RAPPORTS SPÉCIALISÉS DU RIVA

RIVA
CONNECTÉ. AUTOMATISÉ.

Ontario

MAI 2019

LES DONNÉES DANS LE CONTEXTE DES VCA

Défis et recommandations

Centres d'excellence de l'Ontario
Où l'avenir se réalise

TABLE DES MATIÈRES

INTRODUCTION

Pour atteindre le fonctionnement ciblé, les véhicules connectés et autonomes (VCA) dépendent fortement de flux de données diversifiées. Ces données sur le fonctionnement sont générées par les capteurs intégrés au véhicule ou proviennent d'autres sources de données accessibles grâce aux capacités de communication embarquées. Dans le cadre du rapport précédent[1], nous avons publié le premier d'une série de deux rapports spécialisés portant sur les données dans le contexte des VCA. Le premier rapport de la série abordait les différents types de données de VCA et présentait des exemples de cas pratiques et de possibilités opérationnelles. Le présent rapport est le deuxième de cette série sur les données.

Il vise à compléter le portrait en mettant en relief les difficultés que pose l'accès à cette grande quantité de données.

Même si l'accès aux données des véhicules offre une gamme d'avantages et de possibilités opérationnels au chapitre de l'expérience de conduite et dans le domaine des services d'information, il comporte des défis auxquels il est essentiel de s'attaquer si l'on souhaite offrir aux usagers l'expérience de qualité et la sécurité qu'ils attendent des technologies des VCA. À titre d'exemple, les gens sont préoccupés par la confidentialité des données qu'ils communiquent à des tiers pour la prestation de services ou par l'accès à distance aux ressources informatiques intégrées à leurs véhicules aux fins de collecte et de traitement de données.

La cybersécurité est un autre défi de taille qui touche le fonctionnement au complet des VAC. Dans les dernières années, de

1 **Réseau d'innovation pour les véhicules automatisés. (2018). Data in the Context of CAVs - Types and Operational Opportunities. Récupéré de :** https://tinyurl.com/y9kkwlqy

nombreux incidents de piratage visant des véhicules connectés ont été signalés, lesquels ont intensifié les craintes du public à l'égard des VCA et engendré des pertes économiques pour les fabricants d'équipement d'origine (FEO), qui ont dû procéder à des rappels pour corriger les vulnérabilités décelées[2].

La propriété des données des VCA a également été débattue, étant donné que plusieurs entités prennent part aux processus de collecte et d'utilisation de ces données.

Compte tenu des énormes quantités de données recueillies des VCA et de la qualité variable de celles-ci, ces deux questions ont suscité l'intérêt des intervenants en recherche et développement du secteur des VCA. Heureusement, on peut les traiter en se servant des cadres et des solutions proposés dans d'autres domaines de services riches en données, comme l'Internet des objets (IdO)[3], en les adaptant aux caractéristiques et aux exigences des applications de VCA.

L'Internet des Objets (IdO) est un paradigme de réseau à grande échelle qui relie des objets intelligents connectés à l'Internet et permet de contrôler, d'identifier et de recueillir à distance des données à partir de ces objets.

Dans le précédent rapport du RIVA, nous avons traité des principaux avantages de la détection participative des données par les VCA et de l'utilisation de ces données pour fournir des services axés sur l'information. Par exemple, les capteurs intégrés peuvent servir à détecter la circulation et les conditions routières et les événements routiers relevés peuvent être signalés aux autorités, qui pourront alors intervenir rapidement. Pour faciliter un tel paradigme de collecte de données, il importe d'inciter les propriétaires de VCA à rester impliqués dans la boucle de détection participative et de collecte de données en leur offrant des récompenses.

Afin de répondre aux besoins urgents d'approfondir et de faciliter les exigences relatives à la collecte de données dans les VCA, y compris l'accès à ces données, le présent rapport attire l'attention sur les défis de taille à relever pour atteindre cet objectif.

2 **Osborne, C. (2018). The most interesting Internet-connected vehicle hacks on record. Récupéré de :** https://www.zdnet.com/article/these-are-the-most-interesting-ways-to-hack-internet-connected-vehicles/

3 **Morgan, J. (2014). A Simple Explanation of 'The Internet of Things'. Récupéré de :** https://bit.ly/2LeBA6K

Le rapport aborde les grandes préoccupations à l'égard de la confidentialité des données, la cybersécurité et la propriété des données dans les VCA, en soulignant les pratiques exemplaires en la matière et les efforts déployés pour y répondre. Il se penche également sur la difficulté à mettre en place une réglementation et des normes harmonisées pour régir l'utilisation et la représentation des données dans les VCA. Le rapport met également en lumière les enjeux relatifs au volume et à la quantité des données de VCA. Enfin, il examine le défi que pose la participation du public à la collecte des données de VCA et fait état de la nécessité d'offrir des incitatifs ou des récompenses pour enjoindre les gens à contribuer au partage des données de VCA recueillies par leurs propres véhicules.

Pour chaque défi abordé, le rapport propose des recommandations et illustre les avenues empruntées par les gouvernements et les intervenants du secteur des VCA pour y remédier.

CONFIDENTIALITÉ DES DONNÉES

Quand il est question d'accès aux données, la protection de la vie privée est cruciale. Les données recueillies ou signalées par les véhicules peuvent révéler des caractéristiques personnelles des conducteurs et des renseignements sur leurs habitudes de conduite et itinéraires, un scénario qui soulève de légitimes inquiétudes chez la population à propos du partage des données de VCA. Ainsi, lorsque des données géolocalisées sont transmises sur l'environnement, notamment sur les conditions routières, l'emplacement géographique actuel précis des véhicules desquels proviennent ces données est également communiqué. En outre, la collecte d'information sur les habitudes de conduite à des fins de gestion de parc automobile ou par des applications d'assurance fondée sur l'utilisation suscite également des préoccupations chez les conducteurs visés quant à leur vie privée. Puisque les données révèlent des caractéristiques personnelles, elles devraient être considérées comme privées et des solutions devraient être proposées pour les protéger des intrusions.

En raison du caractère essentiel de la question, des solutions conçues pour protéger la vie privée sont étudiées et présentées par les responsables de la collecte de données, les fournisseurs de services et les chercheurs du domaine de la protection de la vie privée. Certaines solutions efficaces consistent à anonymiser les données provenant du véhicule et du conducteur.

L'anonymisation et la **dépersonnalisation**[4] sont des solutions prisées pour dissimuler l'identité des fournisseurs de données et réduire la possibilité d'établir un lien entre eux et les données qu'ils ont communiquées.

Des **obligations** et des **ententes juridiques** doivent également régir les modalités de protection de la vie privée qui s'appliquent aux processus de collecte et d'utilisation des données. Avant toute collecte de données, il faut s'assurer d'obtenir le consentement de chaque participant à des fins de transparence et conformément aux ententes en matière de respect de la vie privée. Le Commissariat à la protection de la vie privée du Canada, en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), a défini sept principes directeurs dont il faut tenir compte pour obtenir un consentement valable[5]. Ces lignes directrices servent à assurer, par leur consentement, que les

4 **GDPR.Report. (2017). Data masking: anonymization or pseudonymization? Récupéré de :** https://gdpr.report/news/2017/09/28/data-masking-anonymization- pseudonymization/

5 **Commissariat à la protection de la vie privée du Canada. (2019). Lignes directrices pour l'obtention d'un consentement valable. Récupéré de :** https://https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de- renseignements-personnels/consentement/gl_omc_201805/

participants de la collecte de données sont informés des renseignements personnels qui sont recueillis, des tiers auxquels ils sont communiqués, des fins auxquelles ils sont recueillis, utilisés ou communiqués et du risque de préjudice et autres conséquences. Dans le cadre de l'obtention du consentement, il faut donner clairement aux individus la possibilité de choisir « oui » ou « non » quant aux types de données qui seront recueillies et ce à quoi elles serviront.

Afin que les pratiques de protection de la vie privée soient prises en compte dès le processus de fabrication des VCA, la Chambre des représentants des États-Unis a adopté le projet de loi H.R.3388 intitulé *Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act* (ou *SELF DRIVE Act*)[6]. Mise en application par le département des Transports des États-Unis, cette loi exige que les fabricants de véhicules mettent par écrit des plans de protection de la vie privée et de cybersécurité avant de commercialiser les véhicules. Le Comité sénatorial permanent des transports et des communications a également recommandé l'élaboration d'un cadre de travail sur les véhicules connectés, dont l'un des principaux éléments sera la protection des renseignements personnels. Le comité a par ailleurs souligné que les FEO doivent intégrer les pratiques exemplaires en matière de protection de la vie privée et de cybersécurité à l'ensemble du processus de fabrication[7].

L'évolution des technologies des VCA risque d'engendrer de nouvelles sources d'atteintes à la vie privée. Les intervenants doivent donc accorder la priorité à la protection de la confidentialité des données et s'assurer d'adapter les pratiques de protection des renseignements personnels aux avancées technologiques dans le secteur des VCA, en tenant compte de leurs répercussions. Ils doivent aussi veiller à mettre à jour les documents sur le consentement et à informer les personnes de tout ajout ou modification aux politiques et aux conditions d'utilisation. Les FEO et les développeurs de technologies doivent sans cesse s'assurer de prendre en considération la confidentialité des données à partir de la base et tout au long du processus général de conception des VCA en suivant de rigoureuses pratiques de **protection intégrée de la vie privée**[8].

La protection intégrée de la vie privée est un cadre de référence reposant sur sept principes de base qui vise à favoriser une prise en compte proactive de la protection de la confidentialité des données au cours du cycle de vie d'un système, y compris durant sa conception, son fonctionnement et sa gestion.

6 **Chambre des représentants des États-Unis. (2017). H.R.3388 – *SELF DRIVE Act*. Récupéré de :** https://www.congress.gov/bill/115th-congress/house-bill/3388

7 **Comité sénatorial permanent des transports et des communications. (2018). Paver la voie : Technologie et le futur du véhicule automatisé. Récupéré de :** https://sencanada.ca/content/sen/committee/421/TRCM/Reports/COM_RPT_TRCM_AutomatedVehicles_f.pdf

8 **Université Ryerson et Deloitte. Protection intégrée de la vie privée – Nouvelle norme de certification de protection de la vie privée. Récupéré de :** https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-fr-ers-privacy-by-design-brochure.PDF

CYBERSÉCURITÉ

Étant donné le caractère vital du fonctionnement des VCA, la cybersécurité revêt une importance majeure quand il s'agit de mettre les données et les systèmes du véhicule à l'abri des cyberattaques. Maintenant que les véhicules disposent de systèmes télématiques et communiquent avec leur environnement, les VCA sont un élément important d'un monde très connecté. Même si cette connectivité depuis et vers les véhicules offre toutes sortes de possibilités opérationnelles, elle engendre un défi manifeste sur le plan de la cybersécurité. De plus en plus connectés, les véhicules seront d'autant plus exposés aux vulnérabilités en matière de sécurité.

L'utilisation plus répandue d'applications logicielles à connexion externe dans les véhicules fera de ceux-ci des cibles de choix pour les auteurs d'attaques et les pirates informatiques. Ces derniers pourraient notamment altérer les données ou les subtiliser, perturber ou mal aiguiller les services, effectuer un détournement à distance et repérer les véhicules et les voler. Ces menaces attirent l'attention sur l'enjeu de cybersécurité propre aux VCA et le besoin d'imposer des exigences strictes en vue du stockage, du traitement et de la transmission en toute sécurité des données de VCA.

L'élaboration de **pratiques** et **normes de cybersécurité** est en cours afin de remédier aux vulnérabilités matérielles et logicielles des systèmes des VCA[9]. Les pratiques exemplaires préconisent l'intégration de règles de

9 **M. H. Eiza et Q. Ni. (2017). Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cyber Security. Récupéré de :** https://bit.ly/2HtJGF7

sécurité au cours du cycle de développement des logiciels et d'architectures tolérantes aux risques pour les données et systèmes de VCA. De plus, des normes internationales sont en train d'être élaborées ou améliorées pour contrer les menaces à la sécurité des VCA. À titre d'exemple, mentionnons la norme 1609.2 de l'Institut des ingénieurs électriciens et électroniciens des États-Unis qui définit des mécanismes pour authentifier et chiffrer les messages grâce à la technologie de communications dédiées à courte portée (CDCP)[10]. D'autres pratiques de cybersécurité suivent un modèle infonuagique pour fournir des solutions centralisées au lieu de mettre l'accent sur la protection distincte de chaque véhicule. La plateforme infonuagique conçue par Ericsson pour les véhicules connectés en est un exemple[11].

La **technologie des chaînes de blocs** a connu un essor récemment en tant que solution pouvant permettre d'améliorer la cybersécurité des VCA. S'appuyant sur une architecture répartie, de solides mécanismes de chiffrement et une rapidité d'exécution, elle semble être une avenue prometteuse pour relever le défi de la cybersécurité des VCA[12].

L'association de normalisation de l'Institut des ingénieurs électriciens et électroniciens des États-Unis (IEEE) est un organisme de l'IEEE qui élabore des normes internationales qui touchent une multitude d'industries. La série de normes 1609.x et la norme 802.11p de l'IEEE traitent de différentes fonctionnalités de la technologie de CDCP des véhicules.

Quand des vulnérabilités sont cernées, les FEO procèdent le plus souvent à des rappels de véhicules. Facilitées par la connectivité, des recommandations sont transmises aux FEO, de sorte qu'ils peuvent communiquer en toute sécurité aux véhicules les mises à jour de micrologiciels ou correctifs de sécurité par radiocommunication, au lieu d'avoir à effectuer des rappels coûteux.

À cause des graves répercussions que les menaces à la cybersécurité peuvent avoir, les gouvernements se penchent étroitement sur la cybersécurité lors de l'élaboration de leurs plans de travail et stratégies en matière de VCA. Ainsi, Transports Canada et le département des Transports des États-Unis collaborent en matière de développement de politiques et d'exigences techniques afin de concevoir une validation de principe du système de gestion des certificats de sécurité (VDP SGCS) transfrontaliers pour les véhicules

10 **Association de normalisation de l'IEEE. (2016). Norme 1609.2-2016 de l'IEEE – IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages. Récupéré de :** https://standards.ieee.org/standard/1609_2-2016.html

11 **Ericsson Connected Vehicle Cloud. Récupéré de :** https://www.ericsson.com/en/internet-of-things/automotive/connected-vehicle-cloud

12 **R. Martin. (2018). 10 Applications for Blockchain in Connected Car Automotive. Récupéré de :** https://igniteoutsourcing.com/blockchain/blockchain-automotive- industry/

13 **Gouvernement du Canada. (2016-2019). Conseil de coopération en matière de réglementation (CCR) Canada – États-Unis : plan de travail en lien avec les véhicules branchés Récupéré de :** http://tc.canada.ca/fra/lois-reglements/tc-usdot-871.html

connectés dans le cadre du plan de travail du Conseil de coopération en matière de réglementation (CCR) Canada – États-Unis en lien avec les véhicules connectés[13]. En janvier 2019, Transports Canada a créé un outil d'évaluation de la sécurité[14] à l'intention des entreprises de l'automobile pour s'assurer que les technologies pour véhicules hautement automatisés qu'elles mettent au point sont sécuritaires. Les résultats de cet outil d'évaluation sont regroupés en trois catégories qui comprennent la cybersécurité et la gestion des données. Par ailleurs, en mars 2019, Transports Canada a attribué au titre du Programme de promotion de la connectivité et de l'automatisation du système de transports (PCAST) un contrat d'une valeur pouvant aller jusqu'à 1,3 million de dollars à ESCRYPT pour permettre l'élaboration d'un système de gestion des certificats de sécurité canadien (SGCS) pour les véhicules connectés[15]. La Stratégie nationale de cybersécurité annoncée dans le Budget de 2018 du Canada marque un autre effort visant à promouvoir la cybersécurité au sein du monde numérique canadien[16].

Aux États-Unis, la National Highway Traffic Safety Administration du département des Transports a adopté une approche de recherche à volets multiples qui s'appuie sur le cadre de cybersécurité[17] du National Institute of Standards and Technologie et incite l'industrie à améliorer le profil de cybersécurité de leurs véhicules aux États-Unis[18].

En août 2017, le ministère des Transports britannique a publié des lignes directrices en matière de cybersécurité axées sur la protection des voitures autonomes contre le piratage. En 2018, la British Standards Institution (BSI) s'est inspirée de ces lignes directrices pour élaborer une norme de cybersécurité[19] en collaboration avec des sociétés des secteurs public et privé, dont Jaguar Land Rover, Ford et Bentley, ainsi que le National Cyber Security Centre, grâce au financement du ministère des Transports.

Devant l'accélération du développement et de l'adoption de technologies de VCA, ces initiatives gouvernementales et de l'industrie doivent continuer d'élaborer des mécanismes rigoureux permettant d'examiner les possibles vulnérabilités matérielles et logicielles des systèmes des VCA et de définir une variété de moyens pour protéger les données et systèmes des VCA.

14 **Transports Canada. (2019). Évaluation de la sécurité des systèmes de conduite automatisés au Canada. Récupéré de :** https://tc.canada.ca/sites/default/files/migrated/tc_safety_assessment_for_ads_fre_s.pdf

15 **Transports Canada. (2019). Transports Canada attribue un contrat à ESCRYPT pour améliorer la confidentialité des communications et la sécurité des véhicules connectés. Récupéré de :** https://tinyurl.com/ydhzebad

16 **Sécurité publique Canada. (2018). Stratégie nationale de cybersécurité. Récupéré de :** https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-fr.aspx

17 **National Institute of Standards and Technology. Cybersecurity Framework. Récupéré de :** https://www.nist.gov/cyberframework

18 **National Highway Traffic Safety Administration (NHTSA). Vehicle Cybersecurity Récupéré de :** https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity

19 **Ministère des Transports britannique. (2018). New cyber security standard for self-driving vehicles. Récupéré de :** https://www.gov.uk/government/news/new-cyber-security-standard-for-self-driving-vehicles

PROPRIÉTÉ DES DONNÉES

Le partage de données est source de débats parmi les intervenants de l'écosystème des VCA. Certains estiment qu'il faut donner un libre accès aux données des VCA pour soutenir les efforts de recherche et de développement en cours dans le secteur. D'autres rejettent ce modèle à libre accès et recherchent les possibilités de transformer les données des VCA en occasions d'affaires[20]. La pratique exemplaire veut que la propriété des données des VCA soit accordée aux personnes qui les fournissent, peu importe si l'accès est libre ou exclusif.

La propriété des données des VCA est une question difficile qu'il faut résoudre. **Elle est complexe, car plusieurs parties prennent part aux processus de production et de collecte de données.** Par exemple, la prestation de services reposant sur l'utilisation de données issues d'une production participative, comme la surveillance de la circulation fondée sur les VCA, impliquerait les véhicules participants et le fournisseur de services de la boucle de collecte de données. Si le véhicule participant est associé à une entreprise de taxi, un tiers entrerait en jeu. Qui plus est, advenant le transfert des données recueillies sur le réseau d'un opérateur ou leur stockage sur un serveur infonuagique, d'autres acteurs risquent de disperser la propriété des données.

Lorsqu'il est question de données personnelles, il faudrait par défaut s'engager à laisser la propriété à la personne à laquelle appartiennent ces données. Le consentement légal de cette personne doit être obtenu par quiconque souhaite accéder à ces données.

La question visant à savoir à qui appartiennent les données non personnelles constitue la pierre d'achoppement de ce débat sur la propriété des données des VCA, car aucun modèle de propriété précis n'a encore été défini.

20 **Deloitte S.E.N.C.R.L./s.r.l. (2018). Connected and autonomous vehicles in Ontario – Implications for data access, ownership, privacy and security. Récupéré de :** https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/consulting/ca-EN-CVAV-Research-Final-Data-Privacy-Security-Report-20180425-AODA.PDF

À cet effet, les parties prenantes de l'écosystème des VCA se sont mises à revendiquer activement des solutions pour trancher cette question controversée et les aider à donner une assise juridique solide à leurs activités de recherche et de développement. De plus, il est recommandé de mettre sur pied des groupes de travail spécialisés chargés d'étudier de possibles modèles de propriété de données et d'élaborer des normes ou des cadres de propriété bien définis, qui tiennent compte de différents types de données de VCA, y compris des possibilités d'utilisation et des modèles d'affaires. Ces efforts de modélisation devront être constamment mis à jour pour refléter les progrès et les changements en matière de mobilité, notamment la transition vers les services de partage de véhicules ou de covoiturage. Parmi les modèles qui méritent d'être étudiés, mentionnons l'utilisation de fiducies de données. Une fiducie de données peut être un particulier ou un organisme qui agit à titre de fiduciaire et gère le processus global de gouvernance des données, dont les droits de propriété à l'égard des données. La fiducie numérique communautaire[21] mise sur pied par MaRS Solutions Lab dans le cadre du projet Quayside de Waterfront Toronto et Sidewalk Labs à Toronto, au Canada en est un exemple.

Le volet européen de la région I de la Fédération internationale de l'automobile a entrepris des efforts en ce sens en lançant la campagne Ma voiture, mes données[22]. L'objectif premier de cette campagne est de faire en sorte que les propriétaires de véhicules restent maîtres de leurs données. Pour ce faire, elle redonne du pouvoir aux propriétaires de véhicules en les sensibilisant à la connectivité et aux possibilités opérationnelles de leurs données et en veillant à ce qu'ils connaissent leurs droits de propriété à l'égard des données.

Dans son rapport sur l'avenir des véhicules automatisés au Canada présenté au Conseil des ministres responsables des transports et de la sécurité routière, le groupe de travail du Comité de soutien de la politique et de la planification (CSPP) sur les véhicules connectés et automatisés propose **d'envisager une participation intersectorielle et inter-régionale en matière de réglementation pour la conception des modèles de propriété des données de VCA.** Le groupe de travail souligne qu'une telle mobilisation faciliterait la prise de décision relative aux modèles et à leur mise en œuvre grâce aux enseignements tirés des pratiques adoptées et des défis rencontrés dans les autres secteurs riches en données et par les organismes de réglementation d'autres régions[23].

21 **MaRS Solutions Lab. (2018). A Primer on Civic Digital Trusts. Récupéré de :** https://marsdd.gitbook.io/datatrust/

22 **Fédération internationale de l'automobile – région I. La campagne Ma voiture, mes données. Récupéré de :** http://www.mycarmydata.eu/

23 **Conseil des ministres responsables des transports et de la sécurité routière. (2018). L'avenir des véhicules automatisés au Canada. Récupéré de :** https://www.comt.ca/Reports/The%20Future%20of%20Automated%20Vehicles%20in%20Canada%202018-f.pdf

RÉGLEMENTATION ET NORMES

À mesure que les VCA seront plus répandus, ils auront besoin d'un langage de données universel pour fonctionner et se connecter en continu en région transfrontalière et tirer avantage de l'Internet des véhicules (IdV) connectés à l'échelle mondiale.

Les chercheurs et les développeurs spécialisés en technologies de l'automobile sont arrivés à la conclusion que sans organisme de réglementation ou structure de gouvernance unique, les progrès technologiques réalisés dans le secteur des VCA ne convergeront jamais en continu vers un environnement automobile homogène et harmonisé[24].

En revanche, si les données des VCA sont exploitées dans un format et une structure uniformes, les avantages des VCA et les possibilités opérationnelles qu'ils offrent seront décuplés.

En ce qui concerne l'adoption d'une norme unifiée applicable aux données, il convient de mentionner les efforts menés par les organismes internationaux de normalisation comme la Society of Automotive Engineers (SAE) International[25] et l'Organisation internationale de normalisation (ISO)[26].

En plus des formats de données, des pratiques normalisées de cybersécurité et une réglementation harmonisée en matière de protection de la confidentialité des

24 **Deloitte S.E.N.C.R.L./s.r.l. (2018). Connected and autonomous vehicles in Ontario – Implications for data access, ownership, privacy and security. Récupéré de :** https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/consulting/ca-EN-CVAV-Research-Final-Data-Privacy-Security-Report-20180425-AODA.PDF

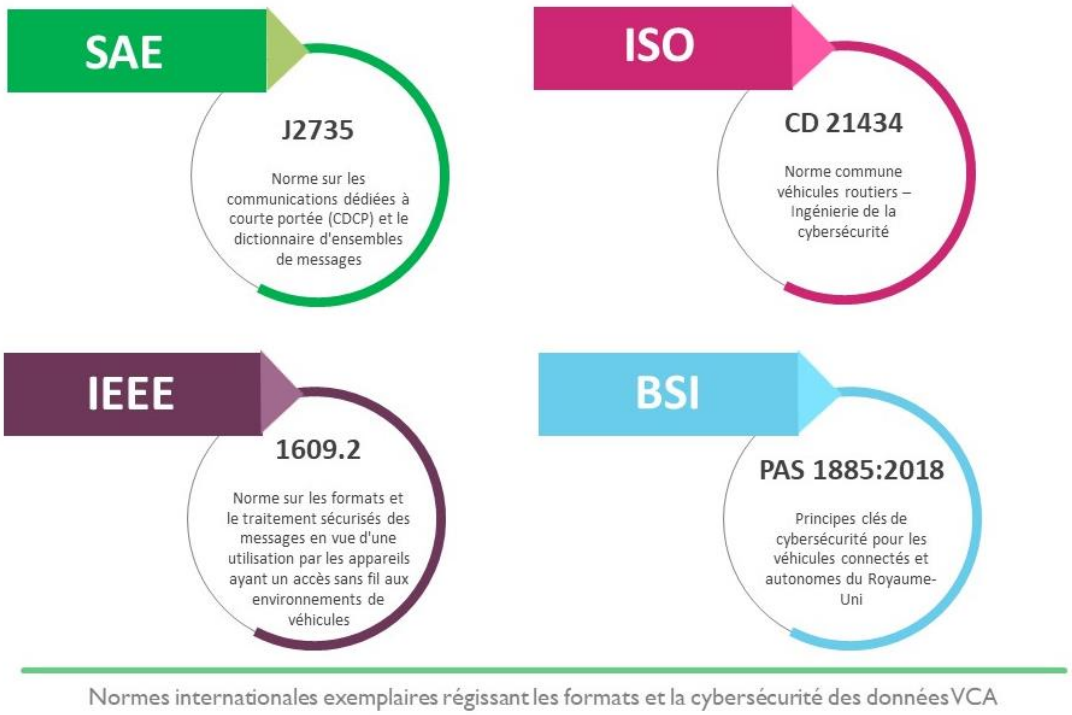
25 **SAE International. (2016). Norme J2735_201603 – Dedicated Short Range Communications (DSRC) Message Set Dictionary. Récupéré de :** https://www.sae.org/standards/content/j2735_201603/

26 **Organisation internationale de normalisation. Normes du ISO/TC 204 Systèmes de transport intelligents. Récupéré de :** https://www.iso.org/fr/committee/54706/x/catalogue/

données sont recommandées pour accélérer et faciliter la prise en compte de ces deux défis de taille liés aux données. Les recommandations mondiales sur la protection de la confidentialité des données et la cybersécurité suivent souvent celles de la NHTSA ou de l'Union européenne (UE).

Le récent règlement général sur la protection des données (RGPD) est un exemple de législation populaire de l'UE[27] pour assurer la protection de la confidentialité des données.

Pour en arriver à l'adoption de normes universelles, il est nécessaire de mettre en place des groupes de travail chargés d'analyser les points forts et les points faibles des normes existantes et de promouvoir l'adoption universelle des normes acceptées mondialement. Pour arriver à suivre l'évolution soutenue des technologies des VCA, il faut concevoir des initiatives visant à accélérer l'élaboration de normes mondiales qui assurent un équilibre entre la réglementation et l'innovation.



Normes internationales exemplaires régissant les formats et la cybersécurité des données VCA

27 **RGPD de l'UE – portail d'information.**
Récupéré de :
https://eugdpr.org/

DONNÉES MASSIVES

D'après Intel[28], un VCA acquiert environ quatre téraoctets de données en temps réel chaque jour par l'intermédiaire de ses capteurs, soit l'équivalent des données quotidiennes produites par près de 3 000 personnes. Ces données sont transmises à des modules d'intelligence artificielle (IA) aux fins d'analyse, de prise de décision et d'automatisation. De plus, la majeure partie de ces données doit être transférée à une plateforme de traitement à distance pour être analysée, surtout durant les phases d'entraînement des VCA. Étant donné que ces données sont acheminées à la plateforme d'analyse distante depuis plusieurs véhicules, cela pose un redoutable défi, car il faut **transférer, stocker** et **traiter des données.**

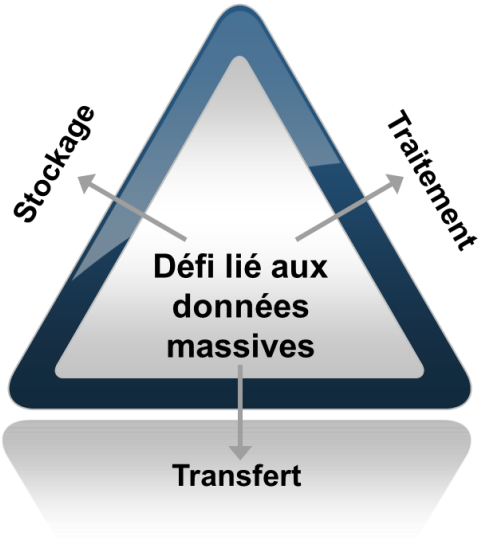
Pour ce qui est de l'IA des technologies des VCA, plus le volume de données recueillies pour entraîner et valider les systèmes autonomes est grand, plus la conduite autonome du véhicule sera précise et sécuritaire. Par ailleurs, les données ainsi recueillies peuvent être utilisées pour fournir une multitude de services axés sur l'information.

Un VCA acquiert quatre téraoctets

de données en temps réel chaque jour par l'intermédiaire de ses capteurs.

28 **Krzanich, B. (2016). Data is the New Oil in the Future of Automated Driving. Récupéré de :** https://newsroom.intel.com/editorials/krzanich-the-future-of-automated-driving/

Même si ces possibilités opérationnelles valent la peine qu'on recueille d'énormes quantités de données, des mécanismes devraient être employés pour surmonter le défi connexe lié aux données.



Par exemple, pour les **stockage,** difficultés liées au il est possible d'appliquer des mécanismes de filtrage, d'agrégation et de fusion aux données dès que les serveurs distants les reçoivent. Une fois les données filtrées et agrégées, des cadres d'informatique répartie comme Apache Hadoop[29], devraient être utilisés pour stocker les fichiers de données.

Effectuer **des recherches** dans ces volumes considérables de données représente aussi tout un défi. Heureusement, les technologies informatiques disponibles pour analyser les données massives[30] répondent à cet enjeu et intègrent des mécanismes de recherche rapide. Dans le cas des données massives, d'autres outils de structure de données peuvent être employés pour optimiser et accroître la capacité de recherche. Au nombre de ces techniques efficaces, mentionnons les filtres de Bloom[31].

Le **transfert** des données n'est pas une mince tâche non plus, car, en raison des volumes considérables transférés, il coûte très cher, consomme beaucoup d'énergie et nécessite une grande quantité de bande passante. L'exécution d'une partie de la phase d'agrégation et de filtrage des données par les unités centrales de traitement intégrées aux véhicules aide à réduire la quantité de données inutiles transférées au dépôt distant et le grand besoin de ressources connexe. Il faut accorder une grande importance à la robustesse et aux mécanismes de protection du canal de transfert des données pour prévenir les attaques et les interruptions lors du transfert des données et les retransmissions et le gaspillage de ressources qui peuvent en découler.

29 **Apache Hadoop.**
Récupéré de :
https://hadoop.apache.org/

30 **Vasist, P. (2018). 7 Trending Big Data Tools and Technologies.**
Récupéré de :
https://acadgild.com/blog/7-trending-big-data-tools-technologies

31 **Talbot, J. (2015). What are Bloom filters?**
Récupéré de :
https://blog.medium.com/what-are-bloom-filters-1ec2a50c68ff

QUALITÉ DES DONNÉES

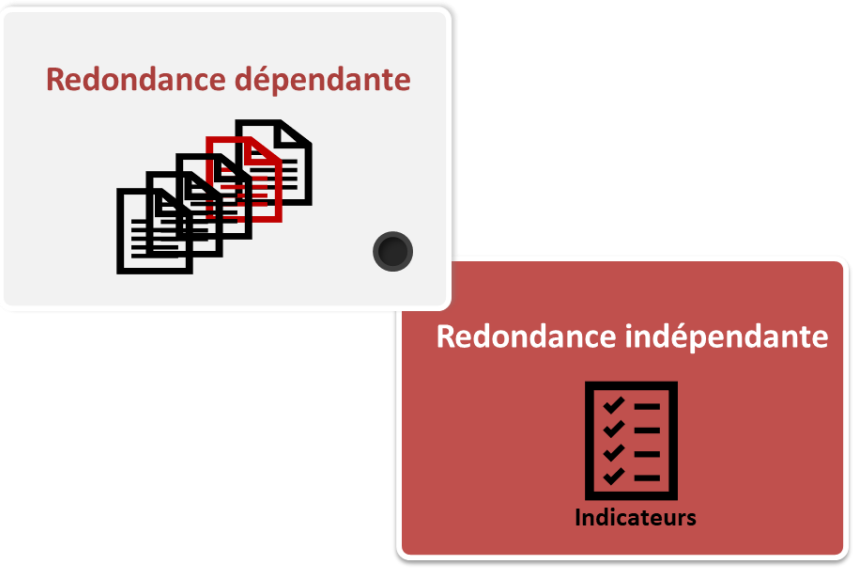
Une diversité au chapitre de la qualité des ressources matérielles et logicielles des VCA et du niveau d'engagement des conducteurs peut nuire à la qualité des données recueillies des VCA. Ainsi, parmi ces données, certaines ne pourraient être utilisées, car elles ne répondent pas aux critères d'exactitude, de pertinence ou d'actualité. Compte tenu de cette préoccupation, l'hôte des données doit disposer d'un cadre d'évaluation des données et l'appliquer aux données qu'il reçoit avant de les stocker, de les communiquer au public ou de les utiliser pour prendre des décisions. L'évaluation des données reçues permet de cerner celles qui sont de piètre qualité et de les omettre, pour ainsi éviter les répercussions liées à leur prise en compte dans les décisions guidées par les données.

Dans le domaine de l'évaluation de données, deux approches sont employées couramment : **la redondance dépendante** et **la redondance indépendante.**

La première approche est tributaire de la réception de données corrélées provenant de différents participants qui effectuent la même tâche de collecte de données. **La détection des données aberrantes**[32] est un exemple courant de cette approche. Dans le cas de la redondance indépendante, il n'est pas nécessaire de disposer des données d'autres participants. L'évaluation des données repose sur des **indicateurs de qualité** prédéterminés comme l'actualité des données et la pertinence spatiotemporelle par rapport aux caractéristiques de données recherchées.

Qu'elles aient été effectuées de manière redondante dépendante ou indépendante, les évaluations de données peuvent servir à calculer les indices de réputation des participants.

32 **Santoyo S. (2017). A Brief Overview of Outlier Detection Techniques.**
Récupéré de :
https://towardsdatascience.com/a-brief-overview-of-outlier-detection-techniques-1e0b2c19e561



Approches d'évaluation des données

Les indices associés aux participants peuvent être enregistrés et employés ultérieurement pour évaluer les données qu'ils envoient. Cette stratégie est appelée évaluation des données fondée sur la réputation[33]. Elle est devenue populaire dans les applications de détection participative parce qu'elle permet d'évaluer les données avec plus d'équité et de fiabilité que les techniques d'évaluation qui ne tiennent pas compte de l'historique des participants.

En plus de servir à l'évaluation des données, les indices de réputation des participants peuvent être utilisés à des fins de recrutement.

Après l'évaluation des données, une **rétroaction** peut être donnée aux fournisseurs à propos de la qualité de leurs données et de leur indice de réputation. Cela peut amener les participants à apprendre de leurs erreurs, pour en arriver à améliorer leur réputation et la qualité des données.

33 **Abdelhamid, S., Hassanein, H. S., Takahara, G. (2018). Reputation-aware, trajectory-based recruitment of smart vehicles for public sensing. Récupéré de :** https://ieeexplore.ieee.org/document/8011479

PARTICIPATION DU PUBLIC

Il est impossible d'exploiter pleinement le potentiel des technologies des VCA sans la participation active du public. Les données recueillies par détection participative représentent une proportion importante des données des VCA et sont fort utiles pour fournir des services fondés sur l'information. Ainsi, en utilisant les capteurs intégrés et la connectivité, les propriétaires des VCA peuvent aider à surveiller la circulation et les conditions routières et à signaler les événements routiers aux autorités ou aux fournisseurs de services.

Une telle participation du public ou collective doit être complétée par une forme de **mesure incitative**, de manière à convaincre les propriétaires de véhicules d'utiliser les ressources qui y sont intégrées à des fins de **détection participative.** Autrement dit, des récompenses devraient être garanties à ces participants en contrepartie de leur contribution constante au processus de détection participative.

Les mesures incitatives se présentes sous trois formes : 1) la volonté de servir le public, 2) la réception d'un service en contrepartie ou 3) l'obtention d'incitatifs pécuniaires[34].

Se fier seulement à la volonté des participants de servir le public ne peut garantir l'obtention de la qualité voulue ni du degré de participation nécessaire. Par conséquent, les mesures incitatives fondées sur le rendement dominent parmi les modèles de participation collective et les récompenses offertes se présentent sous différentes formes.

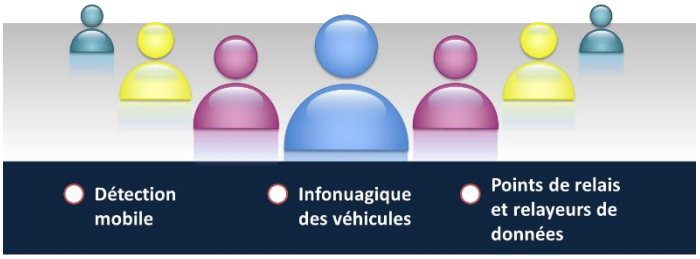
Les mesures incitatives

34 **Abdelhamid, S., Hassanein, H. S., Takahara, G. (2015). Vehicle as a Resource (VaaR).**
Récupéré de :
http://www.queenstrl.ca/uploads/4/6/3/1/4631596/2015_vehicle_as_a_resource_(vaar).pdf

Un modèle d'incitatifs populaire pour la détection participative au moyen de véhicules connectés se présente sous forme de coupons que les conducteurs peuvent utilisés par exemple pour stationner gratuitement ou emprunter des autoroutes à péage.

Quand vient le temps de déterminer la valeur des incitatifs pécuniaires, deux grandes catégories de **modèles** de **tarification** peuvent être prises en compte. La première catégorie repose sur les responsables de la collecte de données, qui, lors du recrutement, prennent soin de déterminer la valeur de la récompense attribuée à chaque participant compte tenu du niveau de participant et de la qualité des données recueillies. La deuxième catégorie de tarification est fondée sur les participants, qui doivent eux-mêmes déterminer leur récompense pécuniaire en indiquant le prix qu'il demande pour les données qu'ils ont communiquées. Le responsable de la collecte de données peut accepter, négocier ou refuser le prix demandé avant d'obtenir accès aux données.

La participation du public n'est pas envisagée seulement dans l'optique de la collecte de données des VCA. **La production participative peut aussi servir à accéder à l'ensemble des ressources des VCA et à les mettre en commun,** y compris les ressources informatiques intégrées, en tant qu'infonuagique des véhicules et de capacités de communications faisant office de points de relais et de relayeurs de données. Pour permettre d'utiliser leurs ressources à ces fins, les propriétaires de véhicules doivent recevoir des mesures incitatives et des récompenses suffisantes, tout en ayant la certitude qu'ils n'ont plus à s'inquiéter des questions de protection de la confidentialité des données et de cybersécurité.



CONCLUSIONS

Dans le présent rapport, nous avons discuté des défis de taille que posent la collecte des données des VCA et l'accès à celles-ci dans le but de faire connaître les domaines clés du secteur des VCA qui font l'objet d'efforts de recherche, de développement, de normalisation et de gestion de politiques. Nous avons également souligné certaines des pratiques exemplaires émergentes et des recommandations formulées pour s'attaquer à ces défis et ainsi offrir aux utilisateurs une expérience homogène, fiable et enrichissante lors de la communication et de la collecte de données des VCA.

Dans un premier temps, nous avons traité de l'importance de la protection de la confidentialité des données et de la cybersécurité pour le fonctionnement global des VCA. La propriété des données, qui est source de maints débats lorsqu'il est question de l'utilisation des données des VCA, a aussi été abordée. Les avantages et les difficultés que comporte la mise en place d'une réglementation et de normes harmonisées d'une région à l'autre pour définir et représenter les données des VCA ont également été présentés. Les défis que représentent le stockage, le traitement et le transfert d'énormes quantités de données de VCA et l'évaluation de la qualité de ces données ont été mentionnés comme points d'intérêt qui pourraient tirer parti des solutions existantes conçues pour d'autres domaines de services riches en données. En dernier lieu, la difficulté de faire participer le public à la collecte des données des VCA a été explorée, en mettant l'accent sur la nécessité d'offrir des incitatifs au public pour le convaincre d'intégrer la boucle de détection participative et d'y rester.

Lorsqu'on s'attaque aux enjeux actuels et tente de les régler, il faut accorder la priorité aux questions de protection de la confidentialité des données et de cybersécurité, en raison de leur caractère essentiel et des graves

répercussions qu'elles peuvent avoir sur le fonctionnement général des VCA. Des cadres de protection de la vie privée stricts doivent être pris en compte pendant la conception des VCA et le cycle complet de traitement des données pour s'assurer de ne pas dévoiler l'identité et les autres caractéristiques privées des fournisseurs de données ni faire en sorte qu'on puisse les prévoir.

Des pratiques de cybersécurité devraient être mises au point, puis déployées dans les technologies des VCA, y compris à l'échelle des véhicules, de leur infrastructure facilitante et des différents niveaux et équipements de leur chaîne d'approvisionnement.

Même si le Canada et l'Ontario ont tous deux adopté des cadres de protection de la confidentialité des données et de cybersécurité, aucun de ces cadres n'a été pleinement adapté au contexte et aux possibilités d'utilisation des VCA.

Chef de file canadien du secteur des VCA, l'Ontario est bien outillé pour diriger les efforts d'harmonisation nationale et transfrontalière de la réglementation et des politiques qui régissent l'accès aux données des VCA, leur collecte et leur utilisation dans l'optique de relever les défis connexes soulevés dans le présent rapport.

Des groupes de travail interdisciplinaires et interrégionaux peuvent être mis sur pied pour collaborer à l'atteinte de cette mission. Il faut garder ces groupes de travail en place pendant l'évolution des technologies, pour être en mesure d'adapter la réglementation et les solutions aux progrès technologiques et transformations qui en découlent.

L'ÉQUIPE DU RIVA

Raed Kadri
Directeur, Technologie automobile
et innovation de la mobilité
(416) 861 1092, poste 9-7400
raed.kadri@oce-ontario.org

Sherin Abdelhamid
Analyste, données techniques
et tendances mondiales
416 861-1092, poste 9-1097
sherin.abdelhamid@oce-ontario.org

Mona Eghanian
Gestionnaire principale, automobile
et mobilité
(416) 861 1092, poste 9-1076
mona.eghanian@oce-ontario.org

Daniel Graham
Gestionnaire, Portefeuille automobile
et mobilité
(416) 861 1092, poste 9-1107
daniel.graham@oce-ontario.org

Martin Lord
Gestionnaire principal, secteur de
l'automobile et de la mobilité
(905) 823 2020, poste 9-3236
martin.lord@oce-ontario.org

Viraj Mane
Gestionnaire, secteur
de l'automobile et de la mobilité
416 861-1092, poste 9-1073
viraj.mane@oce-ontario.org

Shane Daly
Coordinateur, Équipe de
l'automobile et de la mobilité
(416) 861 1092, poste 9-5017
shane.daly@oce-ontario.org

À PROPOS DU RIVA

L'initiative du **Réseau d'innovation pour les véhicules automatisés (RIVA)** est financée par le gouvernement de l'Ontario pour appuyer l'avantage concurrentiel de l'Ontario dans le secteur de l'automobile et renforcer sa position de chef de file nord-américain dans les technologies de pointe de l'automobile et de la mobilité, y compris les systèmes de transport et d'infrastructure.

Cette initiative mise sur le potentiel économique des technologies de véhicules connectés et autonomes (VCA) en appuyant la commercialisation de solutions de pointe conçues en Ontario qui créent des emplois, stimulent la croissance économique et améliorent la compétitivité sur le plan mondial. Le RIVA permet également d'aider les systèmes et l'infrastructure de transport de l'Ontario à s'adapter à ces nouvelles technologies. Le RIVA facilite également la planification et l'adaptation des infrastructures et des systèmes de transport de la province, en fonction de ces technologies émergentes.

PRIORITÉS

Les programmes du RIVA sont axés sur le soutien au développement et à la démonstration de technologies VCA dans les véhicules légers (p. ex., les voitures, les camions et les fourgonnettes), les véhicules lourds (véhicules commerciaux, camions, autobus et VR), les infrastructures de transport, les systèmes de transport intelligents (STI) et les systèmes de soutien du transport en commun.

Le RIVA est administré au nom du gouvernement de l'Ontario par les Centres d'excellence de l'Ontario (CEO). L'initiative comprend quatre programmes distincts et un bureau central. Les programmes du RIVA sont :

- le fonds de partenariats en recherche et développement pour les VA
- le développement des talents
- la zone pilote
- les sites régionaux de développement de technologies

Le bureau central du RIVA est constitué d'une équipe dévouée qui soutient la prestation et l'administration des programmes du RIVA et qui remplit les fonctions essentielles suivantes :

- Liaison et coordination – centre de liaison aidant à coordonner les activités entre l'industrie, le secteur de l'enseignement, les organismes de recherche et les gouvernements, en plus de mettre en contact les partenaires intéressés et les membres du public;
- Détermination des possibilités – transmission des connaissances, recherche, données et renseignements, analyse des tendances, et lien entre la technologie et les politiques;
- Sensibilisation et éducation – promotion des programmes du RIVA, des essais pilotes des VA de l'Ontario, et du secteur en pleine croissance des VCA en Ontario.

Le Réseau répond à cinq objectifs :

Nous souhaitons remercier le gouvernement de l'Ontario pour son soutien aux programmes et aux activités du RIVA.

Nous souhaitons également remercier les organismes partenaires qui travaillent avec les CEO à la prestation des programmes du RIVA, notamment les sites régionaux de développement des technologies et la zone pilote de Stratford.