Sur le radar :
Perspectives juridiques relatives aux véhicules autonomes

MARS 2018

Gérer les cyberrisques liés aux véhicules autonomes et connectés

Tout est une question de données. Elles sont devenues la nouvelle ressource « naturelle », et les véhicules ont désormais la capacité d'en recueillir et d'en stocker de grandes quantités. Cependant, l'accès non autorisé à ces données pose des risques juridiques majeurs pour l'industrie automobile.

Le risque d'atteinte à la cybersécurité des données ne concerne pas uniquement les véhicules autonomes. Les technologies déjà disponibles dans les véhicules connectés comportent les mêmes dangers. Elles offrent différents niveaux de connectivité allant des systèmes de communication et de divertissement (p. ex. SYNC de Ford, OnStar de GM, Entune de Toyota, le système CUE de Cadillac [Expérience utilisateur de Cadillac] et Uconnect de Chrysler) jusqu'à l'aide à la conduite (p. ex. rétroviseurs à caméra, freins d'urgence, freinage automatique en marche arrière, etc.).

Plusieurs études ont démontré la possibilité de « prendre le contrôle » à distance des véhicules connectés. La première cyberattaque publique de ce type remonte à 2015. Le « code » utilisé par les chercheurs leur a permis de transmettre des ordres au tableau de bord, au volant, aux freins et à la boîte de vitesse du véhicule par l'intermédiaire de son système de divertissement, le tout à distance, à partir d'un ordinateur portatif. Ils sont même parvenus à couper la transmission, forçant le véhicule à s'arrêter au beau milieu d'une autoroute inter-États[1]. Parallèlement aux études contrôlées, il existe une multitude de menaces à la cybersécurité, comme l'usurpation d'identité et de données financières personnelles (ciblant les services et applications automobiles en ligne qui contiennent des renseignements bancaires ou sur le crédit), le vol de marchandises et de biens (visant les systèmes de camions connectés qui laissent la marchandise sans surveillance) et les logiciels rançonneurs (qui désactivent une des fonctions d'un véhicule et exigent une somme d'argent en échange de sa restauration).

Contrairement aux véhicules connectés, les véhicules autonomes et sans conducteur nécessitent une automatisation et une connectivité supérieures avec d'autres sources, notamment pour ce qui touche l'infrastructure qui les entoure. L'automatisation accroît la spécification des données et en produit un volume plus élevé. Plus les données seront précieuses aux yeux des tiers qui se rendent coupables de « piratage informatique », plus les enjeux liés aux atteintes à la cybersécurité des véhicules autonomes gagneront en importance. De telles violations de données peuvent avoir de graves conséquences sur les entreprises. En l'absence de réglementation visant précisément la cybersécurité des véhicules autonomes et connectés au Canada, il convient de s'appuyer sur les récentes procédures concernant des cyberattaques pour illustrer les éventuels risques juridiques et commerciaux liés à de telles intrusions dans l'industrie automobile.

---

[1] Greenberg, Andy, « Hackers Remotely Kill a Jeep on the Highway—With Me in It », le 21 juillet 2015. En ligne : https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. Voir également le livre blanc de Chris Valasek et Charlie Miller, « Remote Exploitation of an Unaltered Passenger Vehicle », 2015. En ligne : http://www.ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf.

Au cours des cinq dernières années, le nombre d'actions collectives relatives à des atteintes à la cybersécurité au Canada a considérablement augmenté; plusieurs de ces poursuites ont été accueillies et certaines se sont soldées par des règlements approuvés par le tribunal. Dans la plupart des cas, la réparation offerte aux membres de l'action collective était peu élevée (de 2 500 $ à 5 000 $ par demandeur), mais le montant total des dommages-intérêts et des honoraires d'avocat pouvait s'avérer appréciable en fonction du nombre de plaignants. Par exemple, le règlement approuvé en 2017 dans l'affaire *Drew* v. *Walmart Canada Inc.*[2], qui avait été fixé à 1,25 M$, comprenait le versement d'au plus 5 000 $ à chaque plaignant, un service de surveillance du crédit d'un an et un remboursement des honoraires d'avocat évalué à 250 000 $. Dans ce cas, l'atteinte à la protection des données du logiciel d'impression de photos en ligne de Walmart avait permis l'accès aux renseignements personnels et financiers de consommateurs. Dans le cadre d'une action collective du même ordre visant une cyberattaque[3] qui a touché 3,5 millions de titulaires de compte Sony, la société avait dû verser à chaque plaignant jusqu'à 2 500 $ et les honoraires d'avocat approuvés s'étaient élevés à 265 000 $.

Si aucun litige concernant des véhicules connectés n'a encore été répertorié au Canada, il convient d'examiner deux actions collectives de ce type intentées en Illinois et en Californie. Ces affaires ont eu des issues très différentes. La décision de la Californie[4] portait sur une demande de dommages-intérêts en raison du potentiel piratage lié à la prétendue faiblesse des mesures de sécurité de certains véhicules Toyota. Cette cause a été rejetée dans son ensemble par les tribunaux, car les plaignants ne sont pas parvenus à démontrer suffisamment efficacement le préjudice subi par le risque de piratage, le prix d'achat excessif du véhicule et l'atteinte à leur vie privée. La poursuite intentée contre Fiat Chrysler en l'Illinois[5], quant à elle, n'a pas connu le même traitement. En 2015, Fiat Chrysler avait rappelé des véhicules équipés de systèmes UConnect 8.4A ou UConnect 8.4AN en vue d'une mise à niveau visant à éliminer toute vulnérabilité potentielle à des actes de piratage. Au départ, le tribunal a rejeté les allégations des plaignants quant à la possibilité d'un futur acte de piratage. Toutefois, il a depuis accepté qu'ils aillent de l'avant avec leur prétention selon laquelle leurs véhicules s'étaient dépréciés en raison du risque de piratage. En réponse, Fiat Chrysler a argumenté qu'elle ne pouvait pas être tenue pour responsable d'actes de piratage théoriques et qu'il n'existait aucune preuve que les véhicules concernés avaient perdu de la valeur. Il sera intéressant de connaître le jugement que rendra la cour dans cette affaire.

Les atteintes à la cybersécurité présentent également des risques importants du point de vue de la réglementation. De telles démarches réglementaires s'accompagnent de frais de défense additionnels, de pertes commerciales et d'un ternissement de la réputation des entreprises ainsi que de potentielles sanctions réglementaires. En vertu du règlement d'application récemment publié de la *Loi sur la protection des renseignements personnels et les documents numériques* (la « LPRPDE »), les organisations doivent déclarer les atteintes au Commissariat à la protection de la vie privée et en aviser les intéressés « le plus tôt possible » à la suite d'une atteinte. Le seuil de déclaration dépend du « risque réel de préjudice grave » à l'endroit de toute personne dont les renseignements personnels peuvent avoir été violés. En omettant d'aviser l'organisme de réglementation fédéral, les organisations s'exposent à une amende maximale de 100 000 $ ainsi qu'à l'exercice d'un droit privé d'action par les victimes de l'atteinte.

L'issue de l'action collective ayant fait l'objet d'un règlement en 2016 qui portait sur le piratage du système de paiement par carte de Home Depot illustre les avantages d'aviser en temps opportun les organismes de réglementation appropriés en matière de protection de la vie privée[6]. Dans le cas qui nous occupe, Home Depot avait averti l'organisme de réglementation fédéral et quatre organismes de réglementation provinciaux. Aucun d'entre eux n'a ensuite entrepris de lancer une enquête. Au contraire, ils ont tous fermé le dossier. Cet exemple témoigne de l'importance d'adopter une stratégie d'atténuation des risques, comme la mise en place d'une réponse proactive en cas d'atteinte pour limiter le risque de poursuites par les organismes de réglementation en matière de protection de la vie privée. Cependant, comme l'a montré le rapport d'enquête conjoint de 2016 du commissaire à la protection de la vie privée du Canada et de son homologue australien relativement à l'atteinte aux renseignements personnels dans l'affaire Ashley Madison, les organismes de

[2] *Drew* v. *Walmart Canada Inc.*, 2017 ONSC 3308 (Ontario).
[3] *Maksimovic* v. *Sony of Canada Ltd.*, 2013 CanLII 41305 (Ontario).
[4] Sussman Heather, Doug Meal et David Cohen, « Recent Decisions Highlight Product Cybersecurity Issues » concernant l'affaire *Cahen, et al.* v. *Toyota Motor Corp., et al.*, Cour de district du District nord de la Californie. En ligne : https://www.law360.com/articles/863307/recent-decisions-highlight-product-cybersecurity-issues.
[5] Crosby, Christopher, « Jeep Drivers Fight For Class Cert. in Hacking Suit » relativement à l'affaire *Flynn et al* v. *FCA US LLC, et al.*, Cour de district du District sud de l'Illinois. En ligne : https://www.law360.com/articles/974577.
[6] *Lozanski* v. *Home Depot* 2016 ONSC 5447 (Ontario) à l'article 7.

réglementation n'hésitent pas à ouvrir une enquête. Dans cette affaire, plusieurs infractions aux lois sur la protection de la vie privée ont été constatées[7].

Bien que nous soyons actuellement en présence d'un relatif vide juridique, une certaine surveillance réglementaire se profile à l'horizon dans l'industrie automobile. En effet, au début de l'année 2017, le Commissariat à la protection de la vie privée du Canada a annoncé qu'il financerait un projet indépendant visant à élaborer un code de pratique pour les véhicules autonomes et connectés. Le commissaire à la protection de la vie privée a indiqué qu'il appuyait l'approche de la « protection intégrée de la vie privée[8] » selon laquelle le secteur tient compte de la sécurité et du respect de la vie privée dès le début du processus d'innovation[9]. Si cette approche peut s'avérer utile à l'avenir dans la prévention des atteintes à la cybersécurité en ce qui a trait aux nouvelles technologies, les organisations se retrouvent actuellement livrées à elles-mêmes pour ce qui est de se prémunir contre ce type de risques concernant les technologies connectées.

Si l'industrie automobile a une leçon à retenir, c'est que les actions collectives et les poursuites en matière réglementaire intentées par les organismes de réglementation en matière de protection de la vie privée présentent des risques législatifs et commerciaux importants pour les parties intéressées, bien qu'il reste encore au Canada à appliquer des exigences législatives et réglementaires précises en matière de cybersécurité des véhicules autonomes et connectés. Les technologies offertes aujourd'hui comportent un risque qui pourrait s'accentuer avec l'émergence des technologies axées sur les véhicules autonomes.

Autrices :

Tamara Tomomitsu

Edona Vila

Vous avez des suggestions ou des commentaires? Nous serions heureux de vous lire. Vous pouvez nous écrire à AVs@blg.com.

[7] « Rapport de conclusions d'enquête en vertu de la LPRPDE no 2016-005 : Enquête conjointe sur Ashley Madison menée par le commissaire à la protection de la vie privée du Canada et le commissaire à la protection de la vie privée/commissaire à l'information par intérim de l'Australie », le 22 août 2016. En ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2016/lprpde-2016-005/.

[8] Cadre selon lequel la protection de la vie privée s'inscrit dans la conception du système ainsi que dans la structure et les pratiques organisationnelles. Voir la publication du Commissaire à l'information et à la protection de la vie privée sur la « protection intégrée de la vie privée » du 1er septembre 2013. En ligne : https://www.ipc.on.ca/resource/privacy-by-design.

[9] *Canadian Underwriter*, « Office of the Privacy Commissioner of Canada to fund project on connected cars code of practice », le 30 mars 2017. En ligne : https://www.canadianunderwriter.ca/insurance/office-privacy-commissioner-canada-fund-project-connected-cars-code-practice-1004111087/.

Bureaux BLG

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T +1.403.232.9500
F +1.403.266.1395

Montréal

1000, rue De La Gauchetière Ouest
Bureau 900
Montréal, QC, Canada
H3B 5H4

T +1.514-954-2555
F +1.514-879-9015

Ottawa

World Exchange Plaza
100, rue Queen
Ottawa, ON, Canada
K1P 1J9

T +1.613.237.5160
F +1.613.230.8842

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415