir imposer une amende maximale selon le plus élevé des montants correspondant à 125 000 \$ ou à un montant équivalent à 5 % du chiffre d'affaires mondial de l'exercice financier précédent⁴³¹.

En résumé, il reste à voir comment la législation québécoise fonctionnera dans la pratique, mais certains des principes qu'elle introduit semblent atténuer une partie des risques posés par les voitures connectées. En particulier, l'obligation pour les fabricants de partager les données de diagnostic avec les consommateurs, l'obligation de fournir des logiciels de diagnostic et l'interdiction des techniques rendant plus difficile la réparation ou l'entretien d'un bien nous semblent prometteuses. Toutefois, il convient de noter que le Québec n'est qu'une des législations au sein du Canada et que les véhicules circulent librement entre les provinces canadiennes. Pour que de telles mesures soient réellement efficaces, il serait préférable que celles-ci s'appliquent uniformément à l'ensemble du pays, indifféremment des provinces et territoires.

5.6 Le cadre législatif international

Dans notre recherche, nous avons examiné le cadre législatif international et réglementaire applicable aux États-Unis, en Angleterre, en Union européenne et en Australie. Aucune de ces législations ne disposait de mesures ciblant spécifiquement les voitures connectées⁴³², mais nous avons constaté que chaque législation disposait d'une mosaïque de règles applicables : des règles relatives à la protection de la vie privée et des données personnelles, à la cybersécurité, à la protection des consommateurs, etc.

Ce qui ressort de notre analyse est que certaines de ces législations, notamment le Massachusetts (États-Unis) et l'Union européenne (UE), ont récemment adopté des mesures pour aborder le droit d'avoir accès aux données et aux outils de diagnostic et de réparation des voitures connectées. Comme il s'agit d'une question que, outre le Québec,

⁴²⁹ *Loi sur la protection du consommateur*, RLRQ, c. P-40.1, art. 39.5 à 39.7.

⁴³⁰ *Règlement sur les sanctions administratives pécuniaires relatives à la Loi sur la protection du consommateur*, (2024), Gazette Officielle du Québec, 156e année, no. 50, art. 4 b).

⁴³¹ *Loi sur la protection du consommateur*, RLRQ, c. P-40.1, art. 278.

⁴³² Certaines de ces juridictions disposent de règles régissant les voitures autonomes. Voir, par exemple : UK Parliament, *Automated Vehicles Act 2024* c. 10. Cette Loi ne réglemente que des facteurs liés à la conduite autonome, comme la responsabilité en cas d'accident ou de défaut d'un véhicule autonome, et non les enjeux liés à la connectivité examinés dans ce rapport.

les gouvernements au Canada n'ont pas abordée, il nous a semblé pertinent d'examiner brièvement le droit aux données et aux outils de réparation dans ces législations. Par conséquent, plutôt que d'analyser l'ensemble du cadre législatif applicable dans chacune de ces législations, nous étudierons spécifiquement leur approche sur cette question.

5.6.1 États-Unis

La question du droit d'accès à l'information diagnostique des véhicules est apparue aux États-Unis bien avant l'arrivée des voitures connectées.

Comme nous l'avons vu plus haut, l'introduction de l'électronique dans les véhicules au fil des années a non seulement rendu les réparations plus complexes, mais a également permis aux fabricants de générer et de collecter des données de diagnostic et de réparation. L'introduction de la norme OBD-II a permis aux propriétaires de véhicules et aux mécaniciens indépendants d'accéder à certaines de ces données par un port standardisé. Toutefois, au début des années 2000, les fabricants ont commencé à capter des informations de diagnostic exclues de la norme OBD-II, qu'ils considéraient donc comme exclusives et « propriétaires ». Les mécaniciens indépendants et les propriétaires de véhicules étaient donc désavantagés par rapport aux fabricants et à leurs centres de réparation agréés lorsqu'il s'agissait de diagnostiquer et de réparer les véhicules.

C'est ainsi que le droit de réparer son véhicule est apparu comme un enjeu majeur au début des années 2000. En 2001, un sénateur américain a présenté le premier projet de loi sur le droit à la réparation des propriétaires de véhicules à moteur (le *Motor Vehicle Owners' Right to Repair Act*). Ce projet de loi visait à obliger les fabricants à « divulguer au propriétaire du véhicule, à un atelier de réparation et à la Commission fédérale du commerce (FTC) les informations nécessaires au diagnostic, à l'entretien ou à la réparation du véhicule », à l'exception de certains secrets industriels ; le projet de loi considérait également le non-respect de cette obligation comme un comportement anticoncurrentiel et une pratique déloyale ou trompeuse⁴³³. Le projet de loi n'a jamais été adopté, mais le débat sur la question a resurgi à plusieurs reprises au cours de la décennie suivante, des projets de loi similaires ayant été présentés au Congrès, en 2005 et 2011, sans toutefois être adoptés⁴³⁴.

Après les efforts infructueux du Congrès pour mettre en œuvre une législation sur le droit à la réparation, le Commonwealth du Massachusetts est devenu, en 2012, le premier État américain à inscrire le droit à la réparation dans une loi⁴³⁵. Bien que cette loi ne s'applique

⁴³³ Notre traduction. Paul D. WELLSTONE, « S.2617 - 107th Congress (2001-2002): A bill to protect the rights of American consumers to diagnose, service, and repair motor vehicles purchased in the United States, and for other purposes. » (13 juin 2002), en ligne : <https://www.congress.gov/bill/107th-congress/senate-bill/2617> (consulté le 4 février 2025) (notre traduction).

⁴³⁴ Edolphus TOWNS, « H.R.1449 - 112th Congress (2011-2012): Motor Vehicle Owners Right to Repair Act of 2011 » (18 avril 2011); Joe BARTON, « H.R.2048 - 109th Congress (2005-2006): Motor Vehicle Owners' Right to Repair Act of 2005 » (25 mai 2006).

⁴³⁵ L. CHAN GRINVALD et O. TUR-SINAI, préc., note 219, 283.

qu'au Massachusetts, elle a inspiré l'adoption d'un protocole d'entente, ou « *Memorandum of understanding* » (MOU), par l'industrie automotrice, qui lui est presque identique. Le MOU de 2014 a été signé par quatre groupes représentant les fabricants et l'industrie du marché secondaire et de la réparation. Bien que le protocole d'accord ne soit pas une loi, il réitère les mêmes règles et principes que la législation du Massachusetts, rendant ainsi les dispositions de la loi du Massachusetts indirectement applicables à la quasi-totalité des fabricants automobiles à travers les États-Unis⁴³⁶.

La loi de 2012 et le MOU visaient à établir une égalité d'accès aux informations de réparation entre les concessionnaires ou réparateurs agréés d'une part et les propriétaires de véhicules et les mécaniciens indépendants d'autre part. À ce titre, ces instruments exigent des fabricants automobiles qu'ils fournissent aux mécaniciens indépendants et aux propriétaires de véhicules, pour les modèles déjà en circulation, les mêmes renseignements de diagnostic et de réparation que ceux qui sont mis à la disposition des concessionnaires. Ces informations devraient être disponibles par le biais d'un système électronique d'information, mis en place par le fabricant à des conditions équitables et raisonnables⁴³⁷. Pour les nouveaux véhicules, à partir de 2018, la loi et le MOU exigent en outre que les fabricants « fournissent un accès à leur système de diagnostic embarqué et d'information sur les réparations » de manière standardisée et accessible à partir d'un ordinateur personnel et⁴³⁸. En outre, la loi et le MOU exigent des fabricants qu'ils rendent disponibles tous les outils de diagnostic et de réparation mis à la disposition des concessionnaires⁴³⁹.

Les deux instruments abordent brièvement la question de la connectivité. La loi et le MOU stipulent que si l'accès aux données télématiques nécessaires pour la réparation est fourni aux concessionnaires, cet accès devrait également être fourni aux indépendants, à moins que les données ne soient autrement disponibles par l'intermédiaire du système OBD⁴⁴⁰.

La croissance de la connectivité a rendu la loi et le MOU inadéquats, selon les membres de l'industrie de la réparation. Ces dernières années, le secteur de la réparation a critiqué le fait que les fabricants ne sont pas tenus de fournir les données télématiques autrement disponibles via le port OBD. Cette règle oblige les réparateurs indépendants et les propriétaires de voitures à acheter des outils pour accéder à ces informations via le port OBD plutôt que d'accéder simplement à la version télématique des données. Ces outils peuvent varier d'un modèle à l'autre, ce qui augmente les coûts pour les mécaniciens indépendants⁴⁴¹. En outre, rien dans la loi ou dans le MOU n'exige que les données télématiques soient partagées directement, ni dans un format accessible et normalisé, ni qu'elles soient fournies sans fil ou en continu. Ainsi, tout accès à ces données passe nécessairement par le fabricant ; le mécanicien indépendant ou le consommateur ne peut pas accéder directement aux données (comme il pourrait le faire par le port OBD), ce qui

⁴³⁶ *Id.*

⁴³⁷ Commonwealth of Massachusetts, *Session Law - Acts of 2013*, c 165, arts. 2(a) et (b) ; ALLIANCE OF AUTOMOBILE MANUFACTURERS, GLOBAL AUTOMAKERS, AUTOMOTIVE AFTERMARKET INDUSTRY ASSOCIATION, COALITION FOR AUTO REPAIR EQUALITY, *Memorandum of Understanding*, 2014.

⁴³⁸ Notre traduction. *Id.*, art. 2(d).

⁴³⁹ *Id.*, art. 2(c).

⁴⁴⁰ *Id.*, art. 2(f).

⁴⁴¹ FEDERAL TRADE COMMISSION, préc., note 192, p. 21.

donne au fabricant un contrôle total sur leur coût, le moment où vous les recevez, leur format, etc. En outre, ni les propriétaires de voitures ni les mécaniciens indépendants n'ont accès aux diagnostics à distance ou en continu. Tous ces éléments donnent un avantage aux fabricants et aux concessionnaires, puisque les diagnostics à distance permettent à la fois de diagnostiquer ou prévoir les problèmes sans connexion filaire ou de tester le véhicule et d'analyser les données en continu⁴⁴².

Un autre défaut majeur du MOU est qu'il s'agit en fin de compte d'un accord non contraignant, qui ne s'applique qu'aux signataires, et que les litiges sont tranchés par un panel plutôt que par les tribunaux⁴⁴³. Si la plupart des grands fabricants automobiles sont signataires, d'autres, plus récents, comme Tesla, ne le sont pas.

En 2023, les associations de fabricants automobiles et certains groupes de réparateurs ont signé un accord sur le partage des données de réparation automobile, qui réaffirme les principes du MOU de 2014. L'accord précise en outre que la télématique ne doit pas être utilisée pour contourner les règles du protocole et que les données télématiques nécessaires pour effectuer une réparation doivent être mises à la disposition des propriétaires de véhicules et des réparateurs indépendants de la même manière qu'elles sont mises à la disposition des concessionnaires agréés⁴⁴⁴. Cet accord a toutefois été critiqué par des membres importants du secteur de la réparation, qui n'ont pas participé à son élaboration et qui affirment qu'il reprend simplement le principe du MOU de 2014 et ne remédie donc pas à ses lacunes⁴⁴⁵.

Pour remédier aux lacunes dans sa loi, l'État du Massachusetts a voté une nouvelle initiative populaire en 2020. Une large majorité d'électeurs a soutenu cette initiative qui modifierait la loi de 2013 afin d'obliger les fabricants qui vendent, dans cet État, des véhicules équipés d'un système télématique, à équiper les véhicules d'une « plateforme de données ouverte et normalisée ». Les propriétaires de voitures auraient accès à cette plateforme et à leurs « données mécaniques et diagnostiques par le biais d'une application mobile » qu'ils pourraient partager avec un atelier de réparation indépendant de leur choix. En outre, les réparateurs indépendants seraient en mesure d'utiliser la plateforme pour envoyer des commandes au véhicule « à des fins de réparation, d'entretien et de test de diagnostic ». Les utilisateurs pourraient accéder au système sans l'autorisation du fabricant, sauf dans le cadre d'une procédure d'autorisation normalisée administrée par une partie indépendante⁴⁴⁶. L'initiative devait s'appliquer aux véhicules à partir de l'année modèle 2022, mais sa mise en œuvre a été suspendue à cause d'une action en justice et à la suite de l'avis de la National Highway Traffic Safety Administration (NHTSA) qui a cité des risques à la cybersécurité⁴⁴⁷. La NHTSA a déclaré par la suite

⁴⁴² AFTERMARKETNEWS, « Hanvey: 'OEM Right to Repair MOU an Inadequate Solution' », *aftermarketNews* (17 juillet 2023), en ligne : <<https://www.aftermarketnews.com/hanvey-oem-right-to-repair-mou-an-inadequate-solution/>> (consulté le 30 janvier 2025).

⁴⁴³ ALLIANCE OF AUTOMOBILE MANUFACTURERS, GLOBAL AUTOMAKERS, AUTOMOTIVE AFTERMARKET INDUSTRY ASSOCIATION, COALITION FOR AUTO REPAIR EQUALITY, préc., note 437, art. 6.

⁴⁴⁴ AUTOMOTIVE SERVICE ASSOCIATION, SOCIETY OF COLLISION REPAIR SPECIALISTS, ALLIANCE FOR AUTOMOTIVE INNOVATION, *Automotive Repair Data Sharing Commitment*, 2023, p. 2.

⁴⁴⁵ AFTERMARKETNEWS, préc., note 442.

⁴⁴⁶ Nos traductions. The Commonwealth of Massachusetts, *An Initiative Law to Enhance, Update and Protect the 2013 Motor Vehicle Right to Repair Law*, c 386.

⁴⁴⁷ « Massachusetts Question 1, "Right to Repair Law" Vehicle Data Access Requirement Initiative (2020) », *Ballotpedia*, en ligne :

qu'elle approuvait la mise en œuvre de la loi si les données n'étaient disponibles qu'au moyen de connexions à courte portée, telles que Bluetooth⁴⁴⁸. La loi est entrée en vigueur en 2023⁴⁴⁹.

Cette loi a inspiré un projet de loi fédéral, le *Right to Equitable and Professional Auto Industry Repair Act* (REPAIR Act), qui a été présenté à la Chambre des représentants une première fois en 2021, puis une seconde fois en 2023. Le projet de loi proposait d'adopter de nombreux principes qui se trouvent dans la législation du Massachusetts et il contenait une disposition sur la fourniture aux propriétaires de voitures et à leurs personnes désignées de données télématiques directement et sans fil par le biais d'une plateforme d'accès normalisée⁴⁵⁰. Contrairement à la loi du Massachusetts, la loi REPAIR précisait que les données doivent être accessibles sans restriction ou limitation, y compris les frais, les licences, les dispositifs de décryptage spécifiques, etc.⁴⁵¹. Aucune des deux versions du projet de loi n'a été adoptée.

En résumé, il existe aux États-Unis des mesures visant à garantir un droit positif à la réparation, bien que l'approche soit loin d'être uniforme dans tout le pays pour le moment. La loi de 2013 du Massachusetts et le MOU de 2014 garantissent que les propriétaires de voitures et les réparateurs indépendants ont accès aux mêmes outils et informations que les concessionnaires, moyennant un coût raisonnable. Ce n'est que dans la loi du Massachusetts de 2020 et le projet de loi REPAIR que les consommateurs auraient le droit d'accéder à leurs données télématiques directement, sans l'autorisation des fabricants, et via une plateforme standardisée.

5.6.2 Australie

En 2021, l'Australie a adopté le *Motor Vehicle Information Scheme*, qui exige que les fabricants automobiles partagent les informations sur les réparations avec les réparateurs et les organismes de formation à un prix équitable. L'obligation inclut les logiciels et les mises à jour de logiciels nécessaires au changement de pièces. Toutefois, ce système ne s'étend pas aux données télématiques et exclut les « données générées et transmises automatiquement » par un véhicule pendant qu'il roule, en d'autres termes, les données de diagnostic sans fil⁴⁵². En outre, la loi ne confère aucun droit aux consommateurs eux-

<[https://ballotpedia.org/Massachusetts_Question_1,_%22Right_to_Repair_Law%22_Vehicle_Data_Access_Requirement_Initiative_\(2020\)>](https://ballotpedia.org/Massachusetts_Question_1,_%22Right_to_Repair_Law%22_Vehicle_Data_Access_Requirement_Initiative_(2020)>) (consulté le 3 février 2025).

⁴⁴⁸ U.S. DEPARTMENT OF TRANSPORTATION, NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION, *Lettre à M. Haskell*, 22 août 2023.

⁴⁴⁹ Jack MONAHAN, « Massachusetts Will Now Enforce Auto Right to Repair Law », *iFixit* (28 mars 2025), en ligne : <<https://fr.ifixit.com/News/80102/massachusetts-will-now-enforce-auto-right-to-repair-law>> (consulté le 28 mars 2025).

⁴⁵⁰ Neal P. DUNN, « H.R.906 - 118th Congress (2023-2024): Right to Equitable and Professional Auto Industry Repair Act (REPAIR Act) » (11 février 2023), art. 3(a)(2).

⁴⁵¹ *Id.*, art. 3(a)(2)(A).

⁴⁵² Notre traduction. The Parliament of the Commonwealth of Australia, *Competition and Consumer Amendment (Motor Vehicle Service and Repair Information Sharing Scheme)*, Bill 2021, *Explanatory Memorandum*, par. 1.30.

mêmes, mais seulement aux réparateurs indépendants et aux organismes de formation⁴⁵³.

5.6.3 Union européenne

L'Union européenne a plusieurs instruments juridiques qui s'appliquent aux partages de données diagnostiques des voitures connectées. D'abord, le partage de données de réparation des voitures est quelque peu réglementé par *le Règlement d'exemption par catégorie applicable au secteur automobile* (RECSA). Ce règlement stipule que les contraintes sur les accords verticaux dans la *Traité sur le fonctionnement de l'Union européenne* ne s'appliquent pas aux accords relatifs à la vente ou à la revente de pièces de rechange ou à la fourniture de services de réparation et d'entretien de véhicules si les fabricants ne donnent pas de préférence aux réparateurs agréés dans leurs accords. En d'autres termes, les accords verticaux entre des organismes portant sur la réparation de véhicules ne sont généralement pas interdits par les règles sur la concurrence à condition qu'ils remplissent certaines obligations, notamment, si les fabricants ne refusent pas de donner aux réparateurs indépendants l'accès aux outils, etc., de réparation ou d'entretien⁴⁵⁴.

Ce règlement a été adopté par la Commission européenne pour la première fois en 2010 et renouvelé deux fois par la suite. Dans la mise à jour de 2023, la Commission a publié des lignes directrices précisant que les données générées par les véhicules peuvent être considérées comme un « intrant essentiel » pour la réparation et que la notion d'outils dans le Règlement recouvre les outils de diagnostic électronique et les logiciels⁴⁵⁵. Ainsi, le fabricant ne peut pas conclure un accord préférentiel pour fournir ces outils et ces données à un réparateur agréé plutôt qu'à un indépendant et ne doit pas refuser l'accès de ce dernier à ces données⁴⁵⁶.

Ensuite, le partage des données de réparation est également réglementé par *Le règlement sur des règles harmonisées en matière d'accès équitable aux données et d'utilisation équitable des données*. Ce règlement a été adopté en 2023⁴⁵⁷. Parmi d'autres sujets, il réglemente le partage de données collectées par les objets connectés avec les utilisateurs de ces objets et les tiers de leur choix. Il oblige le détenteur de données ou le fabricant d'un bien connecté, y compris les voitures, de le concevoir et de le fabriquer :

⁴⁵³ *Id.*, art. 1.1.

⁴⁵⁴ COMMISSION EUROPEENNE, « Pratiques anticoncurrentielles : La Commission prolonge le règlement d'exemption par catégorie applicable au secteur automobile et met à jour les lignes directrices supplémentaires » (17 avril 2023), en ligne : https://ec.europa.eu/commission/presscorner/api/files/document/print/fr/ip_23_2248/IP_23_2248_EN.pdf.

⁴⁵⁵ COMMISSION EUROPEENNE, *Modification de la communication de la Commission - Lignes directrices supplémentaires sur les restrictions verticales dans les accords de vente et de réparation de véhicules automobiles et de distribution de pièces de rechange de véhicules automobiles*, 2023/C 133 I/01, art. 29.

⁴⁵⁶ COMMISSION EUROPEENNE, préc., note 454.

⁴⁵⁷ La date d'entrée en vigueur a été fixée à septembre 2025.

de telle sorte que les données relatives auxdits produits et les données relatives aux services connexes, y compris les métadonnées pertinentes nécessaires à l'interprétation et à l'utilisation de ces données, sont, par défaut, accessibles à l'utilisateur, de manière aisée, sécurisée, sans frais, dans un format complet, structuré, couramment utilisé et lisible par machine, et sont, lorsque cela est pertinent et techniquement possible, directement accessibles à l'utilisateur⁴⁵⁸.

À la demande de l'utilisateur, le détenteur de données doit les mettre à la disposition d'un tiers, sans retard, dans un format facilement accessible, sans frais pour l'utilisateur, en continu et en temps réel⁴⁵⁹. Le tiers qui reçoit ces données a certaines obligations aussi⁴⁶⁰. De plus, le détenteur de données doit communiquer plusieurs renseignements à l'utilisateur avant l'achat du bien, notamment sur le type, le format et le volume des données que le produit est capable de générer, si la génération est en temps réel, des modalités du stockage des données et la manière dont l'utilisateur peut y accéder⁴⁶¹.

5.6.4 Analyse

Le Massachusetts, l'Europe et même l'Australie disposent d'une législation sur le droit à la réparation plus poussée que celle du Canada, sauf le Québec. Chacune de ces législations a adopté une approche différente. L'approche australienne est la plus limitée, puisqu'elle garantit uniquement l'accès des réparateurs, et non des consommateurs, aux informations de diagnostic, et exclut les données sans fil. La situation américaine est en évolution et la majeure partie du droit de réparation du pays est régie par un accord non contraignant qui ne prévoit qu'un accès indirect et limité aux données télématiques. À l'ère de la voiture connectée, ces solutions nous semblent inadéquates. Dans les deux cas, le consommateur ou le mécanicien indépendant n'a pas accès aux données de réparation sur un pied d'égalité avec le fabricant.

La loi de 2020 du Massachusetts et la législation de l'Union européenne, en revanche, nous semblent plus prometteuses. Les deux prévoient spécifiquement l'obligation de donner aux propriétaires de véhicules et aux tiers qu'ils désignent l'accès aux données télématiques d'une manière normalisée. En ce sens, la législation ressemble à celle du Québec, mais elle va un peu plus loin, d'une manière qui semble avantageuse pour les

⁴⁵⁸ *Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (Règlement sur les données)*, PE/49/2023/REV/1, art. 3(1).

⁴⁵⁹ *Id.*, art. 5(1)

⁴⁶⁰ *Id.*, art. 6.

⁴⁶¹ *Id.*, p. 3(2). La *Directive (UE) 2019/771 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de vente de biens, modifiant le règlement (UE) 2017/2394 et la directive 2009/22/CE et abrogeant la directive 1999/44/CE*, PE/27/2019/REV/1 contient également des dispositions qui s'appliquent aux véhicules connectés. Elle prévoit notamment l'obligation des fabricants de « fournir des mises à jour, y compris des mises à jour de sécurité, pour faire en sorte que les biens comportant des éléments numériques restent conformes » (considérant 30 ; article 7). Nous n'avons pas poussé plus loin l'étude de cette directive afin de ne pas nous éloigner des préoccupations qui sont au cœur de notre recherche.

consommateurs. Toutes deux prévoient spécifiquement un accès direct par le consommateur, c'est-à-dire sans intervention (ou avec une intervention minimale) du fabricant. Il faut également souligner que la loi du Massachusetts prévoit l'obligation de donner aux mécaniciens indépendants la possibilité d'envoyer des commandes au véhicule, ce qui pourrait permettre de lever des restrictions logicielles sur les réparations et règle certainement la question de réinitialisation avant ou à la suite de l'ajout ou du remplacement de pièces.

Cette approche semble répondre au risque que les concessionnaires et fabricants conservent un monopole sur les données diagnostiques et ainsi, sur la réparation. Nous notons toutefois que rien dans la législation n'interdit aux fabricants de collecter et d'utiliser également ces données. Ainsi, bien que les lois accordent aux consommateurs des droits plus importants sur les données de leur véhicule et de diagnostic, on ne peut pas dire que ces droits soient des droits de propriété ou de contrôle exclusifs.

Ces lois n'ayant été adoptées ou mises en vigueur que récemment, leurs effets réels restent à déterminer. Nous considérons qu'il serait judicieux que les décideurs politiques canadiens suivent de près leur mise en œuvre.

5.7 Faits saillants

Dans cette section, nous avons examiné l'adéquation du cadre législatif quant aux risques et préoccupations en lien avec la protection de la vie privée et le droit à la propriété, y compris le droit à la réparation en ce qui concerne les biens numériques.

Vie privée

Notre examen de la législation canadienne en matière de protection de la vie privée nous amène à deux conclusions principales : premièrement, les fabricants automobiles semblent ne pas respecter certains éléments de la législation canadienne sur la protection de la vie privée et, deuxièmement, la législation actuelle n'est pas adaptée pour faire face aux risques identifiés. Notamment :

- Plusieurs des lois canadiennes n'ont pas de définition adéquate de dépersonnalisation ou d'anonymisation, ce qui laisse la porte ouverte aux entreprises de prétendre que les données sont anonymisées et donc pas assujetties aux restrictions législatives ou contractuelles ;
- Les lois n'imposent que très peu de limites sur la collecte de renseignements personnels ou les objectifs de la collecte ; ces limites sont contextuelles et donc quelque peu floues, et ne peuvent être évaluées qu'une fois que la pratique est déjà en vigueur ;
- Les limites semblent inadéquates pour mitiger les risques liés au partage de données et à l'agrégation, l'utilisation et la revente des données par des entreprises tierces.

En ce qui concerne le consentement :

- Rien dans la loi n'oblige le fabricant à obtenir un consentement exprès dans la plupart des cas. Le consentement implicite peut donc être présumé par le fabricant

- dans plusieurs circonstances prévues dans les lois. Dans certains instruments juridiques, le consentement n'est même pas requis dans certaines circonstances ;
- Le consentement éclairé dans ce contexte est quasiment impossible à obtenir, compte tenu de la complexité de la technologie et du nombre d'acteurs impliqués ;
 - Le consentement est donc une mesure de protection insuffisante qui doit être renforcée par d'autres ;

D'autres mesures de protection qui pourraient combler les lacunes dans la législation comprennent l'établissement de normes de base en matière de protection de la vie privée (par exemple, certains types de collecte, d'utilisation et de partage de renseignements personnels sont spécifiquement interdits) et l'obligation de mettre en œuvre des principes de protection de la vie privée dès la conception.

En ce qui concerne de potentielles violations de la loi par les fabricants :

- Toutes les lois canadiennes indiquent que le consentement ne peut être exigé à des fins qui ne sont pas nécessaires pour avoir accès au bien ou au service. Toutefois, la littérature suggère que les fabricants automobiles n'offrent aucune possibilité ou occasion de refuser la collecte ou l'utilisation de données non nécessaires, sans refuser l'accès au service.
- Au Québec, l'organisme doit assurer que la collecte (ou autre) de données non nécessaires est refusée par défaut. Nous nous demandons si cette exigence est respectée, étant donné le constat précédent.
- Les renseignements potentiellement personnels sont collectés sur des personnes qui n'ont jamais eu l'occasion de donner leur consentement, comme les passagers et les piétons.

Au vu de cette analyse, des risques identifiés dans la section 3 et des constats du sondage et des entrevues rapportés dans la section 4, nous sommes d'avis que l'encadrement législatif actuel est inadéquat. Tout comme le législateur a imposé des limites et obligations aux fabricants en ce qui concerne d'autres aspects des véhicules, tels que les dispositifs de sécurité, les émissions, la pollution, etc., il nous semble logique de mettre en place des protections et règlements qui limitent la collecte, l'utilisation et le partage des données.

La propriété

Les deux systèmes de droit privé canadiens prévoient la possibilité de diviser la propriété d'un bien de la propriété intellectuelle de son logiciel. Ce concept juridique permet au fabricant de garder les droits de propriété du logiciel d'un bien, et ainsi de garder un contrôle sur le bien par le biais de son logiciel même après sa vente ou location au consommateur. Cette division juridique est souvent effectuée par l'utilisation des contrats de licence d'utilisateur final (CLUF), qui énoncent que le logiciel appartient au fabricant et que ce dernier réserve des droits sur son utilisation.

La *Loi sur le droit d'auteur* (LDA) canadienne permet l'utilisation des CLUF. De plus, cette loi interdit le contournement des verrous logiciels (MTP) qui peuvent limiter l'accès au logiciel ou son utilisation, même si l'accès était autrement permis par la loi. Ce faisant, la LDA ne mitige pas les risques aux droits de propriété identifiés ; au contraire, elle permet

aux fabricants d'adopter des pratiques que nous avons identifiées comme désavantageuses pour les consommateurs.

C'est dans ce contexte que les projets de loi C-244 et C-294 ont été adoptés par le législateur fédéral en 2024 afin de réduire des barrières à la réparation créées par ce cadre juridique. Le premier prévoit une exemption aux règles de contournement des MTP en cas de réparation ou d'entretien d'un produit, y compris tout diagnostic connexe. Le projet de loi C-294 modifie quant à lui la LDA pour élargir l'exception d'interopérabilité afin de permettre le contournement d'une MTP pour rendre un programme d'ordinateur ou un dispositif dans lequel il est intégré interopérable avec un autre programme d'ordinateur, un dispositif ou composant. Toutefois, il reste interdit de contourner une MTP pour des raisons de réparation si l'objectif est de fabriquer, importer, fournir, offrir ou mettre en circulation une telle technologie de contournement (sauf s'il s'agit d'un contournement pour des fins d'interopérabilité). Bien qu'il s'agisse d'un pas dans la bonne direction, nous avons ainsi des doutes sur l'utilité de ces modifications.

Une solution plus globale serait d'interdire l'utilisation des MTP qui limitent l'accès à une œuvre, ou au minimum, d'éliminer de la LDA l'interdiction de contourner des MTP qui contrôlent l'accès à une œuvre. C'est-à-dire que la LDA devrait seulement protéger une MTP qui a pour effet de restreindre une utilisation de l'œuvre déjà interdite dans la Loi et non l'accès à une œuvre.

De plus, il nous semble essentiel de mettre des limites sur les clauses contractuelles dans les CLUF qui empiètent excessivement sur les droits de propriété ou autres droits d'usage du consommateur : par exemple, les clauses limitant la réparation, permettant au fabricant de retenir un contrôle du bien, de changer l'offre de service ou de mettre fin à distance à l'usage du bien.

Enfin, rien dans la législation canadienne n'aborde la question d'accès aux données de diagnostic, sauf les nouvelles dispositions de la loi québécoise sur le sujet. La *Loi sur la protection du consommateur* québécoise a été modifiée en 2023 avec l'adoption de plusieurs dispositions sur la réparation, y compris la réparation des automobiles. Les nouvelles dispositions obligent les fabricants automobiles à fournir des données diagnostiques du véhicule au propriétaire, au locataire à long terme ou à son mandataire dans un format lisible, et ce, à un prix raisonnable. Le législateur québécois a aussi adopté une disposition qui interdit formellement au fabricant automobile l'utilisation de techniques ayant pour effet de rendre plus difficile l'accès aux données de réparation ou d'entretien d'une automobile. De plus, le fabricant doit fournir des logiciels de diagnostic et leurs mises à jour pendant une durée raisonnable. Bien qu'il semble y avoir des lacunes dans certaines de ces dispositions, notamment en ce qui concerne l'accès aux logiciels de réparation, nous sommes d'avis que la Loi répond maintenant à certains des risques identifiés dans ce rapport. Il sera important de suivre sa mise en œuvre et d'adopter un régime similaire dans tout le pays.

L'encadrement international

Dans notre analyse de la situation internationale, nous avons constaté que plusieurs législations, notamment le Massachusetts et l'Union européenne, ont adopté des mesures

ciblées en matière de droit de la réparation des véhicules connectés. Au Massachusetts, la loi donne aux propriétaires des véhicules un accès direct par connexion à courte distance à une plateforme de données diagnostiques ouverte et normalisée, accès qu'ils peuvent partager avec un réparateur indépendant. En outre, les réparateurs indépendants seraient en mesure d'utiliser la plateforme pour envoyer des commandes au véhicule à des fins de réparation, d'entretien et de test de diagnostic.

Dans l'Union européenne, un règlement adopté en 2023 oblige les fabricants des objets connectés, y compris les voitures, à fabriquer le bien de telle sorte que les données relatives aux services connectés sont accessibles à l'utilisateur. Une autre directive oblige les fabricants des biens connectés à fournir les mises à jour requises pendant une certaine période.

Ces approches semblent répondre à certains risques identifiés en matière de réparation, notamment au risque que les concessionnaires et fabricants aient un monopole sur les données diagnostiques et se donnent ainsi un avantage indu sur la réparation des voitures connectées.

6 Analyse de données fournies par l'industrie

6.1 Introduction et méthodologie

Dans cette section, nous examinons les informations fournies aux consommateurs par les fabricants automobiles concernant les services connectés. L'objectif de cette recherche est de comprendre l'impact des services connectés sur les droits des consommateurs et d'évaluer la manière dont l'information est présentée à ces derniers. Nous essayons donc de comprendre la réalité de l'impact de ces services versus l'impression générale donnée aux consommateurs.

Pour ce faire, nous avons visité les sites Web canadiens de trois fabricants automobiles et examiné les informations présentées au premier coup d'œil aux consommateurs concernant les services connectés. Nous avons examiné la présentation des fonctionnalités des services connectés et leur impact sur la vie privée et les droits de propriété du consommateur. Nous avons ensuite comparé ces informations avec celles figurant dans les conditions d'utilisation de ces mêmes services.

Nous avons sélectionné trois fabricants automobiles pour ce volet de la recherche : Toyota, Ford et Tesla. Toyota et Ford ont été choisis parce qu'ils sont respectivement les fabricants japonais et américains les plus populaires selon notre sondage. Nous avons sélectionné Tesla parce qu'il s'agit d'une marque plus récente et que ses véhicules ont été conçus pour être connectés depuis le début, ce qui en fait un point de comparaison intéressant avec des constructeurs plus traditionnels comme Toyota et Ford.

6.2 Présentation des services connectés sur le site Web

Tout d'abord, nous avons examiné la présentation des services connectés sur les sites Web des trois fabricants. La présentation des services connectés varie considérablement d'un fabricant à l'autre. Les trois sites Web sont conçus principalement autour des modèles de véhicules : en accédant au site Web, l'utilisateur est invité à sélectionner un véhicule et à en savoir plus. Toutefois, Ford et Toyota proposent également à l'utilisateur d'autres options sur la page d'accueil, y compris un menu contenant un lien vers une page sur les services connectés. Le site Web de Tesla ne propose pas de menu de ce type ; pour en savoir plus, l'utilisateur doit sélectionner un véhicule.

Le site Web de Toyota présente l'information la plus claire et la plus détaillée sur les services connectés. Sa page⁴⁶² sur les services connectés fournit une liste de services, chacun avec un lien vers plus d'information. Lorsque l'utilisateur clique pour obtenir plus d'information sur le service, il se voit présenter quelques paragraphes de texte, suivis de notes de bas de page en petits caractères comprenant des mises en garde telles que :

- Les limites sur la disponibilité de la fonctionnalité dans certains modèles ;

⁴⁶² TOYOTA CANADA, préc., note 7.

- Les limites de la responsabilité de Toyota relativement à la fourniture des services connectés : le fait que les services connectés dépendent de la connexion à un réseau sans fil (4G) et que Toyota n'est pas responsable des interruptions de service du réseau cellulaire et des limites similaires en ce qui concerne le GPS, le dispositif télématique de la voiture, et « d'autres facteurs indépendants de la volonté de Toyota » ;
- Le fait que certaines applications utilisent une grande quantité de données mobiles et que les clients sont responsables de tous les frais associés à l'utilisation des données mobiles ;
- Le fait que les clients peuvent éprouver des problèmes de connectivité entre leur téléphone et leur véhicule à la suite des mises à jour.
- Une invitation à aller visiter la politique de confidentialité (avec un hyperlien) pour en savoir plus au sujet des pratiques en matière de collecte, d'utilisation, de partage et de conservation de données.

Et ainsi de suite. Même si nous doutons que les consommateurs lisent les petits caractères, nous constatons que ces informations suivent directement la description de chaque service connecté. Certaines de ces informations ont été reprises dans la FAQ du site Web sur les services connectés⁴⁶³.

Le site Web de Ford est conçu de la même manière, permettant à l'utilisateur d'accéder à une page sur les services connectés. Toutefois, nous avons trouvé qu'il était difficile de comprendre les services offerts et leurs limites, principalement en raison de la manière dont des services similaires sont présentés sous des noms de marque différents. Par exemple, la « connectivité haut de gamme de Ford » semble permettre la diffusion en continu de vidéo, de musique et de divertissement, des nouvelles et des jeux, alors que « l'ensemble connectivité Ford » propose un point d'accès sans fil, des produits de divertissements et des jeux et des cartes pour la navigation. La « navigation connectée » a sa propre page Web et semble être un service distinct, lié au système SYNC⁴⁶⁴. SYNC est à la fois le nom du système d'infodivertissement et, sur les anciens modèles, celui du système télématique. Sur les modèles plus récents, le système télématique est appelé FordPass Connect⁴⁶⁵, nom facilement confondu avec l'application mobile FordPass.

Néanmoins, l'utilisateur peut cliquer sur ces noms pour accéder à une page distincte pour chaque service, qui fournit davantage d'information sur le service et sur le modèle pour lequel il est disponible. Chaque page comporte également une FAQ, qui répond aux questions relatives au coût, à l'activation des services, à l'abonnement et à la collecte de

⁴⁶³ TOYOTA CANADA, « FAQ du Centre d'aide », en ligne :

<<https://www.toyota.ca/toyota/fr/about/connected-services/help-centre>> (consulté le 3 décembre 2024).

⁴⁶⁴ FORD MOTOR COMPANY, « Services connectés Ford », en ligne :

<<https://fr.ford.ca/technology/connected-services/>> (consulté le 3 décembre 2024).

⁴⁶⁵ FORD MOTOR COMPANY, « Qu'est-ce que FordPass® Connect*? », en ligne :

<<https://fr.ford.ca/support/how-tos/fordpass/fordpass-connect/quest-ce-que-fordpass-connect/>> (consulté le 3 décembre 2024).

données (renvoyant l'utilisateur à la politique de confidentialité). De même, la page Web de l'application mobile présente une vue d'ensemble des services connectés⁴⁶⁶.

Au bas de chaque page se trouve un onglet intitulé « avis juridiques ». L'ouverture de cet onglet permet d'accéder à une liste de 205 avis, en petits caractères. Étant donné que le consommateur doit non seulement faire défiler la page jusqu'en bas et ouvrir cet onglet, mais aussi lire plus de 200 éléments en petits caractères, portant sur une foule de sujets, pour accéder à cette information, nous n'avons pas considéré qu'il s'agit d'une information présentée aux consommateurs.

À première vue, c'est le site Web de Tesla qui présente le moins d'information sur les services connectés. Le site est principalement organisé par type de modèle. Nous avons choisi la Model S pour notre visite du site, ce qui nous a amenés à une page détaillant les caractéristiques du véhicule. Sur cette page, nous avons remarqué que l'accent n'est pas mis sur les fonctions connectées, mais plutôt sur l'écran, le confort, la connexion au cellulaire, les spécifications du véhicule, la batterie, la sécurité, l'autopilote, etc. Ce n'est qu'après avoir défilé jusqu'au bas de la page que nous avons trouvé une mention de la connectivité, dans une note de bas de page indiquant que « Certaines fonctionnalités du véhicule à forte consommation de données nécessitent au moins une connectivité standard, notamment les cartes, la navigation et les commandes vocales » avec un hyperlien vers une page du site Web qui porte sur les services connectés⁴⁶⁷.

Sur cette page se trouve un survol des services connectés disponibles dans les véhicules Tesla. Cette page contient également une FAQ, qui explique certaines des modalités du service, telles que les questions de paiement et d'abonnement, mais sans plus d'informations sur les services connectés eux-mêmes. Nous n'avons trouvé aucune référence à la vie privée ou à la collecte de données sur cette page, outre un hyperlien vers la politique de confidentialité et les mentions légales dans le pied de page.

Dans l'ensemble, l'expérience du site Web est simplifiée et nous ne nous sommes pas sentis bombardés par des petits caractères ou du jargon comme nous l'avons fait sur les autres sites Web ; pourtant, nous n'avons pratiquement rien appris sur les services connectés, la vie privée ou les limites au droit de propriété au cours de cette expérience.

Contrairement aux deux autres fabricants, Tesla permet de commander le modèle en ligne. Lorsque nous avons accédé à la page de commande, nous avons remarqué, directement au-dessus du bouton *Commander*, un petit avis indiquant ce qui suit :

En cliquant sur « commander », j'accepte l'Entente de commande du Model S, Conditions relatives aux accessoires et la Politique d'utilisation équitable des Superchargeurs. Pour en savoir plus sur la façon dont Tesla protège vos données, consultez notre Avis de confidentialité.

⁴⁶⁶ FORD MOTOR COMPANY, « FordPass® | Application de mobilité avec services connectés : soutien aux propriétaires Ford », en ligne : <<https://fr.ford.ca/support/category/fordpass/>> (consulté le 12 décembre 2024).

⁴⁶⁷ TESLA INC., « Connectivité : Soutien », en ligne : <https://www.tesla.com/fr_ca/support/connectivity> (consulté le 15 février 2025).

Nous examinerons ces documents plus en détail dans la section suivante.

6.3 Conditions d'utilisation : les documents examinés

Chaque fabricant que nous avons étudié dispose de plusieurs politiques et autres documents faisant référence à des conditions d'utilisation ou ayant un impact sur les droits des consommateurs, tels que les politiques d'utilisation de leurs renseignements personnels. Nous n'avons pas toujours eu accès à toutes les conditions, car certaines d'entre elles semblent n'être disponibles qu'au moment de l'achat du véhicule ou de son couplage avec l'application mobile.

Pour Toyota, nous avons examiné le document intitulé *Conditions d'utilisation des services connectés*, qui contient une liste des autres documents qui font partie d'« une entente plus vaste régissant notre prestation de services » : 1) l'entente relative aux services chez le concessionnaire⁴⁶⁸, 2) l'avis de confidentialité⁴⁶⁹ 3) le contrat de licence d'utilisateur final du logiciel du véhicule (« le CLUF »)⁴⁷⁰ et 4) toute condition supplémentaire conformément aux conditions dans les *Conditions d'utilisation*⁴⁷¹. Nous avons examiné tous les documents, sauf le quatrième (qui ne porte pas de nom), ainsi qu'un manuel d'utilisateur pour la Toyota Corolla 2024⁴⁷². Ford ne fournit pas de liste de ce type : nous avons donc

⁴⁶⁸ TOYOTA CANADA, *Entente relative aux Services connectés*, 2024, en ligne : <Téléchargeable sur la page <https://www.toyota.ca/toyota/fr/privacy#/al/connected-services-privacy-notice>> (consulté le 25 février 2025).

⁴⁶⁹ TOYOTA CANADA ET TOYOTA CREDIT CANADA, « Politique de confidentialité », *Toyota Canada*, en ligne : <<https://www.toyota.ca/toyota/fr/privacy>> (consulté le 25 février 2025).

⁴⁷⁰ TOYOTA, *Logiciel de véhicule Toyota, Contrat de licence d'utilisateur final (CLUF)*, en ligne : <https://s3.amazonaws.com/toyota.site/toyota-v5/tci-prod/toyota/media/pdf/privacy/2023/Toyota_EULA_fr.pdf?ck=02052025101339> (consulté le 25 février 2025).

⁴⁷¹ TOYOTA CANADA, *Conditions d'utilisation des services connectés du véhicule*, 15 novembre 2021, en ligne : <https://s3.amazonaws.com/toyota.site/toyota-v5/tci-prod/toyota/media/pdf/privacy/2021/Terms_of_Use_21MM_TCI_Toyota_fr.pdf> (consulté le 25 février 2025).

⁴⁷² TOYOTA, *Manuel du propriétaire : Corolla 2024*, 2023, en ligne : <<https://www.toyota.ca/content/dam/toyota/documents/manuals/fr/OM02684D/OM02684D.pdf>>; TOYOTA, *Manuel multimédia du propriétaire : Corolla 2024*, 2023, en ligne : <<https://www.toyota.ca/content/dam/toyota/documents/manuals/fr/OM02686D/OM02686D.pdf>>.

examiné la politique de confidentialité générale⁴⁷³ ainsi que le CLUF⁴⁷⁴ et le manuel du véhicule pour un modèle choisi au hasard (le VUS Escape Active 2025)⁴⁷⁵.

En ce qui concerne Tesla, nous avons examiné les quatre documents affichés à la caisse avant la conclusion de la transaction en ligne pour un Modèle S : l'Entente de commande du Model S⁴⁷⁶, les Conditions relatives aux accessoires⁴⁷⁷, la Politique d'utilisation équitable des Superchargeurs⁴⁷⁸ et l'Avis de confidentialité⁴⁷⁹. Nous avons également examiné le manuel d'utilisateur pour la Model S et la page des « Ressources supplémentaires⁴⁸⁰ », où nous avons trouvé d'autres politiques, telles que la « promesse relative aux brevets » et une « entente pour l'abonnement à la connectivité haute de gamme ». Tesla dispose également d'une deuxième page Web concernant la protection de la vie privée, qui donne une vue d'ensemble plus simple de certains points et contient une brève vidéo⁴⁸¹.

⁴⁷³ FORD MOTOR COMPANY, « Politique de confidentialité de Ford », en ligne :

<<https://fr.ford.ca/help/privacy/>> (consulté le 25 février 2025).

⁴⁷⁴ FORD MOTOR COMPANY, *2025 Escape Manuel du Propriétaire : Informations client: Contrat de licence de l'utilisateur final*, en ligne :

<https://www.fordservicecontent.com/Ford_Content/vdirsnet/OwnerManual/Home/Content?countryCode=CAN&languageCode=FR&Uid=G2154206&ProcUid=G2136215&div=f&variantid=10278&vFilteringEnabled=False&userMarket=CAN&buildtype=web> (consulté le 31 mars 2025).

⁴⁷⁵ FORD MOTOR COMPANY, « 2025 Escape Manuel du Propriétaire », en ligne :

<https://www.fordservicecontent.com/Ford_Content/vdirsnet/OwnerManual/Home/Index?Variantid=10278&languageCode=FR&countryCode=CAN&VIN=&userMarket=CAN&div=f&buildtype=web> (consulté le 28 février 2025). Nous n'avons pas trouvé de politique canadienne sur les conditions d'utilisation des services connectés. Nous avons trouvé une politique équivalente américaine, mais nous n'avons pas fait l'analyse du document, en supposant qu'elle ne s'applique pas au marché canadien : FORD MOTOR COMPANY, « Ford Connectivity Package Terms and Conditions », en ligne : <<https://www.ford.com/support/how-tos/ford-technology/ford-connected-services/ford-connectivity-package-terms-and-conditions/>> (consulté le 31 mars 2025).

⁴⁷⁶ TESLA INC., *Convention d'achat pour Véhicule à Moteur : Conditions*, 2024.

⁴⁷⁷ TESLA INC., « Boutique Tesla : Soutien », en ligne :

<https://www.tesla.com/fr_ca/support/shop> (consulté le 1 avril 2025).

⁴⁷⁸ TESLA INC., « Conditions », en ligne : <https://www.tesla.com/fr_ca/legal/terms> (consulté le 1 avril 2025).

⁴⁷⁹ TESLA INC., « Avis de confidentialité », en ligne : <https://www.tesla.com/fr_ca/legal/privacy> (consulté le 1 avril 2025).

⁴⁸⁰ TESLA INC., « Ressources supplémentaires », en ligne :

<https://www.tesla.com/fr_ca/legal/additional-resources> (consulté le 1 avril 2025).

⁴⁸¹ TESLA INC., « Privacy », en ligne : <https://www.tesla.com/fr_ca/privacy> (consulté le 1 avril 2025).

6.4 Politique de confidentialité

6.4.1 Survol

Dans tous les cas, la politique de confidentialité constitue une condition d'utilisation des services connectés que l'utilisateur doit accepter au préalable. Nous avons donc examiné les politiques de confidentialité de ces fabricants en matière de connectivité et de services connectés. Toutefois, comme nous avons déjà examiné les travaux d'autres chercheurs à cet égard (section 3), nos commentaires sur ces politiques seront brefs. Nos observations vont généralement dans le sens des conclusions de l'enquête de 2023 de la Fondation Mozilla, selon lesquelles les fabricants des voitures connectées collectent des quantités massives de données, dont certaines sont très sensibles, les utilisent et les partagent pour une multitude d'objectifs vaguement définis, avec peu de limites à la collecte, à l'utilisation, à la conservation ou au partage.

Les politiques nous ont semblé assez complètes, celles de Tesla et Toyota étant plus claires et celle de Ford moins claire et plus large.

Collection et utilisation des renseignements personnels

Chacune des politiques de protection de la vie privée fournit un aperçu des types de renseignements personnels collectés et de l'utilisation de ces informations. Dans tous les cas, les politiques indiquent que des données peuvent être collectées sur l'utilisateur, son véhicule (numéro d'identification du véhicule, etc.) et ses interactions avec le fabricant. Les fabricants collectent et utilisent également des données de réparation et de diagnostic, des données de conduite (vitesse, accélération, freinage, etc.), des données d'utilisation de l'infodivertissement et des services connectés. Les politiques expliquent les raisons pour lesquelles ces données sont collectées, qui vont d'utilisations spécifiques (telles que la fourniture d'un certain service connecté) à des utilisations génériques et larges, telles que l'amélioration des services.

Tesla est la seule des trois entreprises qui déclare explicitement qu'elle n'enregistre pas l'historique des localisations et qu'elle n'y ait pas accès, sauf à des données partielles en cas d'accident. Elle indique également qu'elle recueille des informations partielles sur la localisation (les segments de la route) à des fins d'analyse de la fonction de pilotage automatique, collecte que le consommateur peut choisir d'accepter ou de refuser. Elle déclare aussi qu'elle n'associe pas l'identité de la personne aux données du véhicule, et que ces données sont inaccessibles à Tesla sauf si la voiture requiert un entretien ou une réparation ou en cas d'accident et si l'utilisateur donne son consentement. La politique précise également que les autres données, telles que celles capturées par les caméras ou les commandes vocales, sont stockées uniquement dans la voiture, à moins que l'utilisateur ne consente à les partager avec Tesla. La politique de Toyota indique que les données d'identification faciale ne seront enregistrées que sur le véhicule. Pour le reste, nous avons constaté que les collectes et les utilisations sont relativement illimitées.

De plus, les conditions d'utilisation des services connectés de Toyota mentionnent une utilisation dont nous n'avons pas relevé de mention ailleurs :

*Localisation de votre véhicule dans le cadre d'une location ou d'un financement.
Si vous louez ou financez votre véhicule par notre intermédiaire ou celui de l'une*

de nos sociétés affiliées, et que vous avez violé de manière substantielle l'une des conditions des ententes régissant cette location ou ce financement, nous pouvons utiliser les services pour vous localiser ou localiser le véhicule dans le but de communiquer avec vous et/ou de récupérer le véhicule. VOUS CONSENTEZ EXPRESSÉMENT À CE QUE NOUS UTILISONS LES SERVICES DE CETTE MANIÈRE⁴⁸².

Partage de données

Tesla souligne qu'elle ne partage pas d'informations identifiables avec des tiers sans le consentement de l'utilisateur. Toyota déclare également qu'elle ne partage pas les informations du compte de l'utilisateur avec des revendeurs de données, des publicitaires, des assureurs (sauf avec le consentement explicite de l'utilisateur) ou des plateformes de médias sociaux. Cependant, tous les fabricants déclarent qu'ils partagent des données avec d'autres fournisseurs de services ou affiliés, ce qui inclut le partage d'informations à des fins de marketing. Aucune des politiques ne nomme explicitement les fournisseurs de services susceptibles d'avoir accès aux données. Les données peuvent également être partagées lorsque la loi l'exige, ou, dans le cas de Toyota, lorsque la loi le *permet*. Les politiques précisent toutes que les données peuvent être transférées hors du Canada, notamment aux États-Unis.

Conservation des données

Seule Toyota indique une durée précise de conservation des renseignements personnels. Les deux autres fabricants font des déclarations plus générales, en indiquant par exemple qu'ils ne conservent les données à caractère personnel que « le temps nécessaire à la réalisation des objectifs pour lesquels elles ont été recueillies⁴⁸³ ».

Consentement et refus de la collecte de données

La politique de Tesla ne mentionne pas ce qui constitue un consentement, mais nous avons noté que le fait de passer à la caisse lors de l'achat d'un véhicule requiert le consentement à la politique dans son ensemble. La politique mentionne que certains actes requièrent l'accord de l'utilisateur ou un consentement supplémentaire, par exemple le partage de données vidéo à partir du véhicule avec le fabricant. L'utilisateur peut contrôler certains paramètres de collecte de données à partir du véhicule. N'ayant pas accès au véhicule, nous n'avons pas été en mesure de déterminer dans quelle mesure l'utilisateur peut contrôler ces paramètres, au-delà de l'activation ou du refus de l'analyse des données comme les données de segment de route.

Pour renoncer totalement à la collecte de données, l'utilisateur doit communiquer avec Tesla pour désactiver la connectivité, ce qui signifie qu'aucun service connecté ne fonctionnera et que la politique prévient, « il nous sera impossible de connaître ou de vous informer en temps réel des problèmes concernant votre véhicule. Cela peut entraîner la réduction des fonctionnalités de votre véhicule, des dommages graves ou des pannes⁴⁸⁴. »

⁴⁸² TOYOTA CANADA, préc., note 471, art. 13(c).

⁴⁸³ TESLA INC., préc., note 479.

⁴⁸⁴ *Id.*

La politique de Ford déclare qu'« en nous fournissant vos informations ou en utilisant nos produits ou services, vous approuvez notre politique de confidentialité. Si vous n'approuvez pas notre politique de confidentialité, nous vous prions de ne nous fournir aucun renseignement personnel⁴⁸⁵ ». Nous ne comprenons pas comment l'utilisateur peut s'y prendre pour ne fournir aucun renseignement personnel, étant donné que l'achat du véhicule nécessite un échange d'information. La politique indique que l'utilisateur peut modifier certains paramètres de collecte de données à partir du véhicule et le manuel du véhicule indique que le modem télématique peut être désactivé. Toutefois, la politique met le consommateur en garde contre cette pratique : « Veuillez garder à l'esprit que la déconnexion du véhicule ou l'application de modifications aux réglages de partage de données peut avoir des répercussions sur la qualité ou la disponibilité de certains services⁴⁸⁶ ».

La politique de Toyota stipule que les véhicules vendus avant 2023 ont été accompagnés d'instructions permettant de désactiver les services connectés et la collecte de données, mais que tous les véhicules vendus après le 22 septembre 2023 sont livrés en « Mode privé ». Les utilisateurs de ces véhicules doivent activer la collecte en utilisant l'application Toyota ; ensuite, la politique déclare : « en acceptant de recevoir les services, vous avez expressément consenti à la collecte⁴⁸⁷ ». Malgré cela, le document de l'Entente de services de 2024 indique qu'il n'est pas possible d'interrompre la transmission de données du véhicule sans parler à un agent et sans renoncer aux services connectés, et ce, même si la personne coche la boîte sur l'entente pour le refuser et pour indiquer qu'elle ne souhaite pas activer les services connectés dans son véhicule.

Autres utilisateurs et passagers

Les politiques de Ford et de Toyota mentionnent toutes deux que l'utilisateur a la responsabilité d'informer les autres utilisateurs et les passagers de la collecte et de l'utilisation des données du véhicule. Nous n'avons pas trouvé de telle déclaration dans les documents de Tesla.

Renseignements dépersonnalisés ou anonymisés

Les trois fabricants réservent le droit d'utiliser des données anonymes ou dépersonnalisées à n'importe quelle fin. Ford déclare qu'elle peut dépersonnaliser les données des utilisateurs et « utiliser ces renseignements sous cette forme à quelque fin que ce soit⁴⁸⁸ ». Toyota indique qu'elle peut « anonymiser ou cumuler les renseignements personnels collectés auprès de vous et utiliser ces renseignements anonymisés et agrégés à des fins d'analyse de données, de recherche et autres », et ce, même « à la suite de votre demande de suppression de vos informations personnelles⁴⁸⁹ ». La politique de Tesla indique que

Tesla peut également recueillir, utiliser et partager de l'information qui, à elle seule, ne permet pas de vous identifier personnellement. Une telle information peut être utilisée à quelque fin que ce soit, y compris notamment à des fins opérationnelles

⁴⁸⁵ FORD MOTOR COMPANY, préc., note 473.

⁴⁸⁶ *Id.*

⁴⁸⁷ TOYOTA CANADA ET TOYOTA CREDIT CANADA, préc., note 469.

⁴⁸⁸ FORD MOTOR COMPANY, préc., note 473.

⁴⁸⁹ TOYOTA CANADA ET TOYOTA CREDIT CANADA, préc., note 469.

ou de recherche, à des fins d'analyse sectorielle, pour améliorer ou modifier nos produits et services, pour mieux adapter nos produits et services à vos besoins, et là où la loi l'exige⁴⁹⁰.

Responsabilité, sécurité, conformité

Toutes les politiques indiquent les coordonnées du responsable de la protection de la vie privée au sein de l'entreprise, que le consommateur peut contacter s'il a des questions ou pour faire corriger des erreurs. Toutes les politiques mentionnent des mesures de sécurité pour la protection des données.

6.4.2 Analyse

Nous constatons une grande divergence entre les informations présentées au consommateur sur les sites Web et les informations contenues dans les conditions d'utilisation. En effet, les sites Web n'affichent pratiquement aucune information sur les pratiques des fabricants concernant la collecte de données à l'intention des consommateurs en dehors de leur politique de protection de la vie privée. Ford et Toyota renvoient les consommateurs vers la politique dans leurs FAQ, mais sinon, nous n'avons pas remarqué de références à la collecte, l'utilisation ou le partage de renseignements personnels intégrés dans les sites Web des fabricants. Nous n'avons trouvé un lien vers la politique de confidentialité de Tesla qu'au moment du paiement, et nous n'avons vu aucune mention de la confidentialité avant cela, sauf l'hyperlien vers l'avis de confidentialité dans le pied de page.

Dans l'ensemble, nous remarquons que les politiques de protection de la vie privée des fabricants illustrent la faiblesse de la législation canadienne actuelle en matière de protection de la vie privée. Sans procéder à une analyse juridique complète pour déterminer si ces politiques sont conformes à la législation canadienne, nous constatons qu'elles répondent généralement à un grand nombre des exigences juridiques mentionnées dans la section 5.1 ci-dessus, mais qu'elles présentent néanmoins de graves risques pour le droit à la vie privée des consommateurs. Nous avons donc été frappés par les limites inhérentes à ce type de document en tant que forme de protection des consommateurs, notamment pour les raisons suivantes :

- **Manque de lisibilité** : les politiques sont legalistes et longues.
- **Absence de protections claires** : même si une section de la politique semble claire, d'autres parties semblent vagues. Par exemple, que signifie conserver les données « aussi longtemps que nécessaire » ou une promesse de « ne partager les données qu'avec des partenaires ou des affiliés » ? Que signifient ces garanties de protection de la vie privée si toutes ces entreprises peuvent utiliser des données « anonymes » ou dépersonnalisées sans restriction ? Avec des notions aussi vagues, comment un consommateur peut-il évaluer si la politique a été violée ?
- **Mise en œuvre impossible** : même si un consommateur comprenait clairement ses droits, comment pourrait-il savoir s'ils sont violés, sauf en cas de fuite

⁴⁹⁰ TESLA INC., préc., note 479.

- importante de données ? Sans accès à une connaissance de l'intérieur des pratiques de collecte, de l'utilisation et du partage de renseignements personnels, le respect de ces politiques est impossible à évaluer et donc à faire respecter.
- **Peu de limites à ce que les entreprises peuvent faire avec les données** : pour autant qu'elles le mentionnent dans leurs politiques. Par exemple, rien n'empêche une entreprise de vendre des données à un courtier de données, pour autant que cela figure dans sa politique.
 - **Peu de choix** : Le consommateur doit consentir à l'ensemble de la politique afin d'avoir accès aux services intégrés dans son véhicule. Nous applaudissons le fait que tous les fabricants ont intégré des paramètres qui permettent à l'utilisateur de contrôler certains aspects de la collecte de données à partir de leurs véhicules ; malheureusement, nous ne sommes pas en mesure d'évaluer l'ampleur de cette protection.

6.5 Conditions affectant le droit de propriété de l'utilisateur

6.5.1 Survol

Nous avons examiné de nombreux documents pour mieux comprendre l'impact de la connectivité et des services connectés sur les droits d'usage propriété de l'utilisateur sur le véhicule : manuels de propriété, CLUF, conditions d'utilisation de services connectés et d'autres politiques et conditions d'achat liées à la propriété intellectuelle.

Obsolescence et limites d'utilisation

Les conditions d'utilisation des services connectés de Toyota mentionnent que « les services sont susceptibles d'être modifiés ou interrompus » et que Toyota se réserve le droit de modifier, de limiter l'utilisation ou de cesser d'offrir l'un des services à tout moment, notamment en raison d'actions de fournisseurs de services tiers ou « des modifications de la technologie sans fil/GPS sous-jacente ou de soutien⁴⁹¹ ». En effet, le document indique que les véhicules Toyota qui dépendent de la technologie de réseau 3G perdront plusieurs fonctions et auront des fonctionnalités limitées lors du retrait de ce réseau. Le document indique les modèles affectés, y compris certains de l'année modèle 2020⁴⁹².

Tesla mentionne dans au moins deux documents⁴⁹³ qu'elle ne garantit pas tous les aspects nécessaires au maintien de la connectivité, notamment le réseau cellulaire. L'entente de commande indique que « les fonctionnalités incluses avec la Connectivité haut de gamme sont sujettes à modification et elles peuvent être limitées ou indisponibles en raison de matériel désuet », par exemple, causé par le changement du réseau de télécommunications⁴⁹⁴.

Mises à jour

⁴⁹¹ TOYOTA CANADA, préc., note 471.

⁴⁹² *Id.*, art. 11.

⁴⁹³ TESLA INC., préc., note 480 : Entente pour l'abonnement à la connectivité haut de gamme et entente de commande.

⁴⁹⁴ TESLA INC., préc., note 476.

La convention d'achat de Tesla indique aussi que le fabricant fournit des mises à jour régulièrement par Wi-Fi, mais qu'elle peut cesser de fournir des mises à jour pour un véhicule selon plusieurs facteurs, tels que son paramétrage ou son âge. Tesla déclare ne pas être responsable du coût de la mise à niveau d'un véhicule pour qu'il puisse continuer à recevoir les mises à jour dans ce cas ni de tout problème survenant après l'installation d'une mise à jour en raison de « matériel désuet ou endommagé ou d'un mauvais fonctionnement (sauf dans les cas couverts par votre garantie)⁴⁹⁵ ».

Dans son CLUF, Ford indique que l'utilisateur reconnaît que Ford ou ses affiliés peuvent « vérifier automatiquement la version ou les composants du LOGICIEL que vous utilisez et [...] fournir des mises à jour ou des ajouts au LOGICIEL automatiquement téléchargeables dans vos APPAREILS⁴⁹⁶ ».

Le CLUF de Toyota indique que l'utilisateur est responsable d'installer les mises à jour et que, s'il ne le fait pas, certaines fonctions peuvent être désactivées. De plus, certaines mises à jour peuvent modifier la fonctionnalité des systèmes⁴⁹⁷.

Modification unilatérale

Les conditions d'utilisation des services connectés de Toyota déclarent que la fourniture des services peut être modifiée ou annulée à tout moment et pour n'importe quelle raison. Le fabricant peut mettre fin aux services connectés « sans motif », comme en cas de désuétude de réseau, après un préavis de 30 jours, ou « avec motif », par exemple, « si vous enfrez quelque partie que ce soit de la présente entente⁴⁹⁸ ». L'entreprise se réserve également le droit de modifier n'importe quel élément du contrat et déclare que le seul recours de l'utilisateur qui refuse ces changements est d'annuler le service⁴⁹⁹. Le CLUF indique : « Vous reconnaissez que Toyota se réserve le droit d'interrompre le Logiciel ou les Services, en tout ou en partie, en tout temps⁵⁰⁰ ». Puisque le « Logiciel » réfère à tout logiciel « installé à l'origine par ou au nom de Toyota sur votre Véhicule », nous comprenons que cette clause s'applique au véhicule complet.

Le CLUF de Ford mentionne que « Sous réserve de tout autre droit, FORD MOTOR COMPANY peut résilier ce CLUF si vous ne vous conformez pas à ses conditions ». Ford se réserve également le droit « de cesser d'offrir, sans responsabilité d'aucune sorte, tout service sur Internet qui vous est fourni ou auquel on vous donne accès par l'utilisation du LOGICIEL⁵⁰¹ ». Étant donné que la définition du LOGICIEL dans le CLUF réfère aux logiciels installés à « plusieurs appareils, y compris SYNC® et différents modules de commande », il nous semble que ces clauses réfèrent à l'ensemble des logiciels du véhicule, incluant le logiciel des fonctionnalités connectées.

La politique de Tesla est beaucoup plus restreinte. Elle indique que l'entreprise peut suspendre ou annuler un abonnement à la connectivité haut de gamme seulement si le

⁴⁹⁵ *Id.*

⁴⁹⁶ FORD MOTOR COMPANY, préc., note 474.

⁴⁹⁷ TOYOTA, préc., note 470, art. 9.

⁴⁹⁸ TOYOTA CANADA, préc., note 471, art. 8(a) et (b).

⁴⁹⁹ *Id.*, art. 10(b).

⁵⁰⁰ TOYOTA, préc., note 470.

⁵⁰¹ FORD MOTOR COMPANY, préc., note 474.

service est utilisé pour des raisons d'utilisation non autorisée ou inappropriée ou si la personne arrête de payer⁵⁰².

Limites sur la réparation

Nous n'avons pas trouvé des références aux limites sur le droit à la réparation dans les documents examinés. Pourtant, les CLUF de Ford et de Toyota interdisent l'ingénierie inverse, la décompilation et le désassemblage, sauf si l'activité est expressément permise par la loi applicable.

Propriété intellectuelle

Le CLUF de Ford déclare que l'utilisateur est autorisé à utiliser le logiciel sur l'appareil (la voiture et ses systèmes), mais que le logiciel est concédé sous licence et qu'il n'est pas vendu. Ainsi, le consommateur ne peut pas copier le logiciel ni le distribuer, le modifier, le transférer, etc.

La politique des services connectés de Toyota indique que « Les services ne vous ont pas été et ne vous sont pas vendus. Au contraire, sous réserve du respect de l'entente, il vous est accordé une licence limitée, non exclusive et révocable pour utiliser les services uniquement dans la mesure où nous ou les fournisseurs de services les rendons disponibles par le biais du système et/ou du logiciel⁵⁰³ ». Le CLUF contient des déclarations similaires.

Tesla se distingue des deux autres par l'absence d'un CLUF et nous n'avons pu trouver nulle part de déclaration selon laquelle l'utilisateur n'est pas propriétaire du logiciel. Au contraire, l'entreprise désigne une partie de son code source ouvert (*open source*), bien que certains logiciels soient néanmoins brevetés. L'entreprise a fait une déclaration juridiquement contraignante dans une « Promesse relative aux brevets », qui déclare que Tesla « n'intentera aucune poursuite judiciaire en matière de brevets contre toute personne qui utilise sa technologie de bonne foi ». La politique explique qu'un tiers agit en toute bonne foi s'il ne profite pas ou n'a pas d'intérêt financier dans la propriété intellectuelle utilisée, ne conteste pas les brevets de Tesla et ne met pas en marché toute imitation de produit Tesla⁵⁰⁴.

6.5.2 Analyse

Encore une fois, nous avons constaté une grande différence entre les informations présentées aux consommateurs sur les sites Web des fabricants et celles figurant dans les documents juridiques. Presque aucune information sur les restrictions de propriété ou l'obsolescence n'a été présentée aux consommateurs sur la partie non juridique du site Web. La seule mention que nous ayons vue de ces limites se trouvait dans les petits caractères affichés par Toyota dans la description de certains services connectés, notamment en ce qui concerne l'éventuelle obsolescence ou indisponibilité du service en cas de modification du réseau de télécommunications.

⁵⁰² TESLA INC., préc., note 480 : Entente pour l'abonnement à la connectivité haut de gamme.

⁵⁰³ TOYOTA CANADA, préc., note 471, art. 12(b).

⁵⁰⁴ TESLA INC., préc., note 480 : Promesse relative aux brevets.

Tesla semble imposer moins de restrictions aux droits des consommateurs que ses concurrents. Nous constatons que seule Tesla n'indique pas qu'elle peut modifier les fonctionnalités des services connectés au moyen de mises à jour, qu'elle peut mettre fin unilatéralement à l'accord de service pour quelque raison que ce soit, qu'elle est propriétaire du logiciel ou que l'ingénierie inverse est interdite.

Les contrats ont confirmé les risques que nous avons identifiés précédemment dans le rapport :

- Il existe un risque d'obsolescence de la technologie connectée qui n'est pas nécessairement assumé par le fabricant ;
- Les mises à jour sans fil peuvent modifier ou limiter les fonctionnalités qui existaient au moment de l'acquisition du véhicule.
- Certains fabricants se réservent le droit de cesser d'offrir les services connectés ou même le logiciel du véhicule ;
- Le fabricant peut utiliser la connexion sans fil pour surveiller l'utilisation du véhicule par l'utilisateur dans le cadre de l'application du CLUF.

Nous notons l'absence de clauses limitant les réparations, ce qui contraste avec les observations que nous avons faites à ce sujet dans la section 3. Cela nous amène à émettre l'hypothèse que la plupart des limites à la réparation sont dues à des verrous numériques et à une non-disponibilité d'informations de diagnostic, plutôt qu'à des clauses contractuelles restrictives.

6.6 Faits saillants

Dans cette section, nous avons examiné les sites Web et les politiques de Toyota, Ford et Tesla. Nous avons étudié la manière dont les services connectés sont présentés aux consommateurs et les conditions d'utilisation de ces services. Les conditions d'utilisation comprennent les politiques de confidentialité ainsi que les accords d'utilisation des services connectés, les contrats de licence de l'utilisateur final (CLUF), les mentions dans les manuels du propriétaire et d'autres documents liés à la vente du véhicule.

En examinant les politiques de protection de la vie privée, nous avons réaffirmé les conclusions d'autres chercheurs décrites dans la section 3, notamment le fait que les fabricants de voitures connectées collectent et utilisent de grandes quantités de renseignements personnels, qu'ils les partagent avec des sociétés affiliées et qu'ils les conservent pendant des périodes souvent imprécises. Les politiques sont longues et complexes et ne donnent généralement que de vagues garanties sur ce qui peut ou ne peut pas être fait avec les données, bien que la politique de Tesla comprenne pour sa part quelques engagements plus fermes. Le consentement est soit présumé de par l'utilisation du véhicule, soit donné par le consommateur au moment de la conclusion de la transaction avec le fabricant, ou donné au moment de l'inscription à l'application mobile. Les fabricants permettent aux utilisateurs de modifier les paramètres de confidentialité à l'intérieur du véhicule, mais pour refuser complètement la collecte de données, il faut parler à un représentant de l'entreprise et renoncer à tous les services connectés.

Nous n'avons trouvé pratiquement aucune de ces informations sur les sites Web des fabricants dans leurs descriptions des services connectés ; au mieux, ils ont fourni un lien vers leurs politiques de confidentialité.

En ce qui concerne les droits de propriété, nous avons noté que tous les fabricants font référence à l'obsolescence potentielle ou à l'indisponibilité éventuelle de la technologie basée sur le réseau de télécommunications. Toyota indique que certaines de ses technologies seront obsolètes avec le retrait du réseau 3G, prévu pour 2025, y compris pour les véhicules de 2020. Ford et Toyota se réservent l'intégralité des droits de propriété sur le logiciel et déclarent qu'elles peuvent à tout moment mettre fin aux services connectés ou même au CLUF (et donc au droit d'utilisation du logiciel du véhicule !). Elles indiquent également que les mises à jour peuvent modifier la fonctionnalité du logiciel ou des services connectés. Ford déclare qu'elle peut surveiller la version ou les composants du logiciel utilisé par l'utilisateur. Cela indique que la perte d'usage complète du véhicule ou la diminution de ses fonctionnalités est une possibilité réelle.

Les politiques de Tesla sont plus favorables à l'utilisateur ; l'entreprise met certains de ses logiciels en *open source* et s'engage à ne pas engager de poursuites en cas d'utilisation de bonne foi de l'un de ses brevets.

Hormis les références à l'obsolescence ou aux restrictions avec le réseau cellulaire, aucune de ces informations n'est présentée sur la description générale des services connectés ou des véhicules sur le site Web des fabricants.

Toyota et Ford interdisent toutes deux l'ingénierie inverse. Aucune des politiques ne fait référence à la réparation au-delà de cette interdiction. Nous émettons donc l'hypothèse que les principales limites au droit de réparation identifiées dans la section 3.3 proviennent des verrous numériques et du manque d'accès aux informations de diagnostic plutôt que des contrats.

7 Point de vue des parties prenantes et des experts

7.1 Introduction

Après avoir effectué notre recherche, nous avons sollicité l'avis des experts, organismes de réglementation et organisations d'intérêt public sur nos résultats. L'objectif de cette consultation était de recueillir les opinions des parties prenantes sur les problématiques et les risques identifiés, sur l'adéquation du cadre juridique et réglementaire existant et sur des pistes de solution aux problèmes identifiés.

Pour ce faire, nous avons contacté des autorités réglementaires en matière de protection du consommateur, en protection de la vie privée et en concurrence, ainsi que des groupes d'intérêt public en matière de technologie, de vie privée et d'environnement. Enfin, nous avons également sollicité l'opinion de professeurs et chercheurs en matière de concurrence, de droit à la réparation, de propriété intellectuelle et de protection de la vie privée.

Parmi la trentaine des personnes et organismes contactés, sept ont accepté de participer à notre enquête. Nous n'avons pas consulté toutes les parties sur chacun des points du rapport ; nous avons plutôt cherché à obtenir leur avis sur les éléments les plus pertinents par rapport à leur expertise ou à leurs intérêts de recherche. Nous avons envoyé aux intervenants un document qui résumait les résultats de notre recherche et posait des questions sur leurs opinions concernant ces résultats. Les intervenants ont répondu soit par écrit, soit lors d'un entretien oral.

Les professeurs :

- **Anthony D. Rosborough**, assistant professor of Law & Computer Science at Dalhousie University, Halifax, and doctoral researcher in Law at the European University Institute.
- **Alissa Centivany**, assistant professor at the Faculty of Information and Media Studies at the University of Western Ontario and co-founder of the Canadian Repair Coalition (CanRepair), a non-profit organisation that seeks to bring together supporters of the right to reparation from across the country.
- **Jacinthe Cloutier**, directrice des programmes de 1^{er} cycle en Sciences de la consommation et professeure agrégée en Sciences de la consommation à l'Université Laval.
- **Karounga Diawara**, professeur titulaire à la Faculté de droit et directeur du Centre d'études en droit économique de l'Université Laval.

Le professionnel de recherche :

- **Enrico Guénard**, professionnel de recherche à l'Université Laval, qui a également une expérience professionnelle en tant qu'analyste au sein d'une entreprise spécialisée dans la vente de données relatives aux véhicules connectés.

Les groupes de défense des droits et d'intérêt public :

- **OpenMedia**, un organisme à but non lucratif qui œuvre pour un Internet abordable, sans surveillance et démocratique et pour faire avancer la démocratie et les droits numériques à travers l'Amérique du Nord.

- **Option consommateurs**, une association à but non lucratif située au Québec qui a pour mission d'aider les consommateurs et de défendre leurs droits.

7.2 La protection de la vie privée

7.2.1 Risques

Toutes les parties prenantes consultées sur l'impact de la voiture connectée sur la vie privée ont partagé des inquiétudes et ont souligné l'importance et la gravité des risques liés à la collecte, l'utilisation et le partage des renseignements personnels dans ce contexte.

Intrusion dans la vie privée, surveillance, manipulation

Jacinthe Cloutier a souligné l'aspect de l'intrusion injustifiée dans la vie privée :

Quand on a accès aux déplacements des personnes, on en sait beaucoup sur leur vie privée, au-delà de la donnée collectée. Par exemple, on sait à quelle épicerie il a l'habitude de faire ses achats, le temps passé dans le supermarché, etc., données intéressantes pour cette industrie, mais totalement inutiles pour le fabricant de voitures.

OpenMedia et Option consommateurs ont également évoqué le fait que des données extrêmement sensibles peuvent être collectées. OpenMedia a mis l'accent sur la possibilité de créer des profils sur les consommateurs, qui peuvent être vendus.

Quant à Alissa Centivany, elle affirme que la collecte, l'utilisation et le partage de renseignements personnels par les fabricants soulèvent de sérieuses questions éthiques et juridiques. Elle évoque le fait que les outils de surveillance sont désormais intégrés dans plusieurs types de technologies. Ce type de surveillance de masse permet aux entreprises de manipuler les opinions et les décisions des consommateurs à des fins commerciales et politiques.

Enrico Guénard a partagé plusieurs exemples provenant de son expérience professionnelle qui démontrent d'une manière concrète les risques posés par la collecte, l'utilisation et le partage massifs des données. Par exemple, il a déjà vu des entreprises qui ont envisagé de vendre des données de véhicules connectés qui permettraient « d'identifier la présence d'individus à des cliniques d'avortement aux États-Unis, à un moment où cette question politique était très clivante au sein de la population américaine ». Les personnes concernées étaient « identifiables grâce aux données de véhicules connectés (ex. : marque et année du véhicule et code postal).

M. Guénard soulève d'autres risques :

[pour] l'identification de véhicules à des endroits préjudiciables (poste de police, crime organisé, établissement reconnu relativement à de la prostitution), les risques peuvent aller jusqu'à identifier le propriétaire d'un véhicule pour faire du chantage en croisant avec des données de médias sociaux.

Absence de consentement et de choix

OpenMedia a fait part de ses préoccupations quant à la difficulté de refuser les pratiques de collecte, etc., de données. Il a noté que la plupart des consommateurs qui achètent un nouveau véhicule ne peuvent pas en choisir un qui ne collecte pas de données, en particulier compte tenu de la transition vers les véhicules électriques.

En ce qui concerne le consentement, M. Guénard a parlé du manque de littéracie chez les consommateurs en matière de protection de leurs données personnelles et indique que cela « occasionne probablement des abus de la part d'entreprises qui collectent de telles informations ». Cependant, même ceux qui sont conscients de ces pratiques n'ont guère le choix :

Personnellement, le simple fait de ne pas pouvoir refuser que des données soient collectées m'amène à repousser l'achat d'un véhicule récent en espérant que le cadre légal s'améliore au Canada pour encadrer de telles pratiques. Le fait de pouvoir refuser que de telles données soient collectées et que cet engagement du fabricant du véhicule soit pleinement respecté serait un critère décisif dans le choix du véhicule que j'achèterais.

Option consommateurs a également trouvé dans ses recherches que :

Les politiques de confidentialité ne lient généralement pas les données aux fins pour lesquelles elles sont collectées. Les consommateurs peuvent donc difficilement savoir quelle donnée est utilisée pour quelle fin spécifique, ce qui pose des enjeux sur le consentement éclairé fourni pour le traitement de leurs renseignements personnels.

En outre, l'organisation a noté que des concepts tels que l'anonymisation et la dépersonnalisation sont souvent invoqués dans les politiques de protection de la vie privée sans aucune définition ou signification claire.

La professeure Centivany a observé que les données sont souvent sauvegardées par les fabricants, partagées et ensuite utilisées à des fins qui n'étaient pas nécessairement prévues au moment de la collecte, et que les consommateurs n'ont généralement pas la possibilité de consentir à cette utilisation secondaire ou tertiaire.

Risques pour la sécurité

M. Guénard a évoqué certains risques de sécurité liés à ces pratiques :

La collecte par le fabricant [...], l'agrégation de ces données massives à des fins de revente, la revente et le traitement des données par des courtiers qui ne respectent pas nécessairement le cadre d'utilisation des dites données, et finalement l'utilisateur final des données achetées qui peut parfois faire un usage détourné des données en ne respectant pas les termes d'utilisation... À chacune de ces étapes, la gouvernance des données, la sécurité des données et le respect des notions de vie privée et d'anonymisation des données peuvent être compromis. J'ai à plusieurs reprises observé des façons non sécuritaires d'échanger des données avec des clients où le risque élevé de fuite aurait pu être préjudiciable.

7.2.2 Adéquation du cadre législatif

L'encadrement législatif en matière de protection de la vie privée et sa mise en application sont inadaptés à la situation, selon les parties prenantes.

Mise en application

Jacinthe Cloutier a trouvé que la loi semble offrir des protections adéquates, mais que l'application est difficile :

Qui se rend compte de ces infractions, ou encore comment un simple conducteur peut s'en rendre compte ? Ce ne peut pas être la responsabilité du consommateur. On lui en met beaucoup dans sa cour, alors qu'il n'a pas nécessairement les compétences pour capter ce qui cloche dans la relation avec l'entreprise.

OpenMedia a également déclaré que la législation canadienne sur la protection de la vie privée, y compris le projet de loi C-27, présentait des lacunes importantes en ce qui concerne l'absence de mécanismes d'application et de sanctions solides. Les organismes de surveillance sont :

often under-resourced and lack the teeth necessary to effectively deter large corporations from violating privacy rights. This is particularly concerning in the complex ecosystem of connected cars. Stronger enforcement requires increased funding for regulatory bodies, more proactive investigations, and the imposition of meaningful financial penalties for non-compliance.

Consentement

OpenMedia s'est montré aussi critique de l'encadrement en général, déclarant que les lois canadiennes en matière de la vie privée, y compris le projet de loi C-27, sont insuffisantes pour protéger les consommateurs dans cet âge numérique. L'organisme a souligné plusieurs faiblesses dans le régime actuel, qui permet des exemptions larges et importantes au principe du consentement. Option consommateurs et OpenMedia ont déclaré que le cadre législatif relatif au consentement devait être renforcé. Le recours à des politiques de protection de la vie privée longue et complexes pour les voitures connectées ne favorise pas un consentement éclairé. Les politiques de protection de la vie privée doivent être rédigées dans un langage clair et simple, et indiquer clairement quelles données sont collectées, comment elles sont utilisées et avec qui elles sont partagées.

Jacinthe Cloutier a également affirmé que le besoin de demander le consentement du consommateur est utile comme mécanisme de protection de la vie privée, mais seulement dans la mesure où la personne comprend ce à quoi elle consent, ce qui n'est pas le cas dans le contexte actuel des voitures connectées. « Pour le moment c'est indigeste, incompréhensible même pour une personne hautement scolarisée ». Elle observe que même si la personne comprend ce à quoi elle consent lors de la transaction, il reste difficile d'évaluer les risques à long terme.

7.2.3 Des pistes de solutions

Jacinthe Cloutier a plaidé pour une plus grande éducation des consommateurs sur l'utilisation et la vente de leurs données. Cependant, une intervention législative est également nécessaire, étant donné le déséquilibre inhérent entre les parties. Elle a parlé des limitations légales sur l'utilisation de données, et a recommandé que l'utilisation des données doive « se limiter au bon fonctionnement du véhicule. Le partage [des données de localisation] pourrait être effectué uniquement si la personne a besoin d'une intervention (panne, malaise, etc.). »

Elle fait valoir qu'il faut repenser le modèle d'affaires actuel, dans lequel les fabricants conservent tout le contrôle des données et tous les bénéfices et profits de leur utilisation et revente. Elle soutient qu'il faut changer le modèle pour « que la personne qui achète le véhicule devient entièrement propriétaire et a le droit d'accepter ou non de partager ses données ». On peut penser aussi à d'autres solutions, par exemple, « la personne qui loue sa voiture pourrait le faire à un coût très faible en échange de ses données, en ayant toute l'information, de façon vulgarisée, de l'emploi de ses données ». En résumé, le consommateur doit avoir plus de contrôle sur ses données ou, à défaut, en bénéficier financièrement, au moins.

OpenMedia a parlé de la nécessité d'une réglementation contraignante en matière de protection de la vie privée pour l'ensemble du secteur. L'organisme milite pour une réforme législative urgente qui permettrait réellement aux individus de s'émanciper de ces pratiques et aux entreprises de rendre des comptes. Ainsi, l'organisme a recommandé l'adoption d'une charte numérique qui énonce le droit à la vie privée, la limitation des finalités de la collecte des données, les principes de minimisation de la collecte, etc., des données et un droit à l'oubli. Il a également recommandé d'interdire la collecte des données qui ne sont pas strictement nécessaires pour assurer la fonctionnalité de base du véhicule. En outre, le Commissaire à la protection de la vie privée (ou son équivalent provincial) devrait pouvoir enquêter sur le comportement d'une entreprise qui requiert la collecte de données avant de donner au consommateur l'accès à une fonctionnalité du véhicule qui ne nécessite pas intrinsèquement cette collecte.

D'une manière générale, OpenMedia recommande de donner au Commissaire à la protection de la vie privée des pouvoirs accrus lui permettant d'enquêter de manière proactive, d'émettre des ordonnances contraignantes et d'imposer des sanctions importantes en cas de violation. Il a également recommandé d'obliger les entreprises à mener des évaluations de l'impact relativement à la protection des données et à les rendre publiques avant de déployer de nouvelles technologies qui collectent des quantités importantes d'informations personnelles.

En ce qui concerne le consentement, OpenMedia fait valoir qu'il faut assurer que les consommateurs ont le choix d'utiliser les fonctionnalités essentielles du véhicule sans être obligés à consentir à la collecte excessive de leurs données. Les fabricants doivent donner aux consommateurs un accès à des contrôles granulaires qui permettent d'accepter ou de refuser des pratiques spécifiques de collecte de données.

OpenMedia et Option consommateurs ont tous deux recommandé d'établir des normes juridiques claires concernant l'anonymisation, et OpenMedia a recommandé d'exiger une vérification indépendante des processus d'anonymisation.

Nous avons également demandé aux répondants s'il y avait des solutions non législatives à promouvoir.

Enrico Guénard s'est dit optimiste quant aux avancées technologiques comme l'utilisation de la chaîne de blocs et la sécurité cryptographique, qui permet « la décentralisation des données et à un virage vers la protection autosouveraine des données personnelles ». Il a fait valoir que « le consommateur serait mieux protégé et en meilleure position s'il pouvait lui-même gérer à la pièce les informations qu'il partage avec des tiers ».

Jacinthe Cloutier a évoqué certaines mesures que les fabricants pourraient prendre pour améliorer la situation, même sans une intervention législative. Elle a suggéré de remettre au consommateur un document explicatif vulgarisé qui résume quelles données seront recueillies et quelles utilisations en seront faites. Elle suggère aussi de permettre au consommateur de choisir les données à divulguer. Elle a également souligné l'importance de veiller à ce que les consommateurs puissent utiliser la voiture même si le consentement n'est pas donné et de ne collecter des données que si le consentement est clairement donné.

Option consommateurs a mentionné que des « lignes directrices pourraient être développées sur la communication des informations au sujet du traitement des renseignements personnels en langage clair ».

OpenMedia a indiqué que l'autorégulation ne pourrait être satisfaisante que si la protection de la vie privée était respectée dès la conception et par défaut, si les entreprises assuraient une transparence et un contrôle significatifs des données, et s'il y avait des audits indépendants et une obligation de rendre compte des pratiques en matière de collecte et de sécurité des données. L'organisme a fait valoir que toute autorégulation de l'industrie doit être élaborée dans le cadre d'une véritable consultation avec les groupes de défense des consommateurs et les experts en matière de protection de la vie privée, et pas uniquement avec les acteurs de l'industrie.

7.3 Droits de propriété, droit à la réparation et la protection des consommateurs

7.3.1 Droits de propriété : risques et problématiques

Le contrôle après la vente : un pouvoir déstabilisant et problématique

Nous avons présenté nos conclusions concernant l'impact de la connectivité sur les droits de propriété aux parties prenantes et leur avons tout d'abord demandé si elles considéraient que la capacité des fabricants à conserver le contrôle après l'achat constituait un risque pour les consommateurs. Tous les répondants consultés sur ce point ont reconnu qu'il s'agissait d'un risque important et ils ont utilisé les mots « effrayant, anxiogène, *incredibly problematic*, *destabilizing* et *significant* » pour décrire la situation.

OpenMedia, Alissa Centivany et Anthony Rosborough ont avancé que le fait que le fabricant garde un contrôle sur le bien après l'achat a pour effet de modifier les normes relatives à l'achat et à la propriété. Ce qui était auparavant implicite pour les consommateurs dans la notion d'achat ou de propriété est remis en cause par cette relation de contrôle continu.

Le professeur Rosborough rappelle que la notion de propriété englobe typiquement un ensemble de droits (bundle of rights), tels que le droit d'utiliser le bien, de le louer, de le détruire, etc. Lorsqu'une personne acquiert un bien, elle a des attentes normalisées sur ce qu'implique cette acquisition et sur ce qu'elle peut faire avec son bien. Toutefois, la connectivité permet au fabricant d'accorder ou de révoquer des caractéristiques après l'achat, ce qui affecte ce que le propriétaire peut faire de son bien.

What connectivity often does through [Internet of Things] or other types of tethering is it de-standardizes that relationship between the consumer and the product, where you don't know at the time of sale what it is you're buying.

Alissa Centivany a également abordé cette question, affirmant que le maintien du contrôle sur le bien après sa vente contredit la notion d'achat. Les consommateurs ont des attentes quant aux droits liés implicitement à la propriété, qui sont mis à mal par ces pratiques. En outre, ces pratiques sont loin d'être transparentes : les consommateurs ne savent généralement pas que le fabricant peut modifier les conditions de propriété après l'achat. Toutefois, elle a fait remarquer que même si ces pratiques étaient transparentes, elles resteraient problématiques.

OpenMedia a fait valoir que le principal risque de ces types de pratiques est qu'elles font en sorte que le droit de propriété ressemble de plus en plus à un droit de licence ou de location.

Tous trois ont fait remarquer que ces pratiques reposent sur une relation asymétrique entre le consommateur et le fabricant et qu'elles amplifient cette asymétrie. La professeure Centivany a souligné le fait que lorsque les fabricants exercent un contrôle après l'achat, par exemple en supprimant certaines fonctionnalités, ils prennent des décisions non négociables dont le consommateur n'est peut-être même pas conscient et auxquelles il n'est pas en mesure de s'opposer. Le professeur Rosborough a qualifié cette situation de « relation abusive ».

OpenMedia et Option Consommateurs ont également évoqué le risque du modèle d'abonnement permis par la connectivité ; les deux organisations ont critiqué la pratique qui consiste à faire payer les consommateurs en continu pour utiliser du matériel déjà acheté.

Le bien-être et l'autonomie des consommateurs

Les professeurs Centivany, Rosborough et Cloutier ont tous souligné le fait que la perte de contrôle sur ses biens peut affecter le bien-être et l'autonomie d'une personne.

Alissa Centivany a qualifié ces pratiques d'« intrusion dans la vie des consommateurs », qui « sape leur autonomie et l'exercice de leur autodétermination relativement à des technologies qui leur appartiennent et qui sont essentielles dans leur vie quotidienne ».

Jacinthe Cloutier a mentionné que « les consommateurs qui ont conscience de ces possibilités peuvent vivre une anxiété supplémentaire à la vie déjà stressante. Un propriétaire d'un objet, quel qu'il soit, ne devrait pas être soumis à autant de variables hors de son contrôle ». Elle a aussi mis en garde contre le risque d'habitude : « au début on accepte certains éléments et avec le temps on en accepte de plus en plus et on perd le contrôle, dans ce cas-ci, de la propriété de notre véhicule et ce qu'on peut en faire ». Elle soulignait donc l'importance de mettre fin incessamment à ces pratiques et aux restrictions sur la réparation (ci-dessous).

Anthony Rosborough a observé que :

When people feel that their ability to own things is being taken away from them, they react in very strong ways. I think there's a risk that this destabilizes people on a social level, when there's less of a concrete understanding of what it means to own a car, for example, which is often the symbol of freedom and autonomy in North American life. It becomes just another iPad or an app on your phone.

Obsolescence

Option consommateurs, OpenMedia et la professeure Centivany ont également évoqué le risque d'obsolescence programmée lié aux logiciels des véhicules connectés. Option consommateurs a souligné le risque qui se présente lorsque le « fabricant cesse de faire les mises à jour de véhicules intelligents d'un certain âge alors que le véhicule lui-même serait autrement fonctionnel ». OpenMedia, pour sa part, a soulevé des craintes concernant les mises à jour qui rendent, intentionnellement ou non, les anciens véhicules moins fonctionnels ou moins sûrs.

La sécurité et le vol des véhicules

Le professeur Rosborough a brièvement évoqué les risques liés à la cybersécurité et au vol de véhicules. Mentionnant le piratage du véhicule Chrysler (mentionné à la section 3.4.2 du rapport), il s'est demandé si la connectivité des véhicules augmentait réellement la sécurité, compte tenu des risques qu'elle présente pour la santé, la sécurité et le droit de propriété.

7.3.2 Droit à la réparation : risques et problématiques

Les restrictions sur la réparation sont anticoncurrentielles et douteuses

Toutes les parties consultées sur l'enjeu de la réparation des voitures connectées ont fait valoir que les restrictions imposées par les fabricants sont intentionnelles et ont un effet anticoncurrentiel.

OpenMedia a mis l'accent sur les risques liés à l'application à distance des restrictions en matière de réparation et aux dépendances logicielles pour la réparation.

Anthony Rosborough a fait valoir que les restrictions à la réparation identifiées dans le rapport, notamment l'utilisation d'autres verrous logiciels, sont le résultat de choix de conception délibérés faits par les fabricants pour restreindre la réparation sur les marchés secondaire. Il a fait remarquer que l'entretien, la réparation et l'assistance technique représentent une part importante de l'activité économique liée aux véhicules, et que le contrôle de ce marché est financièrement avantageux. Les fabricants plus anciens,

comme GM et Ford, ont plus de difficulté à restreindre la réparation indépendante, car ils ont déjà établi des chaînes d'approvisionnement impliquant des réparateurs tiers. Toutefois, les nouveaux venus, comme Tesla, réussissent relativement bien à centraliser et à contrôler l'ensemble de la chaîne d'approvisionnement en matière de réparation. Il a observé que cela fait partie d'une tendance plus large, où les entreprises insistent sur un modèle de contrôle exclusif (« *command and control* ») et sur l'intégration verticale des chaînes d'approvisionnement.

I think Apple was one of the first to really start this with an ecosystem business design. But it's just gotten to the point now where every company is trying to do it, trying to lock you into their ecosystem... trying to create so-called ecosystems of profitability where there are high switching costs. And really, no one wants it.

Selon le professeur Rosborough, la tendance pourrait évoluer, car les consommateurs se conscientisent aux restrictions qui leur sont imposées et visent une plus grande autonomie. Il a fait valoir que le modèle de contrôle actuel n'est pas le seul et qu'il existe des modèles d'innovation plus ouverts. Par exemple, la norme USB a été développée à l'origine par des acteurs de l'industrie qui estimaient qu'une norme commune et l'interopérabilité créeraient un marché plus important pour tous les acteurs. De même, les fabricants pourraient aujourd'hui s'entendre sur des normes et innover à partir de plates-formes ouvertes.

Karounga Diawara, Alissa Centivany, Jacinthe Cloutier et OpenMedia ont tous souligné l'impact des pratiques telles que le couplage de pièces et la restriction de l'accès aux données de diagnostic sur la capacité des réparateurs indépendants à être compétitifs et l'augmentation des coûts qui en découlent pour les consommateurs. Le professeur Diawara a précisé que « l'augmentation des prix de réparation des voitures connectées doit être entendue au sens large en incluant une possible diminution de la qualité de la réparation attendue ». Limiter l'accès aux réparations indépendantes peut être particulièrement préjudiciable dans les zones rurales où le fabricant peut ne pas avoir de succursale.

Le professeur Diawara a également commenté que « ce refus [de partage de données diagnostiques] ne saurait être justifié par le seul droit de propriété des fabricants », car l'impact est de « réduire la concurrence dans le marché subséquent de la réparation des voitures connectées, en y excluant les réparateurs indépendants » et de consolider la position des fabricants et de leurs concessionnaires dans ce secteur.

La professeure Centivany a aussi mis l'accent sur le fait que l'autonomie du consommateur est limitée par les restrictions sur l'accès aux données de diagnostic ou aux réparations de base. Si un conducteur ne peut pas lire lui-même un code de diagnostic de base, sa capacité de prendre une décision concernant la réparation est compromise. OpenMedia a également souligné le gaspillage que représentent de telles pratiques, qui peuvent conduire à « des durées de vie plus courtes pour les véhicules, contribuant ainsi à des déchets électroniques inutiles ».

La sécurité ne justifie pas les restrictions sur la réparation. Ni OpenMedia, ni Anthony Rosborough, ni Alissa Centivany n'ont estimé que les raisons de sécurité invoquées par les fabricants pouvaient justifier leur décision de limiter l'accès aux données et aux

logiciels de réparation; ils s'entendaient pour dire que la sécurité était un prétexte utilisé pour restreindre l'accès à la réparation.

Les recherches de la professeure Centivany lui ont permis de constater que les fabricants, dans de nombreux secteurs (automobile, défense militaire, appareils ménagers, etc.), tentent de restreindre la réparation en invoquant des raisons de sécurité, et ce, bien souvent sans présenter aucune preuve ni aucun exemple spécifique à l'appui de leurs prétentions.

Tous trois ont fait valoir que les problèmes de sécurité peuvent être atténués par une meilleure conception du véhicule plutôt que par la restriction de l'accès aux réparations. En effet, s'il existe des risques pour la sécurité, c'est parce que les fabricants les ont introduits ou maintenus par des choix de conception défectueux ou délibérés. Comme l'a dit le professeur Rosborough,

Think about the example of an airplane. There is a security problem in the fact that many people have access to it, and we don't want people to hijack it or bring on weapons. What's the solution? Do we prohibit everyone from bringing on anything that's sharp or dangerous? No, it just means you have to put it in your checked bag and you have to disclose it. So we've designed a system that can enable a certain amount of openness and security at the same time.

[Automobile manufacturers] design cars with computerization, part serialization and parts pairing through software, and then turn around and say this is necessary for security. It's not. They've designed the product in this way and created their own justification for it, in the hopes that no one will question it.

La professeure Centivany a fait remarquer que les voitures connectées présentent en soi des risques importants pour la vie privée et la sécurité (par exemple, le vol, les fuites de données, le piratage), qui n'ont rien à voir avec le partage des données de diagnostic et des logiciels de réparation. Les fabricants ont conçu un système non sécuritaire et ils sont les mieux placés y remédier ; qu'ils ne l'aient pas fait suggère que la sécurité n'est pas une priorité.

7.3.3 Adéquation du cadre législatif : lacunes et suggestions

Nous avons demandé aux parties prenantes de commenter le cadre législatif canadien existant concernant les droits de propriété et le droit de réparer face aux risques que présentent les véhicules connectés. Tous les répondants à cette question ont déclaré que le cadre actuel est inadéquat pour traiter les problèmes identifiés. Cela a pour effet de favoriser les fabricants et d'affaiblir les droits des consommateurs.

Les restrictions au contournement des mesures techniques de protection doivent être éliminées

Tout d'abord, nous avons posé des questions sur les restrictions relatives au contournement des verrous numériques dans la *Loi sur le droit d'auteur* et les nouvelles exemptions introduites par les projets de loi C-244 et C-294, qui permettent aux individus de contourner ces verrous pour les fins de réparation ou d'interopérabilité. OpenMedia et les professeurs Centivany et Rosborough estiment que les nouvelles dispositions

constituent un pas dans la bonne direction, mais qu'ils sont insuffisants pour faire face aux risques identifiés.

Les professeurs ont critiqué l'amendement apporté avant son adoption au texte du projet de loi C-244, qui semble ne permettre qu'aux individus, et non aux acteurs commerciaux, de contourner les verrous numériques à des fins de réparation. Selon les deux professeurs, l'ambiguïté de la formulation de l'amendement suggère qu'il pourrait y avoir des exceptions à ces restrictions. Quoi qu'il en soit, les amendements limitent l'utilité des autorisations de contournement, puisque la plupart des individus ne peuvent pas ou ne veulent pas contourner les verrous numériques par eux-mêmes. La professeure Centivany a noté que l'amendement démontre les limites de la conception purement individualiste du droit à la réparation : la loi qui permet maintenant aux individus de contourner les verrous numériques risque de ne pas améliorer l'accès réel à la réparation. Un véritable accès à la réparation nécessite des infrastructures et l'intervention de réparateurs qualifiés.

Le professeur Rosborough a observé que l'accord Canada-États-Unis-Mexique limite la capacité du législateur à modifier davantage la Loi sur le droit d'auteur et à permettre le contournement des mesures techniques de protection (MTP) dans des contextes commerciaux. Le traité lie les mains du gouvernement fédéral à cet égard ; s'il devait être renégocié, ces dispositions pourraient être modifiées pour donner plus de latitude au législateur canadien. Idéalement, selon le professeur Rosborough, la Loi sur le droit d'auteur serait modifiée pour permettre le contournement de toute MTP qui ne protège pas contre une violation du droit d'auteur (c'est-à-dire la reproduction, l'exécution ou la distribution d'une œuvre protégée).

OpenMedia a noté que les dispositions introduites par les projets de loi C-294 et C-244 sont utiles pour traiter les MTP dans certains contextes, mais que la connectivité pourrait permettre de nouvelles méthodes pour entraver la réparation, sapant ainsi l'intention derrière ces exemptions. Une législation sera nécessaire pour traiter ces questions également.

Une législation favorisant le droit à la réparation est nécessaire

Les trois intervenants ont fait valoir que le Canada a besoin d'une législation sur les enjeux en matière de réparation qui aille au-delà des dispositions de la Loi sur le droit d'auteur relatives aux MTP. Comme le dit OpenMedia, le cadre législatif actuel et les nouveaux projets de loi « n'imposent pas le partage des données, outils et mises à jour logiciels nécessaires à une réparation efficace. Une législation beaucoup plus contraignante est nécessaire ». Le professeur Rosborough a également souligné le fait que la modification de la Loi sur le droit d'auteur n'aborde qu'une partie du problème et que les réformes doivent être plus larges :

Circumvention, that is, allowing people to break locks, is not a guaranteed solution for many reasons. It requires technical expertise. It assumes that there's a willingness to break these locks and that there is some commercial interest in doing so.

I think an equal and complementary legislative framework needs to impose obligations on manufacturers not to use [digital locks] in certain product categories

or in certain cases. So it's not about whether or not [locks] receive protection under the Copyright Act, but whether from a regulatory perspective, [manufacturers] are allowed to use certain methods of encryption and authentication on products and devices where we don't think those techniques should be used, because we think it's bad for business and bad for the planet.

En d'autres termes, il faut des garanties législatives pour prévenir l'usage de verrous numériques dans certains contextes, ce qui annulerait la nécessité de les contourner.

Cela dit, le professeur Rosborough a réitéré l'importance d'autoriser le contournement des MTP dans le contexte de la réparation, tout en légiférant pour limiter l'utilisation des verrous numériques :

The two approaches work in harmony. From a top-down regulatory perspective, we can never know all of the technical needs of repair, maintenance, diagnosis over time. Products change. There are new techniques, new barriers that will present themselves, and those with a technical inclination and with the means ought to be able to force [repair] to happen where it has been made impossible. Legislation and regulation can only move so quickly. Let's say we enact a perfect scheme right now to guarantee the right to repair on connected cars. In two years, there's no guarantee that that's going to apply when there's a new communication protocol, a new form of encryption, some new software technique, some new connectivity. I think there needs to be a kind of backstop so that the independent repairer can still push ahead and force the repair, even if the manufacturer prevents it.

La professeure Centivany a expliqué que la réparation peut être entravée par la conception même, sans que cela n'ait à voir avec les verrous numériques ou la législation sur le droit d'auteur, et qu'une réforme législative est également nécessaire pour résoudre ce problème.

Any product can be designed to promote repairability, to undermine it, or to be ambivalent to it. I think what we're seeing [in vehicle manufacturing] is more ambivalence and antagonism toward repair than products that are designed with repair in mind.

Elle a donné l'exemple du fait que les voitures conçues avec un capot. Cette conception favorise la réparabilité, puisque le capot donne accès aux parties internes du véhicule et permet la réparation et l'entretien. Cependant, les constructeurs semblent s'éloigner d'une conception des véhicules favorisant la réparation, notamment avec les véhicules électriques. Par exemple, elle a parlé de la difficulté de réparer les châssis des véhicules Tesla, dont certains sont moulés sous pression en une seule pièce au lieu d'être composés de plusieurs pièces. Si le cadre est endommagé lors d'un accident, son intégrité entière peut être compromise et la réparation peut être plus complexe que le simple remplacement de la pièce endommagée.

Aucune disposition en droit canadien ne prévoit que les véhicules doivent être conçus de manière à favoriser la réparation. La professeure Centivany s'est montrée favorable à l'idée de réglementer la conception même, pour assurer une meilleure réparabilité. Le

droit de la concurrence peut également être utile à cet égard, puisque les restrictions en matière de réparation permettent à ceux qui dominent le marché d'exploiter leur position et de freiner la concurrence dans le domaine de la réparation.

OpenMedia et Option consommateurs ont également plaidé pour la promotion d'une plus grande prise en compte de la réparabilité dans la conception, notamment par l'établissement de normes visant à faciliter la réparabilité et l'interopérabilité. Le professeur Rosborough a également souligné l'importance d'utiliser des normes techniques pour promouvoir l'ouverture et l'interopérabilité. Il doute fort de l'intérêt pour l'industrie d'élaborer volontairement de normes ouvertes, « les avantages d'une concurrence fermée étant trop importants ». Ainsi, certaines normes, relatives, par exemple, aux protocoles de communication, élaborées en collaboration avec des experts techniques, doivent être imposées par l'État. Il a cité l'exemple de l'Union européenne, qui exige que les petits appareils électroniques disposent d'un port de recharge de type USB-C ; à défaut, le produit ne peut pas être vendu dans l'UE. De telles normes sont cruciales pour les voitures connectées, compte tenu de l'importance des véhicules en tant que produits de consommation et de leur longue durée de vie.

La législation québécoise sur le droit de à la réparation devrait être adoptée dans tout le Canada

OpenMedia et les professeurs Centivany, Rosborough et Diawara appuient la législation québécoise sur le droit à la réparation et soutiennent que le reste du Canada devrait adopter une législation similaire.

Le professeur Rosborough a salué le fait que la législation québécoise traite de l'accès aux données de diagnostic, corrigeant une lacune de l'accord CASIS. Il regrette toutefois que la loi n'impose pas la gratuité pour l'accès à ces données. Selon lui, la commercialisation des données, qui permet aux fabricants d'imposer des conditions restrictives à leur accès, est problématique en soi, au-delà de la question du coût. Ces conditions pourraient être utilisées pour décourager la concurrence et intégrer des mécaniciens indépendants à la chaîne d'approvisionnement verticale des constructeurs. Par exemple, le fabricant pourrait conditionner l'accès aux données de diagnostic à un coût raisonnable à l'utilisation d'une plateforme propriétaire qui nécessite un abonnement à long terme et un engagement d'exclusivité. Si l'accès aux données n'est pas encadré, ça laisse la porte ouverte à

another type of profiteering that reduces competition. The data is being given at a low price, but the value is being captured through other means in this scenario.

I would not underestimate the desire of these companies to find some way of using this opportunity to sell diagnostic data at a reasonable price as a way of capturing more value and limiting competition. I think they will. And not because they're evil, but that's the motivation of a capitalist entity.

En effet, les experts en réparation interrogés dans la section 3.3.3 ont indiqué qu'il s'agit du modèle qui est apparu après la signature du protocole d'accord de 2014 et qui continue à poser des problèmes pour les réparations.

Le professeur Rosborough a donc soutenu qu'il valait mieux mettre fin à la commercialisation de l'accès aux données de diagnostic. Mais, si l'accès est commercialisé, la réglementation devrait interdire au fabricant d'imposer de restrictions sur l'utilisation, le partage ou la divulgation des données.

Le professeur Diawara a également souligné l'importance de partager les données de diagnostic avec les consommateurs et leurs représentants « pour protéger davantage la variété de l'offre dans le secteur de la réparation de voitures connectées et préserver les intérêts du consommateur et des acteurs non dominants du marché ».

OpenMedia a fait valoir que « le droit à la réparation et la véritable propriété numérique de nos données et de nos appareils sont des droits fondamentaux des consommateurs à l'ère numérique ». Garantir un véritable droit à la réparation, c'est-à-dire « obliger les fabricants à donner aux propriétaires et aux réparateurs indépendants, à un coût juste et raisonnable, accès aux données de diagnostic, aux manuels de réparation, aux mises à jour logicielles et aux outils nécessaires », favoriserait la concurrence, réduirait le gaspillage et permettrait aux individus de contrôler les produits dont ils sont propriétaires. L'organisme a suggéré que les fabricants s'attaquent aux problèmes de sécurité en établissant « des protocoles de partage sécurisé de données avec des professionnels de la réparation indépendants agréés, comme cela a été fait dans d'autres juridictions ».

La professeure Centivany a également estimé que la législation québécoise favorisait la concurrence et la durabilité. Elle apprécie le fait qu'elle ne soit pas spécifique à une industrie et qu'elle impose au contraire à tous les fabricants la responsabilité de mettre à disposition les pièces, l'information et les outils, et ce, à un coût raisonnable. Elle s'est également prononcée favorablement sur les dispositions de la loi en matière de garantie (qui ne sont pas abordées dans le présent rapport), notamment celles qui concernent spécifiquement les véhicules et la garantie plus générale de bon fonctionnement, qui couvre les coûts de réparation d'un produit pendant toute sa durée.

I think that the warranty issue is one of the most important issues. In Canada, we don't have any federal law that governs contracts for the sale of goods or services that [establishes] minimum warranty guarantees. The warranty of good working order that's in the Quebec bill - we should have that at a federal level. Anytime any sale for anything in Canada takes place, that should be an implicit part of the agreement and there should be recourse if that's not the case. It would help improve things like durability and product quality.

7.3.4 D'autres pistes de solutions

Outre leurs recommandations concernant la *Loi sur le droit d'auteur* et l'adoption d'un encadrement pour améliorer la réparabilité dès la conception des véhicules, les parties prenantes ont proposé de nombreuses autres solutions aux problèmes en matière de propriété et réparation, qu'elles soient législatives ou non.

Comme la professeure Cloutier l'a suggéré ci-dessus en matière de vie privée, le professeur Diawara a suggéré de transférer la propriété des données de diagnostic aux consommateurs au moment de leur acquisition du véhicule. Il soutient que c'est ce que la législation québécoise a effectivement fait.

Un tel transfert/partage de propriété amenuiserait grandement le contrôle actuel des fabricants sur les données de diagnostic et rendrait le marché plus concurrentiel au bénéfice des consommateurs et des autres acteurs (réparateurs indépendants notamment).

OpenMedia et Option consommateurs ont également plaidé pour l'adoption de règles visant l'interdiction de « l'obsolescence programmée et la mise en place d'entraves intentionnelles à la réparation des appareils » ; pour OpenMedia, il s'agit notamment d'assurer que les fabricants fournissent des mises à jour de sécurité et de fonctionnalité pour une période raisonnable après la vente du véhicule.

OpenMedia et la professeure Centivany ont souligné l'importance d'imposer des limites aux contrats de licence d'utilisateur final (CLUF). OpenMedia a recommandé « d'interdire aux CLUF de déroger aux droits fondamentaux des consommateurs, y compris le droit de réparer et de modifier leur propriété à des fins légitimes ». La professeure Centivany a également déclaré que, selon elle, « de nombreuses clauses des CLUF sont abusives et ne devraient pas être opposables contractuellement ». Elle a réitéré sa recommandation que le Canada dans son ensemble adopte des garanties légales de base. OpenMedia a également plaidé pour « la modernisation de la législation sur la protection des consommateurs afin d'aborder spécifiquement les défis uniques posés par les produits connectés et de garantir un droit de propriété sur les données, promouvant ainsi le bien-être des consommateurs en ce qui concerne la collecte de données, les mises à jour logicielles et le droit à la réparation ».

La professeure Centivany a également recommandé d'exiger des fabricants qu'ils divulguent des données sur le nombre de réclamations au titre de la garantie, les motifs de ces réclamations, le coût de la réparation du problème, le délai d'apparition du problème après l'achat, et ainsi de suite. Ces renseignements permettraient aux consommateurs et aux groupes d'intérêt des consommateurs d'évaluer le coût réel de la possession d'un véhicule spécifique tout au long de sa durée de vie et de comparer les véhicules entre eux. Comme ces données sont déjà collectées par les fabricants, cette obligation ne serait pas particulièrement onéreuse à mettre en œuvre. Cette idée est potentiellement complémentaire de la notion d'indice de réparabilité, qui pourrait être attribué aux véhicules pour indiquer dans quelle mesure ils sont faciles et coûteux à réparer, une idée qu'Option Consommateurs approuve.

Option consommateurs et la professeure Centivany ont également souligné l'importance de soutenir la réparation indépendante. Elle a fait remarquer que la plupart des réparations sont effectuées au niveau local et qu'elles nécessitent des techniciens qualifiés; toutefois, « ces restrictions sur la réparation durent depuis suffisamment longtemps pour que les réparateurs aient été écartés du marché ». Pour résoudre ce problème, il est nécessaire d'investir dans des programmes de formation pour des réparateurs qualifiés au sein des communautés locales.

Les parties ont été généralement pessimistes quant à l'autorégulation. OpenMedia a elle aussi souligné l'importance de l'adoption d'un cadre réglementaire, mais en l'absence d'une telle réglementation, elle a plaidé pour que l'industrie développe et adopte « des normes et des protocoles ouverts pour les logiciels et les données des véhicules afin d'empêcher l'enfermement propriétaire (*vendor lock-in*) et de promouvoir la

concurrence ». Elles ont également appuyé l'idée du partage volontaire des données de diagnostic par les acteurs de l'industrie et la création « d'alternatives open source aux outils et logiciels de réparation propriétaires » qui « augmenteraient la transparence et permettraient un plus grand contrôle par l'utilisateur et une meilleure réparabilité ».

7.4 Faits saillants

Dans cette section, nous avons sollicité l'avis de sept intervenants sur les résultats de notre recherche. Ces intervenants ont souligné la gravité de plusieurs des risques identifiés dans le rapport et ont insisté sur la nécessité de les traiter rapidement.

En ce qui concerne la protection de la vie privée, les intervenants ont souligné les risques associés à la collecte massive de données par les fabricants ainsi qu'à leurs utilisation et partage. Cette pratique mène à une intrusion importante dans la vie privée des consommateurs. En outre, ils ont souligné le fait que les consommateurs n'ont pas le choix de refuser ou de consentir à ces pratiques et qu'ils doivent essentiellement s'y soumettre à ces pratiques. En effet, même si les consommateurs sont théoriquement invités à donner leur consentement, celui-ci est miné dans ce contexte par les déséquilibres de pouvoir entre les parties, l'absence de choix véritable et le manque de compréhension des pratiques en question. Les intervenants ont évoqué quelques solutions potentielles : une plus grande transparence de la part des fabricants, une meilleure éducation des consommateurs et, surtout, une législation contraignante qui limite la collecte de données et qui donne des pouvoirs d'exécution renforcés aux autorités réglementaires responsables. Certains intervenants ont également mis l'accent sur la notion de « *privacy by design* » et sur la reconnaissance de la vie privée en tant que droit fondamental.

Les intervenants ont également parlé de l'impact de la connectivité sur les droits de propriété des consommateurs. Tout d'abord, ils ont discuté le fait que la connectivité permet aux fabricants de contrôler à distance le logiciel et les fonctionnalités du véhicule, et ce, même après son acquisition par le consommateur. Tous les intervenants qui se sont exprimés sur cette question ont souligné la gravité de cette pratique. En effet, elle remet en cause la notion même de propriété ou d'acquisition d'un bien. Certains ont également noté que la connectivité créait un risque d'obsolescence prématurée, ainsi que des risques en matière de sécurité.

L'impact de la connectivité et des verrous numériques sur la réparation a également été souligné. Tous les experts qui se sont exprimés sur cette question ont convenu que l'utilisation de la connectivité ou des verrous numériques pour limiter la réparation des véhicules était anticoncurrentielle. Ils ont rejeté l'argument que les besoins de sécurité justifiaient les restrictions imposées par les fabricants à la réparation des véhicules.

Plusieurs solutions à ces problèmes ont été proposées : adopter des lois pour encadrer les clauses dans les contrats de licence d'utilisateur final, obliger les fabricants à partager les données diagnostiques avec les consommateurs et les réparateurs indépendants, clarifier et ajouter des garanties légales pour le consommateur, etc. Tous les intervenants se sont montrés favorables à la législation québécoise, en particulier aux dispositions obligeant les fabricants à partager les données de diagnostic.

Les intervenants ont convenu que la *Loi sur le droit d'auteur* devrait être modifiée pour permettre le contournement des verrous numériques dans le contexte de la réparation, mais ils ont également fait valoir que le Canada avait besoin d'une législation positive sur le droit à la réparation. Cette législation pourrait promouvoir la réparation en interdisant l'utilisation de verrous numériques dans certains contextes ou en exigeant que les véhicules soient conçus pour favoriser la réparation.

En résumé, notre discussion avec les intervenants a mis en évidence le fait que les véhicules connectés posent de multiples risques substantiels pour les droits des consommateurs et que ces risques doivent être traités de toute urgence.

8 Conclusions et recommandations

8.1 Conclusions

Presque tous les nouveaux véhicules mis sur le marché sont maintenant connectés et les consommateurs canadiens sont de plus en plus contraints d'acquérir des véhicules dotés d'une connexion au monde externe. Toutefois, notre société et nos lois ne sont pas adaptées pour ce développement. Notre recherche nous amène à la conclusion que les risques que présente la voiture connectée pour les consommateurs sont importants et urgents et qu'ils doivent être atténués.

Les problèmes causés par la connectivité dans les voitures sont multiples : intrusion massive dans la vie privée des consommateurs, impliquant la surveillance et la manipulation par les entreprises et potentiellement par l'État, ainsi que la commercialisation d'informations privées et hautement sensibles. Perte de contrôle et de prévisibilité sur le bien acquis par le consommateur (dans ce cas, un bien qui coûte cher et qui est souvent indispensable). Exigence de frais pour avoir accès à certaines fonctionnalités d'un produit que l'on a déjà acquis. Perte du droit de réparer ses propres biens ou de les faire réparer par la personne de son choix. Exclusion des mécaniciens indépendants et des fabricants de pièces de réparation du marché par les fabricants automobiles, ce qui fait grimper les coûts de la réparation et réduit l'innovation. Diminution de la durabilité et de la réparabilité. Risques pour la cybersécurité et la sécurité physique. La liste est longue.

L'encadrement législatif canadien est actuellement inadéquat pour gérer ces risques et protéger les consommateurs. Nous concluons que des réformes devraient être entreprises rapidement, pour assurer la protection des consommateurs en ce qui concerne notamment leurs droits à la vie privée, à la propriété de leurs biens et à la réparation.

Le fardeau de l'atténuation de ces risques ne peut pas être placé sur les consommateurs. Les problèmes découlent essentiellement de la conception des véhicules et des choix faits par les fabricants automobiles. Il est absurde de maintenir que les consommateurs puissent exercer quelque pouvoir à cet égard ; quel consommateur peut obliger un fabricant à concevoir son véhicule en tenant compte de la réparabilité, du respect de sa vie privée ou de ses droits de propriété ? Quel consommateur peut exiger du fabricant qu'il mette fin à ses pratiques de collecte, d'utilisation et de partage des renseignements personnels, ou qu'il donne accès aux données diagnostiques à un réparateur tiers ? Et pourtant, le cadre législatif actuel fait peser sur le consommateur la plus grande partie des responsabilités. Le contexte législatif canadien fait peu pour empêcher les fabricants de se livrer aux pratiques identifiées, à l'exception de quelques règles dans la législation sur la protection de la vie privée et de la nouvelle loi québécoise sur le droit à la réparation. Actuellement, l'une des seules protections du consommateur est qu'il doit consentir (ou non) aux politiques de protection de la vie privée et aux accords de licence d'utilisateur final avant la collecte, l'utilisation ou le partage de ses données et de celles du véhicule ; en matière de réparation, le gouvernement fédéral vient d'adopter une règle disant que le consommateur peut contourner un verrou numérique s'il doit réparer son véhicule et que

le verrou entrave sa capacité de le faire. Comme nous l'avons vu, ces droits sont pratiquement dénués de sens dans ce contexte. Le consommateur n'a ni choix, ni pouvoir de négociation, ni les compétences nécessaires pour mettre en œuvre ces droits dans le contexte de la voiture connectée.

Les véhicules sont des biens complexes qui sont réglementés afin de garantir une conception adéquate et de minimiser les risques en matière d'environnement et de sécurité. Avec l'introduction de la connectivité dans les véhicules, ces réglementations doivent aller plus loin en termes de réparation et s'étendre à la vie privée et au contrôle du véhicule et de son logiciel après prise de possession par le consommateur.

Ces règles doivent être établies par l'État. C'est l'industrie qui a créé ces problèmes et qui a d'importantes incitations financières à les perpétuer. Nous n'avons vu aucun signe d'un intérêt à les atténuer. Puisque l'industrie ne résoudra pas nécessairement ces problèmes et que les consommateurs ne peuvent pas le faire seuls, les gouvernements doivent en assumer la responsabilité.

En particulier, nous demandons au gouvernement fédéral d'intervenir au stade de la conception des véhicules. Bon nombre des problèmes identifiés dans ce rapport sont liés à des éléments qui sont introduits au stade de la conception des voitures connectées. Les véhicules pourraient être conçus pour promouvoir la cybersécurité, la protection de la vie privée et la réparabilité, mais ce n'est pas le cas. L'État devrait enquêter sur ces pratiques et établir de meilleures normes pour la conception des véhicules, si nécessaire. Par exemple : la pratique consistant à conserver les données des consommateurs sur les serveurs des fabricants présente-t-elle plus de risques que d'avantages ? Serait-il préférable de stocker les données diagnostiques localement, dans le véhicule, plutôt que sur un serveur centralisé afin de donner un plus grand contrôle aux consommateurs en ce qui concerne la réparation ? Comment la conception du véhicule peut-elle être optimisée pour assurer une meilleure réparation ou une meilleure compatibilité entre la voiture et des pièces ou des logiciels tiers ?

Enfin, bien que notre rapport se soit concentré sur les véhicules, nos recherches indiquent que les problèmes identifiés s'étendent à tous les biens connectés. Dans l'ensemble, nous devons, en tant que société, réfléchir à ce qu'implique la protection des consommateurs dans un monde qui est de plus en plus connecté. Les consommateurs risquent de perdre des droits importants relativement à la vie privée et à la propriété lorsque des biens deviennent connectés. Pour éviter cette situation, il pourrait être nécessaire d'imposer des responsabilités strictes aux fabricants en ce qui concerne la collecte et l'utilisation des renseignements personnels, le maintien du contrôle sur le logiciel d'un bien après sa vente ainsi que la réparabilité, et ce, pour tout bien connecté.

8.2 Recommandations

Attendu que les véhicules sont des biens de consommation importants, du fait de leur coût élevé et de leur caractère essentiel pour de nombreux consommateurs ;

Attendu que presque tous les nouveaux véhicules sur le marché nord-américain sont maintenant connectés dans une certaine mesure ;

Attendu que la connectivité permet aux fabricants automobiles de se livrer à un certain nombre de pratiques qui présentent des risques pour les consommateurs ;

Attendu que les consommateurs ne sont pas au courant de ces pratiques et ne sont pas en mesure d'atténuer ces risques ;

Attendu que les fabricants de véhicules ne sont apparemment pas disposés à atténuer ces risques sans y être contraints par la loi ;

Union des consommateurs recommande aux législateurs du Canada, provinciaux ou fédéral, selon le cas, d'adopter des mesures spécifiques pour réglementer les voitures connectées, en suivant les recommandations présentées ci-dessous. Nous recommandons également que toutes les législations provinciales soient harmonisées, notamment pour que tous les Canadiens bénéficient des mêmes protections.

En outre, étant donné l'applicabilité de nos conclusions et de nos recommandations à tous les biens connectés, nous recommandons également que les législateurs du Canada adoptent des réglementations équivalentes qui s'étendent à tous les biens connectés.

8.2.1 La protection de la vie privée

Attendu que la connectivité permet aux fabricants automobiles de collecter des quantités massives de données à partir des véhicules, y compris des renseignements personnels et des informations très sensibles ;

Attendu que certains de ces renseignements personnels sont difficiles, voire impossibles, à anonymiser ;

Attendu que les fabricants utilisent ces données non seulement pour fournir des services connectés au consommateur, mais aussi à des fins vaguement définies qui n'ont aucune relation apparente avec le consommateur ou le véhicule en question, comme la sécurité, le marketing et la recherche ;

Attendu que les fabricants vendent ou partagent les renseignements personnels des consommateurs avec des tiers, tels que les assureurs, l'État et les courtiers en données ;

Attendu que les tiers utilisent également ces données à des fins commerciales, les agrègent avec d'autres données, les partagent avec d'autres tiers, etc. ;

Attendu que ces pratiques constituent une intrusion massive dans la vie privée des consommateurs et présentent divers risques pour eux en lien avec le profilage, la surveillance, la publicité ciblée et la manipulation ;

Attendu que les données ainsi collectées sont sujettes à des cyberattaques et à des fuites de données ;

Attendu que la grande majorité de ces pratiques n'est pas interdite par la législation canadienne sur la protection de la vie privée pour autant que le consommateur y « consente » et que la collecte de données ne soit pas intrinsèquement « déraisonnable » ou « illégitime » ;

Attendu que ces pratiques sont généralement inconnues ou mécomprises par les consommateurs avant, lors de ou après l'acquisition du véhicule ;

Attendu que ces pratiques ne sont divulguées que partiellement par le biais des politiques de protection de la vie privée, qui sont souvent complexes, vagues et incomplètes ;

Attendu que la législation canadienne sur la protection de la vie privée autorise le consentement implicite dans la plupart des contextes, ou que les consommateurs peuvent « consentir » en signant un document ou en cliquant sur un bouton sans que ces pratiques qui y sont mentionnées au passage aient été portées à leur connaissance ;

Attendu que les risques associés à ces pratiques sont généralement difficiles à évaluer pour les consommateurs ;

Attendu que les consommateurs n'ont guère le choix d'accepter ou de refuser ces pratiques lors de l'acquisition d'un véhicule, même s'ils en ont connaissance, étant donné que tous les fabricants ont des pratiques similaires et que presque tous les véhicules neufs comportent ces risques ;

Attendu que les consommateurs n'ont pas nécessairement le choix d'accepter ou de refuser ces pratiques une fois le véhicule acquis, puisque les fabricants ne permettent généralement pas aux consommateurs de s'y soustraire sans perdre l'accès à tous les services connectés et autres fonctionnalités du véhicule ;

Attendu que les consommateurs n'ont généralement pas la possibilité de consentir au partage des données avec des tiers nommés, ni à leurs pratiques ni à leur partage de données avec d'autres tiers ;

Attendu que le caractère raisonnable de la collecte ou de l'utilisation des renseignements personnels est contextuel et qu'il est décidé par le fabricant, sous réserve d'une révision a posteriori par un commissaire à la protection de la vie privée, alors que ces pratiques ont déjà été mises en œuvre ;

Union des consommateurs recommande aux législateurs du Canada d'adopter ou de modifier la législation en matière de protection de la vie privée afin qu'elle prévoie :

- L'adoption d'une définition de l'anonymisation qui n'inclut que les données qui ne peuvent pas être réidentifiées, même lorsqu'elles sont agrégées avec d'autres ensembles de données ;

- L'adoption des limites à l'utilisation des données anonymisées aux fins sérieuses et légitimes ;
- L'interdiction totale de la collecte et de l'utilisation de certains types de renseignements personnels sensibles et révélateurs par les fabricants automobiles, tels que les données de localisation détaillées ou les données relatives aux habitudes de conduite, sauf dans des cas limités où les données sont nécessaires pour fournir un service pour lequel le consommateur a explicitement opté ;
- L'interdiction totale de la collecte des renseignements personnels qui ne sont pas nécessaires pour le fonctionnement du véhicule ou des services connectés ;
- L'interdiction totale de la collecte de renseignements personnels sur des personnes qui ne sont pas en mesure de donner leur consentement ou à qui il n'est pas demandé ;
- L'interdiction totale de l'utilisation et du partage des renseignements personnels à des fins qui ne sont pas liées au fonctionnement du véhicule ou des services connectés sans l'accord explicite du consommateur ;
- L'interdiction totale du partage des renseignements personnels, sans l'accord explicite du consommateur, avec des tiers qui ne fournissent pas un service au consommateur ou qui n'offrent pas de service directement lié au fonctionnement du véhicule ;
- L'interdiction totale du partage des données par des tiers avec d'autres parties sans le consentement explicite du consommateur donné directement et explicitement au tiers ;
- Renforcer les pouvoirs du Commissaire à la protection de la vie privée (et de ses équivalents provinciaux) pour surveiller le respect de ces règles et pour sanctionner toute violation.

En ce qui concerne la conception du véhicule, nous recommandons au législateur fédéral d'adopter une législation qui prévoit :

- Que les fabricants donnent aux consommateurs un contrôle granulaire sur la collecte et l'utilisation des données par leurs véhicules afin qu'ils puissent opter pour la connectivité à certaines fins (telles que l'assistance d'urgence) et la collecte et l'utilisation de leurs données à ces fins, sans opter pour la collecte et l'utilisation de leurs données au-delà de ces fins ;
- Que les fabricants donnent aux consommateurs le choix de désactiver toute connectivité et donc toute collecte de données par le fabricant, sans que cela affecte autrement le fonctionnement de l'automobile ;
- Que la collecte et l'utilisation des données soient désactivées par défaut et qu'elles ne soient activées que si le consommateur y consent expressément ;
- Que les fabricants informent explicitement les consommateurs des pratiques de collecte et d'utilisation des données, ainsi que des risques qui y sont associés, et de leur droit de retirer leur consentement à la collecte ou à l'utilisation de leurs données ou de déconnecter entièrement leur véhicule du réseau cellulaire ou d'Internet.

Nous recommandons également que le gouvernement fédéral établisse, en consultation avec des experts technologiques et des experts en protection de la vie privée, des normes minimales et obligatoires pour la mise en œuvre des principes de protection de la vie privée dès la conception.

8.2.2 Les droits de propriété et de réparation

Concernant le contrôle du bien après la vente

Attendu que le transfert de propriété qui s'opère lors de l'achat d'un véhicule confère normalement au propriétaire un certain nombre de droits, tels que le droit d'utiliser le bien dans les limites de la loi, de l'aliéner, de le réparer, etc.

Attendu que les fabricants et les vendeurs de biens contenant des logiciels maintiennent les droits de propriété sur le logiciel du bien après la vente de ce dernier, par le biais de contrats de licence de l'utilisateur final (CLUF) ;

Attendu que les CLUF restreignent la manière dont le logiciel du bien peut être utilisé par le propriétaire de ce bien, même après son acquisition ;

Attendu que ces restrictions sur le logiciel du bien peuvent être utilisées pour limiter les droits du consommateur sur le bien qu'il a acquis, y compris son droit d'utiliser ou de réparer le bien ;

Attendu que la connectivité permet aux fabricants de surveiller l'utilisation des biens connectés et de leur logiciel et d'appliquer à distance des restrictions relatives à leur utilisation ;

Attendu que la connectivité permet aux fabricants, à distance, de mettre à jour le logiciel et de changer les fonctionnalités du bien, par exemple en bloquant ou en débloquent certaines fonctionnalités ou certains services, ou même de le contrôler à distance ;

Attendu que ce contrôle à distance permet au fabricant de modifier les conditions d'usage du bien ou du service après l'acquisition du bien par le consommateur, par exemple en bloquant ou en modifiant les fonctionnalités qui ont été incluses lors de la vente ;

Attendu que ces pratiques portent atteinte aux droits de propriété et érodent les droits des consommateurs par rapport aux biens qu'ils ont acquis, et qu'elles peuvent avoir de graves conséquences financières et autres pour les consommateurs ;

Attendu que les consommateurs ne sont généralement pas au courant de ces pratiques et de ce qu'elles impliquent, lorsqu'ils acquièrent un véhicule ;

Attendu que les consommateurs ne peuvent pas consentir à ces pratiques ;

Attendu qu'il n'existe que peu ou pas de législation encadrant ces pratiques ;

Union des consommateurs recommande aux législateurs du Canada d'adopter une législation qui :

- Interdit les clauses dans les CLUF qui limitent le droit du consommateur propriétaire d'avoir le contrôle exclusif de sa voiture ou de la réparer ;
- Interdit les clauses dans les CLUF qui permettent, par modification logicielle, d'imposer des restrictions à l'utilisation du bien ou de ses fonctionnalités après la vente du bien ;
- Interdit aux fabricants de traiter les fonctionnalités physiques incluses dans le véhicule (comme les sièges chauffants, l'autonomie de la batterie, etc.) comme des services dont les conditions peuvent être modifiées au fil du temps ;
- Interdit aux fabricants d'exercer un contrôle direct sur un bien, à distance, sauf suite à une demande expresse du consommateur ;
- Interdit aux fabricants de modifier à distance une fonctionnalité du véhicule de manière à réduire sa durée de vie ou celle de ses pièces.

En outre, en ce qui concerne l'obsolescence

Attendu que les voitures connectées peuvent devenir prématurément obsolètes si elles ne sont pas correctement mises à jour ;

Attendu que les biens ou services connectés peuvent cesser de fonctionner si la fonctionnalité repose sur le serveur du fabricant et que ce serveur est en panne ou abandonné par le fabricant ;

Union des consommateurs recommande aux législateurs canadiens d'adopter ou de modifier la législation pour assurer que les fabricants de véhicules connectés aient l'obligation de fournir les logiciels et les mises à jour pour les véhicules après leur vente, et ce, pendant une période raisonnable déterminée par la réglementation.

Union des consommateurs recommande également au gouvernement fédéral d'établir, en consultation avec des experts en technologie, de développer et de mettre en œuvre une solution pour maintenir les services dans le cas où un fabricant automobile cesse ou refuse d'offrir un service hébergé sur son serveur.

En outre, en ce qui concerne les verrous numériques

Attendu que les voitures ont une longue durée de vie et nécessitent des réparations et des entretiens réguliers ;

Attendu que les fabricants automobiles utilisent des mesures techniques de protection (MTP) pour restreindre l'accès à la réparation des véhicules de plusieurs manières, par exemple en exigeant l'utilisation d'un logiciel pour permettre d'effectuer les réparations et changer les pièces ;

Attendu que ces restrictions sur la réparation limitent la capacité des consommateurs et des mécaniciens indépendants à effectuer des réparations et donnent un avantage en cette matière aux fournisseurs et à leurs concessionnaires ;

Attendu que l'absence de concurrence dans le domaine de la réparation limite le choix des consommateurs et fait grimper les coûts ;

Attendu que les consommateurs attachent une grande importance à la possibilité de choisir leur technicien de réparation ;

Attendu que les restrictions à la réparation et à l'interopérabilité limitent également l'innovation et la concurrence sur le marché secondaire de la réparation et de l'entretien ;

Attendu que l'interopérabilité et l'utilisation de normes ouvertes encouragent l'innovation et la concurrence ;

Attendu que le contournement des MTP qui restreignent l'accès à l'œuvre (le logiciel) est interdit par la *Loi sur le droit d'auteur* ;

Attendu que cette interdiction a pour effet de limiter l'accès à la réparation et la conception de pièces interopérables pour les voitures connectées ;

Attendu que la *Loi sur le droit d'auteur* a été récemment modifiée par le gouvernement fédéral pour permettre aux particuliers de contourner les MTP à des fins de réparation non commerciales ou d'interopérabilité ;

Attendu que la plupart des réparations et le développement de pièces de rechange ne sont pas effectués par des particuliers, mais plutôt par des techniciens qualifiés ou des acteurs commerciaux ;

Attendu que la *Loi sur le droit d'auteur* vise en général à protéger les œuvres contre les utilisations non autorisées telles que la reproduction et la distribution, et non à limiter l'accès à une œuvre par une personne qui dispose d'une licence ;

Attendu que l'un des objectifs de la *Loi sur le droit d'auteur* est d'encourager l'innovation ;

Union des consommateurs recommande au législateur fédéral de modifier la *Loi sur le droit d'auteur* afin d'éliminer les dispositions interdisant le contournement des MTP qui restreignent l'accès aux œuvres.

En outre, en ce qui concerne la réparabilité des voitures dès la conception

Attendu que les MTP sont intégrées dans les véhicules en raison de choix de conception délibérés par les fabricants pour restreindre l'accès au logiciel et pour créer des obstacles à la réparation ;

Attendu que le contournement des MTP demande du temps et des compétences ;

Attendu que la conception qui favorise le plus la réparation est celle qui n'utilise pas de MTP en premier lieu ;

Attendu qu'il n'existe au Canada aucune interdiction légale d'utiliser des techniques ayant pour effet de rendre plus difficile pour le consommateur d'entretenir ou de réparer un bien, sauf dans la *Loi sur la protection du consommateur* québécoise ;

Union des consommateurs recommande aux législateurs provinciaux ou au législateur fédéral d'adopter une disposition comme celle intégrée dans la *Loi sur la protection du consommateur* québécoise, qui interdise l'utilisation de techniques ayant pour effet de rendre plus difficile la réparation ou l'entretien d'une automobile.

En outre, nous recommandons l'adoption d'une réglementation qui oblige les fabricants à partager les outils de réparation, y compris les logiciels, avec les consommateurs et les réparateurs gratuitement ou à coût raisonnable.

En outre, nous recommandons au gouvernement de consulter des experts techniques et en matière de réparation en vue de l'élaboration de normes visant à garantir de meilleures réparabilité, ouverture et interopérabilité dans la conception des véhicules. Nous recommandons que ces normes, une fois élaborées, aient force de loi.

En outre, en ce qui concerne les données de diagnostic

Attendu que les fabricants restreignent également la réparation des véhicules en limitant l'accès des consommateurs et de leurs représentants aux données de diagnostic, que ce soit en refusant purement et simplement l'accès, en imposant des prix exorbitants ou d'autres conditions d'accès restrictives ;

Union des consommateurs recommande aux législateurs provinciaux ou au législateur fédéral d'adopter une législation telle que la disposition de la *Loi sur la protection du consommateur* québécoise qui établit le droit du consommateur d'accéder à et d'utiliser les données de diagnostic de son véhicule. Nous recommandons également que toutes les législatures, y compris celle du Québec, adoptent des règles selon lesquelles l'accès à ces données ne puisse être subordonné à des limites anticoncurrentielles ou à d'autres limites prohibitives (telles que des coûts élevés, des frais d'abonnement, etc.).

En outre, nous recommandons au gouvernement de consulter des experts indépendants en réparation et des représentants des intérêts des consommateurs sur le renforcement des droits des consommateurs à leurs données de diagnostic.

Équipe de recherche

Analystes : Mmes Julia Atack et Anne-Marie Leblanc

Révision : M. Marcel Boucher

Évaluation de la méthodologie : M. Marc Lacoursière

Coordination : M. Maxime Dorais

Nos remerciements à l'Association pour la protection des automobilistes (APA) ainsi qu'à tous ceux et toutes celles qui ont contribué de près ou de loin à la réalisation de ce rapport de recherche.

Union des consommateurs a reçu du financement en vertu du Programme de contributions pour les organisations sans but lucratif de consommateurs et de bénévoles d'Innovation, Sciences et Développement économique Canada. Les opinions exprimées dans ce rapport ne sont pas nécessairement celles d'Innovation, Sciences et Développement économique Canada ou du gouvernement du Canada.

LA FORCE D'UN RÉSEAU

ASSOCIATIONS MEMBRES :

ACEF Appalaches – Beauce – Etchemins

ACEF de l'Est de Montréal

ACEF de Laval

ACEF du Grand-Portage

ACEF du Sud-Ouest de Montréal

ACEF du Nord de Montréal

ACEF Estrie

ACEF Lanaudière

ACEF Montérégie-Est

ACEF de Québec

ACEF Rive-Sud de Montréal

Espace Finances Lévis

Centre d'intervention budgétaire et sociale (CIBES) de la Mauricie

Service d'Aide au Consommateur (Mauricie)

ASSOCIATIONS AFFILIÉES :

Association des consommateurs pour la qualité dans la construction (ACQC)

Centre d'éducation financière EBO (Ottawa)

union
des consommateurs

info@uniondesconsommateurs.ca
uniondesconsommateurs.ca

Téléphone : 514 521-6820
Sans frais : 1 888 521-6820
Télécopieur : 514 521-0736

7000, avenue du Parc, bureau 201
Montréal (Québec) H3N 1X1