

SOMMAIRE



La Direction générale de la politique de mobilité durable et de l'électrification du ministère des Transports étudie les implications éthiques des voitures connectées et des systèmes de transport intelligents. Pour y arriver, elle a soumis, en mars 2019, plusieurs questions à l'attention de la Commission de l'éthique en science et en technologie. Le présent document offre des pistes de réponse à ces questions. Le tableau suivant synthétise les questions posées et les réponses de la Commission :

Résumé des pistes de réponse aux questions spécifiques du MTQ

Questions posées	Réponses et sections clés du document où elles sont développées
Quels types d'information le manufacturier automobile peut-il collecter à propos des véhicules connectés et de leurs utilisateurs ?	• Imposer une limite stricte sur les types d'information qu'un manufacturier peut collecter serait peu judicieux. C'est davantage l'usage des données qui cause problème. • Appliquer un principe de proportionnalité entre les moyens et les fins pour les données collectées. En gros, les véhicules connectés ne devraient pas collecter des données qui ne servent pas des objectifs justifiés, précis et démontrés (§4.5).
Comment faire en sorte que les utilisateurs comprennent suffisamment les modalités de collecte des données par les véhicules pour pouvoir y consentir de manière libre, éclairée et continue ?	• Mettre de l'avant des politiques pour que les utilisateurs de véhicules connectés aient plus facilement accès aux informations pertinentes et aux paramètres de transfert de données. Ces politiques auront pour effet de réduire la charge mentale des consommateurs, des vendeurs et des loueurs de véhicules (§4.2-4.3). • Accroître la transparence des manufacturiers contribuerait aussi à la qualité du consentement (§4.8).
L'utilisateur devrait-il être en mesure de limiter ou d'empêcher la collecte de données personnelles ?	• S'assurer que les compagnies impliquées dans le développement de véhicules connectés et de STI respectent les mesures de protection de la vie privée dans la conception des objets (<i>privacy by design</i>). • Ces principes permettraient à l'utilisateur de limiter ou d'empêcher la collecte de données via, par exemple, des mécanismes comme le « mode déconnecté » (§4.6).
Quelles obligations pourraient s'appliquer aux manufacturiers quant au traitement des données ?	• S'assurer que l'utilité collective attendue résultant du stockage, de la concentration, du traitement ou de la vente des données compense pour les risques de sécurité et de violation de la vie privée des utilisateurs (§4.7).
À supposer que les manufacturiers stockent les données du véhicule sur un serveur externe, les entreprises québécoises du secteur automobile, devraient-elles y avoir accès ?	• En vertu des principes de <i>privacy by design</i>, le fait de stocker les données du véhicule sur un serveur externe est moins qu'idéal (§4.6 et §5). • Si les consommateurs acceptent un stockage externe de leurs données et si les risques économiques découlant de cette pratique sont trop importants pour les entreprises québécoises, il est envisageable de donner accès à ces données aux entreprises d'ici à titre d'<i>infrastructures essentielles</i> (§5).
Quel niveau de protection doit-être exigé pour les véhicules connectés ?	• Au-delà des lois et règlements déjà en place, des mesures de précaution devraient être respectées par les entreprises qui développent les véhicules connectés, dont le respect des mesures de protection de la vie privée dans la conception des objets (<i>privacy by design</i>) (§2.1, §4.6-4.7).
Quelles sont les responsabilités de l'État, des manufacturiers, des intermédiaires, des propriétaires et de l'État ?	• Il serait peu judicieux de responsabiliser les consommateurs à outrance. • L'État et les manufacturiers doivent avoir un rôle de premier plan dans la protection de la vie privée des citoyens. L'État devrait mettre en place des politiques de protection des données personnelles (§4.1-4.2).

PISTES DE RÉPONSE AUX QUESTIONS SPÉCIFIQUES DU

MINISTÈRE DES TRANSPORTS



PROPORTIONNALITÉ

Les véhicules connectés ne devraient pas collecter des données qui ne servent pas des objectifs précis, démontrés et justifiés. Les moyens mis en œuvre à des fins (sécurité, profitabilité, etc.) doivent être proportionnels aux fins qui sont poursuivies. Tout ce qui dépasse ce qui est strictement nécessaire pour atteindre l'objectif doit être évité et le moyen qui porte le moins atteinte aux droits et libertés doit être privilégié.

UTILITÉ COLLECTIVE



L'utilité collective probable de stocker, concentrer, traiter et vendre ces données doit être supérieure aux conséquences négatives probables touchant la vie privée des utilisateurs.

ÉTAT ET ENTREPRISES RESPONSABLES



Plutôt que de responsabiliser les consommateurs à outrance, l'État et les manufacturiers doivent avoir un rôle de premier plan dans la protection de la vie privée des citoyens. L'État devrait mettre en place des politiques de protection des données personnelles.

CONSENTEMENT DE QUALITÉ



Des politiques doivent être mises de l'avant pour que les consommateurs de véhicules connectés ou de STI aient plus facilement accès aux informations pertinentes et aux paramètres de transfert de données. Ces politiques auront aussi pour effet de réduire la charge mentale des consommateurs, des vendeurs et des loueurs de véhicules.



PRIVACY BY DESIGN

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

RÔLES ET RESPONSABILITÉS

DES DIFFÉRENTS ACTEURS



CITOYENS

- Font preuve de prudence et de discernement dans la gestion de leurs données.
- Utilisent les mécanismes à leur disposition pour prendre des décisions libres et éclairées quant à la transmission de leurs informations personnelles.



ENTREPRISES DU SECTEUR DES TÉLÉCOMMUNICATIONS

- Assurent un environnement connecté sécuritaire pour les citoyens et les entreprises.



MANUFACTURIER

- Respecte et facilite le consentement pour la collecte et la transmission des données.
- Ne nuit pas à l'essor économique des garages, loueurs et vendeurs de véhicules locaux.
- Développe des technologies en conformité avec les principes de privacy by design.
- Gère les données recueillies par les véhicules selon le principe de proportionnalité.
- Est transparent dans ses actions et intentions.



ÉTAT QUÉBÉCOIS ET CANADIEN

- Encadre et régule les secteurs des transports et des télécommunications.
- Respecte la vie privée des citoyens.
- Établit les protections de base dont jouissent les citoyens.



LOUEURS ET ENTREPRISES DU SECTEUR AUTOMOBILE

- Respectent le consentement et la vie privée des citoyens.
- Gère les données recueillies par les véhicules selon le principe de proportionnalité.
- Est transparent dans ses actions et intentions.