*Vol. 35, nº 2*

# Revue des décisions marquantes de l'année 2022 en matière de vie privée et de protection des renseignements personnels

**Simon Du Perron et Catherine Labasi Sammartino***





* Avocats au sein de l'équipe Cybersécurité, respect de la vie privée et protection des renseignements personnels du cabinet Borden Ladner Gervais.

[Note : cet article a été soumis à une évaluation à double anonymat]

**RÉSUMÉ**

Cet article analyse et commente certaines décisions marquantes de l'année 2022 en ce qui concerne le respect de la vie privée et la protection des renseignements personnels. Abordant des décisions rendues au Québec, au fédéral et en Ontario, cette recension examine particulièrement l'application de la législation québécoise à l'utilisation d'un algorithme d'intelligence artificielle dans le milieu scolaire, la collecte de données de géolocalisation par une application mobile et le recours au délit d'intrusion dans l'intimité de common law en matière d'actions collectives.

**MOTS-CLÉS**

Vie privée – intelligence artificielle – géolocalisation – actions collectives – Loi 25

**ABSTRACT**

This article analyzes and comments on some of the landmark decisions of 2022 with respect to privacy and data protection. Focusing on rulings from Quebec, Ottawa and Ontario, this review specifically examines the application of Quebec's privacy legislation to the use of an artificial intelligence algorithm in student management, the collection of location data by a mobile application and the interpretation of the common law tort of intrusion upon seclusion in class actions.

**KEYWORDS**

Privacy – Artificial intelligence – GPS tracking – Class actions – Bill 64

## INTRODUCTION

2022 constitue une année charnière pour le droit au respect de la vie privée et à la protection des renseignements personnels. Au Québec, 2022 marque l'entrée en vigueur des premières obligations introduites par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (ci-après « Loi 25 »)[1] dans la *Loi sur la protection des renseignements personnels dans le secteur privé* (ci-après « Loi sur le privé »)[2] et la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après « Loi sur l'accès »)[3], notamment la désignation d'un responsable de la protection des renseignements personnels et le signalement des incidents de confidentialité. En outre, le législateur québécois nous réservait une surprise de fin d'année avec le dépôt du projet de loi nº 3[4], la version revue et corrigée du projet de loi nº 19 mort au feuilleton en raison des élections provinciales, qui vise à doter le Québec d'un cadre juridique spécifique pour le traitement de renseignements de santé et de services sociaux.

Le législateur fédéral s'est également distingué avec le dépôt de deux projets de loi qui touchent à la cybersécurité et à la protection des données : le projet de loi C-26[5] et le projet de loi C-27[6]. Le premier vise principalement les entreprises sous réglementation fédérale qui exploitent des services et systèmes d'importance critique pour la sécurité nationale, tandis que le second constitue une nouvelle

1. *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, L.Q. 2021, c. 25 (ci-après « Loi 25 »).
2. *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P-39.1 (ci-après « Loi sur le privé »).
3. *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1 (ci-après « Loi sur l'accès »).
4. *Loi sur les renseignements de santé et de services sociaux et modifiant diverses dispositions législatives*, projet de loi nº 3 (sanctionné – 4 avril 2023), 1re sess., 43e légis. (Qc).
5. *Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*, projet de loi nº 26 (2e lecture à la Chambre – 27 mars 2023), 1re sess., 44e légis. (Can.).
6. *Loi de 2022 sur la mise en œuvre de la Charte du numérique*, projet de loi nº 27 (sanctionné – 30 mars 2021), 1re sess., 44e légis (Can.).

mouture du projet de loi C-11, qui est mort au feuilleton en 2021. Fait notable, en plus des éléments repris à son prédécesseur, soit la réforme générale de la *Loi sur la protection des renseignements personnels et les documents électroniques* (ci-après « LPRPDE »)[7] et la création d'un Tribunal de la protection des renseignements personnels et des données, le projet de loi C-27 propose également l'adoption d'une réglementation spécifique aux systèmes d'intelligence artificielle inspirée de l'approche européenne en la matière[8].

Il est donc intéressant d'analyser les récentes décisions des tribunaux et des commissaires à la protection de la vie privée dans la foulée de l'enthousiasme (mais également de l'incertitude) que suscitent ces importantes réformes. Ainsi, nous commencerons notre revue de l'année au Québec avec l'analyse d'une décision concernant le développement d'un algorithme d'intelligence artificielle dans le milieu scolaire. Nous nous déplacerons ensuite vers Ottawa pour aborder les conclusions d'une enquête des commissaires canadiens de protection de la vie privée portant sur l'utilisation de la géolocalisation par une application mobile. Nous terminerons notre route en Ontario avec l'examen d'une trilogie de décisions rendues par les tribunaux de la province en matière de certification d'actions collectives fondée sur l'atteinte au droit à la vie privée.

## 1. LE DROIT ET L'INTELLIGENCE ARTIFICIELLE : LA SURPRENANTE DÉCISION *VAL-DES-CERFS*

### 1.1 Contexte

À la suite de la parution d'un article de journal[9], la Commission d'accès à l'information (ci-après « CAI ») a déclenché une enquête concernant le développement d'un algorithme par le centre de services scolaire du Val-des-Cerfs permettant de cibler les élèves qui présentent un risque important de décrochage scolaire[10].

---

7. *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5 (ci-après « LPRPDE »).
8. COMMISSION EUROPÉENNE, *Proposition de règlement du parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle)*, en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0206&from=EN>.
9. Giuseppe VALIANTE, « Un algorithme repère les décrocheurs », *La Presse*, 1er novembre 2018.
10. *Enquête concernant le Centre de services scolaire du-Val-des-Cerfs (anciennement Commission scolaire du Val-des-Cerfs)*, 2022 QCCAI 1020040.

Développé en partenariat avec une équipe d'un cabinet comptable, cet algorithme d'apprentissage automatique permet de générer un ensemble d'indicateurs prédictifs du risque de décrochage scolaire à partir de l'analyse de plus de 300 types de données brutes différentes, notamment des résultats académiques ainsi que des statistiques relatives à l'aide financière, à l'absentéisme, aux mesures disciplinaires et aux fréquents changements d'adresse. Pour la réalisation du mandat confié à son fournisseur, le centre de services scolaire lui a temporairement permis d'accéder à une copie de sa base de données après avoir retiré 80 types de données considérées comme sensibles, notamment le nom des élèves et de leurs parents et leurs coordonnées.

Comme le centre de services scolaire est un organisme public assujetti à la Loi sur l'accès[11], la CAI s'est penchée sur la conformité de ce projet aux obligations en matière de protection des renseignements personnels.

## 1.2 Observations

### *1.2.1 La cruciale distinction entre les renseignements dépersonnalisés et anonymisés*

La définition de « renseignement personnel » constitue une notion clé puisqu'elle détermine l'application ou non des dispositions de la Loi sur l'accès et de la *Loi sur le privé en matière de protection des renseignements personnels*. Dans le corpus juridique québécois, est considéré comme un renseignement personnel « tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier »[12].

La Loi 25 ajoute deux nouvelles définitions qui viennent circonscrire la portée de la notion de renseignement personnel. Ainsi, un renseignement peut être *dépersonnalisé*, lorsqu'il ne permet plus d'identifier directement la personne concernée[13], ou il peut être *anonymisé*, lorsqu'il est en tout temps raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'iden-

11. Loi sur l'accès, préc., note 3, art. 3 et 6.
12. Loi sur l'accès, préc., note 3, art. 54 (telle qu'amendée par la Loi 25) ; Loi sur le privé, préc., note 2, art. 2 (telle qu'amendée par la Loi 25). À noter que les amendements à ces articles entrent en vigueur le 22 septembre 2023.
13. Loi sur l'accès, préc., note 3, art. 65.1 al. 5 (telle qu'amendée par la Loi 25) ; Loi sur le privé, préc., note 2, art. 12 al. 4(1) (telle qu'amendée par la Loi 25). À noter que les amendements à ces articles entrent en vigueur le 22 septembre 2023.

tifier directement ou indirectement la personne concernée[14]. Cette distinction revêt une grande importance puisque les renseignements dépersonnalisés, contrairement aux renseignements anonymisés, demeurent considérés comme des renseignements personnels assujettis à la législation. Cette qualification s'explique par le fait que ceux-ci permettent d'identifier indirectement la personne concernée, c'est-à-dire en ayant recours à d'autres renseignements disponibles, à une clé de correspondance ou à d'autres techniques de réidentification[15].

Bien qu'elles n'entrent en vigueur que le 22 septembre 2023[16], la CAI a néanmoins considéré ces nouvelles notions dans sa qualification des données utilisées dans le cadre du développement de l'algorithme. Ainsi, la CAI indique que les mesures prises par le centre de services scolaire pour éviter que les données transmises à son mandataire ne permettent d'identifier les élèves et leurs parents, notamment le retrait des noms et des coordonnées, ne sont pas irréversibles puisqu'il demeure possible pour l'organisme d'identifier les élèves en utilisant d'autres données recueillies tout au long de leur cheminement scolaire[17]. Il s'agit donc de renseignements personnels dépersonnalisés qui demeurent sous le champ d'application de la Loi sur l'accès.

Cette interprétation inédite confirme le critère élevé pour parvenir à l'anonymisation de renseignements personnels en vertu de la législation québécoise. Ainsi, le simple fait de retirer des identifiants directs (ex. : nom, adresse, numéro d'assurance maladie ou de permis de conduire, adresse IP, etc.) d'un ensemble de données ne sera pas considéré suffisant pour conclure à l'anonymisation de renseignements. Qui plus est, il importe de considérer les capacités de réidentification propres à chaque organisation pour déterminer si les mesures prises empêchent, de façon irréversible, l'identification indirecte des individus. Une organisation qui dispose d'un grand volume de données sur un groupe de personnes (ex. : clients, employés, usagers, étudiants, etc.) devra donc prendre des mesures plus robustes qu'une organisation qui dispose d'un échantillon de données plus réduit. Enfin, les organisations qui développent des projets d'intelligence artificielle

14. Loi sur l'accès, préc., note 3, art. 73 al. 2 (telle qu'amendée par la Loi 25) ; Loi sur le privé, préc., note 2, art. 23 al. 2 (telle qu'amendée par la Loi 25). À noter que les amendements à ces articles entrent en vigueur le 22 septembre 2023.
15. COMMISSION D'ACCÈS À L'INFORMATION (CAI), *Pandémie, vie privée et protection des renseignements personnels*, 2 mai 2020, p. 9.
16. Loi 25, préc., note 1, art. 175.
17. *Enquête concernant le Centre de services scolaire du-Val-des-Cerfs*, préc., note 10, par. 15 et 16.

sur la base de l'analyse de données dites « anonymisées » devront vraisemblablement développer une documentation étoffée de leurs méthodes d'anonymisation ainsi qu'une analyse chiffrée du risque de réidentification afin de convaincre la CAI de leur conformité aux critères prévus par la loi et aux meilleures pratiques généralement reconnues.

### *1.2.2 Nouvel éclairage sur l'utilisation de renseignements personnels à des fins compatibles*

En règle générale, un organisme public ne peut utiliser des renseignements personnels qu'aux fins pour lesquelles ils ont été recueillis, sauf avec le consentement des personnes concernées[18]. Le législateur a toutefois prévu certaines exceptions à cette règle pour des cas d'utilisation spécifique. Introduit dans la Loi sur l'accès en 2006[19], l'article 65.1 prévoit qu'un organisme public peut utiliser un renseignement personnel, sans le consentement de la personne concernée, à une autre fin que celles pour lesquelles il a été recueilli lorsque cette fin est compatible avec les fins initiales, c'est-à-dire lorsqu'il y a un lien pertinent et direct entre la fin nouvelle et les fins indiquées lors de la collecte du renseignement[20]. À noter que la Loi 25 introduit une exception similaire dans la Loi sur le privé[21].

L'exception au consentement pour l'utilisation de renseignements personnels à des fins compatibles a été très peu discutée en jurisprudence ainsi que dans les décisions de la CAI. À titre explicatif, les auteurs Raymond Doray et François Charrette indiquent qu'« il y a utilisation à des fins compatibles lorsqu'on peut établir un rapport logique et prévisible entre l'objet pour lequel le renseignement a été recueilli à l'origine (usage primaire) et la nouvelle fin pour laquelle l'organisme désire maintenant l'utiliser (usage secondaire) »[22].

---

18. Loi sur l'accès, préc., note 3, art. 65.1. Voir également *Code civil du Québec*, RLRQ, c. CCQ-1991, art. 37.
19. *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*, projet de loi nº 86, 2e sess., 37e légis. (Qc).
20. Loi sur l'accès, préc., note 3, art. 65.1 al. 2(1) et al. 3.
21. Loi sur le privé, préc., note 2, art. 12 al. 2(1) et al. 3 (telle qu'amendée par la Loi 25). À noter que cet amendement entre en vigueur le 22 septembre 2023.
22. Raymond DORAY et François CHARETTE, *Accès à l'information : loi annotée, jurisprudence, analyse et commentaires*, Montréal, Éditions Yvon Blais, 2008, p. III/65.1-2 (à jour le 01-09-2019).

En l'espèce, la CAI souligne que les élèves et leurs parents n'ont pas consenti à l'utilisation de leurs renseignements afin de développer un algorithme permettant de générer des indicateurs prédictifs du risque de décrochage scolaire et ils n'ont pas été informés de cette utilisation lors de la collecte des renseignements[23]. La CAI a toutefois conclu que cette utilisation secondaire était valide, considérant que le développement de l'algorithme constitue une fin compatible avec l'un des objectifs généraux de l'organisme lors de la cueillette initiale des renseignements des élèves, soit le fait d'assurer leur réussite scolaire[24]. L'organisme a d'ailleurs indiqué à la CAI que son initiative s'inscrivait dans le cadre de l'objectif de diplomation et de qualification des élèves qui fait partie de la *Politique de la réussite éducative* du ministère de l'Éducation[25].

Cette conclusion reflète une plus grande flexibilité dans l'interprétation de la notion de fins compatibles qui se démarque de l'approche restrictive préconisée jusqu'à présent dans la jurisprudence[26]. En précisant que la compatibilité peut s'évaluer à la lumière des objectifs généraux d'un organisme et non seulement avec les fins qui ont été précisément mentionnées aux individus lors de la collecte, la CAI reconnait la pertinence et l'utilité de cette exception lorsqu'une utilisation était difficilement prévisible au moment de la collecte des renseignements. À notre avis, cette interprétation démontre également que l'évaluation de la compatibilité d'une fin n'est pas qu'une question objective (à savoir si la fin nouvelle est directement liée aux fins initiales), mais nécessite de tenir compte des attentes raisonnables des personnes concernées par rapport à l'utilisation de leurs renseignements personnels par l'organisme. Cela transparait d'ailleurs dans les débats parlementaires portant sur l'article 65.1 de la Loi sur l'accès :

> Et, M. le Président, si je peux me permettre aussi, peut-être. Comme légistes, on est toujours guidés aussi par la jurisprudence en matière de respect de la vie privée parce que la protection des renseignements personnels, c'est une forme de mise en œuvre du droit plus fondamental au respect de la vie privée, droit qui, lui-même, découle du droit à la dignité de toute personne, et ce qui a amené la jurisprudence à dire que

23. *Enquête concernant le Centre de services scolaire du Val-des-Cerfs*, préc., note 10, par. 18.
24. *Id.*, par. 20.
25. *Id.*, par. 19.
26. Voir *Université Concordia*, 2015 QCCAI 1004421-S et *Université de Sherbrooke*, 2015 QCCAI 1005313-S.

> toute personne a droit à une expectative raisonnable de vie privée. Et ça se traduit aussi par le fait que l'individu a le droit de ne pas se faire prendre par surprise avec l'utilisation d'un renseignement à son sujet. Alors, ici, on a essayé, là, d'avoir ça en tête. Alors, le fait de pouvoir utiliser des renseignements à des fins compatibles, je pense que ça ne prendra pas le citoyen par surprise […].[27] (Nos soulignements)

Par ailleurs, l'interprétation de l'article 65.1 de la Loi sur l'accès par la CAI confirme que les exceptions au consentement en matière d'utilisation de renseignements personnels à des fins secondaires demeurent applicables lorsque l'utilisation s'effectue par un fournisseur de services pour le compte de l'organisme. En effet, en l'espèce, c'est l'équipe du cabinet comptable retenu par le centre de services scolaire qui a utilisé les renseignements personnels dépersonnalisés pour développer l'algorithme prédictif. Précisons toutefois que ce traitement de renseignements était encadré par une entente conclue conformément à l'article 67.2 de la Loi sur l'accès[28].

### *1.2.3 La qualification juridique des inférences générées par l'intelligence artificielle*

La CAI a ensuite étudié le statut juridique des indicateurs prédictifs générés par l'algorithme développé par le centre de services scolaire. L'organisme a fait valoir que l'analyse effectuée par son outil constitue une valorisation de données qu'il possède déjà et non une création de nouveaux renseignements personnels[29]. Or, la CAI est plutôt d'avis que l'outil développé par le centre de services scolaire n'est pas qu'un simple algorithme permettant d'extraire ou de répertorier des données brutes ; il s'agit d'un système d'intelligence artificielle complexe qui a la capacité de produire de nouveaux renseignements, soit des indicateurs prédictifs du risque de décrochage scolaire[30]. Ces renseignements doivent, selon la CAI, être considérés comme des renseignements personnels puisqu'ils « permettront à l'organisme de dresser un profil de l'élève et qui [*sic*] sont susceptibles d'avoir un effet sur les décisions prises à son sujet »[31].

---

27. *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*, projet de loi nº 86 (Étude détaillée), 2e sess., 37e légis. (Qc), vol. 39 nº 17 (M. Dussault).
28. *Id.*, par. 8.
29. *Id.*, par. 22 et 23.
30. *Id.*, par. 26 à 28.
31. *Id.*, par. 29.

La CAI prend donc fermement position en faveur de la qualification des données inférées, c'est-à-dire le savoir créé par le traitement des données primaires[32], à titre de renseignement personnel, dès lors que celles-ci concernent une personne physique[33]. Toutefois, il convient de souligner que la CAI ne s'est pas réellement penchée sur le caractère identificateur des indicateurs prédictifs en l'espèce. La CAI appuie plutôt son raisonnement sur la possibilité que ces renseignements soient utilisés par le centre de services scolaire dans le cadre d'une décision prise au sujet de l'élève, ce qui ne constitue pourtant pas un critère de qualification selon la définition de renseignement personnel.

En outre, la CAI mentionne que la production des indicateurs prédictifs équivaut à une nouvelle collecte de renseignements personnels à laquelle l'organisme n'était pas en mesure de procéder avant le développement de son outil[34]. Par conséquent, l'organisme doit s'assurer que cette collecte s'effectue en conformité avec la Loi sur l'accès, c'est-à-dire qu'elle doit respecter le critère de nécessité prévu à l'article 64 ainsi que l'obligation d'information prévue à l'article 65[35]. Ainsi, afin de satisfaire son obligation d'information, la CAI ordonne au centre de services scolaire d'informer les parents d'élèves dont les renseignements ont servi au développement de l'algorithme :

- du projet et de son objectif ;
- du fait que des renseignements personnels colligés lors de l'inscription et du cheminement scolaire de ces élèves ont été utilisés dans le cadre de ce projet ;
- du fait que l'analyse de ces renseignements personnels par l'algorithme a permis de créer de nouveaux renseignements personnels sur ces élèves ; et
- des fins pour lesquelles ces renseignements ont été recueillis, des catégories de personnes qui y ont eu accès et de leurs droits d'accès et de rectification[36].

---

32. Pierre-Luc DÉZIEL, « Les limites du droit à la vie privée à l'ère de l'intelligence artificielle : groupes algorithmiques, contrôle individuel et cycle de traitement de l'information », (2018) 30:3 *C.P.I.* 834.
33. La CAI avait déjà pris cette position dans un document : CAI, *Pandémie, vie privée et protection des renseignements personnels*, 2 mai 2020, p. 9 et 10.
34. *Enquête concernant le Centre de services scolaire du-Val-des-Cerfs*, préc., note 10, par. 28 et 35.
35. *Id.*, par. 30 à 33.
36. *Id.*, par. 58.

La CAI précise que l'organisme devra s'assurer de respecter cette obligation à l'égard de toute collecte future de renseignements personnels par le biais de l'outil[37]. Cela signifie que le centre de services scolaire devra développer un avis spécial, destiné aux parents d'élèves, relatif à son utilisation de l'algorithme.

Il convient de souligner que la CAI n'indique pas que l'organisme aurait dû obtenir le consentement des parents d'élèves dont les renseignements ont été impliqués dans la conception de l'outil. La non-application de l'exigence du consentement en l'espèce est selon nous cohérente dans la mesure où la CAI reconnait que le développement de l'algorithme s'inscrit dans le cadre d'une utilisation de renseignements personnels à des fins compatibles qui fait l'objet d'une exception au consentement[38]. Cela rejoint également les propos du professeur Pierre-Luc Déziel au sujet de l'interaction entre les processus de valorisation des données et le principe du consentement :

> [O]n jugerait contre-productif d'exiger des organismes publics et des entreprises qui souhaitent valoriser des renseignements personnels de communiquer à nouveau avec les personnes à la source de ces renseignements pour solliciter un second consentement. Il est fréquent que les jeux de données que les entreprises ou les organismes souhaitent valoriser concernent des cohortes de plusieurs dizaines de milliers de personnes. Le temps, l'énergie et les sommes qui sont nécessaires pour contacter ces personnes engagent des investissements qui pourraient s'avérer dissuasifs. C'est dans cette optique que les processus de valorisation sont souvent articulés par le biais d'exceptions au consentement individuel normalement requis pour la collecte, l'utilisation ou la divulgation de renseignements personnels.[39]

Ainsi, les organisations qui utilisent des données dépersonnalisées afin de développer un algorithme d'intelligence artificielle en s'appuyant sur une exception au consentement n'auraient qu'à se conformer aux exigences de nécessité et d'information prévues dans les lois de protection des renseignements personnels. Alors que le respect du critère de nécessité peut se démontrer dans le cadre d'une évaluation des facteurs relatifs à la vie privée effectuée en amont du projet, l'obligation d'information est particulièrement difficile à

37. *Id.*, par. 37.
38. *Id.*, par. 52.
39. Pierre-Luc DÉZIEL, « La valorisation des renseignements personnels au Québec et au Canada : la promesse des projets de loi nº 64 et C-11 », (2021) 33:2 *C.P.I.* 1200.

remplir lorsque les finalités d'un projet sont déterminées par les résultats générés par l'apprentissage automatique.

En effet, les techniques sophistiquées d'intelligence artificielle se heurtent à la « limite structurelle » du droit à la vie privée qui ordonne ses obligations selon un cycle particulier de traitement de l'information allant de la collecte jusqu'à la destruction des renseignements personnels[40]. Or, les finalités précises du traitement de renseignements personnels par un algorithme d'apprentissage automatique, comme celui développé par le centre de services scolaire, ne se révèlent généralement qu'après la phase d'entrainement de l'algorithme, c'est-à-dire après l'analyse des données primaires. Ainsi, il est pratiquement impossible pour une organisation de satisfaire pleinement son obligation d'information considérant que la nature des données inférées par l'algorithme, qui selon la CAI peuvent constituer de nouveaux renseignements personnels, demeure inconnue à l'étape de la collecte des données primaires. Comme l'indique le professeur Déziel : « Les étapes de collecte, d'utilisation et de divulgation des renseignements personnels, prévues de manières successives et distinctes par la loi, sont effectuées de manière presque simultanée et semblent difficilement dissociables dans le domaine de l'intelligence artificielle. »[41]

Malgré le défi que représente l'implantation de certaines de ses conclusions pour les organisations, la décision de la CAI concernant le Centre de services scolaire du Val-des-Cerfs fournit un éclairage pratique en matière d'application des lois de protection des renseignements personnels, incluant certaines des nouvelles dispositions de la Loi 25, aux systèmes d'intelligence artificielle.

## 2. NE GÉOLOCALISE PAS QUI VEUT : LES LEÇONS DE L'AFFAIRE TIM HORTONS

### 2.1 Contexte

Le 29 juillet 2022, la chaîne de restauration Tim Hortons a annoncé qu'elle allait offrir un café et un beigne gratuits aux clients ayant utilisé son application mobile entre le 1er avril 2019 et le 30 sep-

40. Au sujet de la « limite structurelle » du droit à la vie privée, voir P.-L. DÉZIEL, préc., note 32.
41. P.-L. DÉZIEL, préc., note 32, p. 845.

tembre 2020[42]. Cette proposition de règlement fait suite à plusieurs actions collectives intentées dans la foulée de la publication des conclusions de l'enquête conjointe des différents commissaires à la protection de la vie privée au Canada (ci-après les « Commissaires ») concernant la collecte de données de localisation des utilisateurs de l'application mobile Tim Hortons[43].

Alertés par un article de journal révélant que l'application mobile Tim Hortons avait enregistré l'emplacement du journaliste plus de 2 700 fois en l'espace de cinq mois, y compris lorsque l'application était fermée[44], les Commissaires ont déclenché une enquête visant à déterminer si Tim Hortons avait recueilli et utilisé les données des utilisateurs de l'application en conformité avec la législation applicable en matière de protection des renseignements personnels.

L'enquête indique que la chaîne canadienne a mis à jour son application mobile en mai 2019 afin d'intégrer une fonctionnalité permettant de suivre et de recueillir l'emplacement de l'appareil des utilisateurs. Plus précisément, Tim Hortons a mandaté un fournisseur américain, Radar Labs Inc. (ci-après « Radar »), afin d'intégrer une technologie lui permettant de déduire le lieu du domicile et le lieu de travail d'un utilisateur, ainsi que les visites chez une entreprise concurrente, à partir de l'analyse de différentes données générées par l'appareil (GPS, Wi-Fi, réseaux cellulaires, système d'exploitation mobile, etc.)[45].

L'application demandait à chaque utilisateur d'autoriser, de manière expresse, les fonctions de localisation. Une fois autorisée, l'application effectuait un suivi de l'emplacement de l'appareil tant en avant-plan (c.-à-d. application ouverte) qu'en arrière-plan (c.-à-d. application fermée). Or, la foire aux questions (ci-après « FAQ »)

---

42. LA PRESSE CANADIENNE et Brett BUNDALE, « Violation de la vie privée : Tim Hortons conclut un projet de règlement », *Le Devoir*, 29 juillet 2022, en ligne :<https://www.ledevoir.com/economie/739614/violation-de-la-vie-privee-tim-hortons-conclut-un-projet-de-reglement>.
43. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE LA COLOMBIE-BRITANNIQUE, COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ALBERTA ET COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Enquête conjointe sur le suivi de localisation par l'application de Tim Hortons*, Conclusions en vertu de la LPRPDE nº 2022-001 (ci-après « CPVP *et al.* »).
44. James MCLEOD, « Double-double tracking: How Tim Hortons knows where you sleep, work and vacation », *Financial Post*, 12 juin 2020.
45. CPVP *et al.*, préc., note 43, par. 27.

accessible sur l'application affirmait que les données de localisation n'étaient utilisées que lorsque l'application était ouverte[46].

Tim Hortons avait pour intention d'utiliser les données de localisation afin de faciliter la diffusion de publicités ciblées et la transmission de promotions et d'offres via l'application. Par exemple, un résident de Montréal en voyage à Toronto aurait reçu des offres promotionnelles liées aux succursales de la Ville Reine alors qu'un utilisateur assistant à un match des Canadiens de Montréal aurait reçu une notification poussée l'informant d'une offre spéciale dans le restaurant du Centre Bell. Toutefois, en raison d'une révision des priorités commerciales internes, Tim Hortons n'a jamais utilisé les données de localisation à des fins promotionnelles ; celles-ci n'ont servi qu'à réaliser des analyses de marché sur une base agrégée[47]. En juillet 2020, l'application comptait plus de 1,6 million d'utilisateurs actifs[48].

## 2.2 Observations

### *2.2.1 Le caractère raisonnable de la collecte de données de localisation*

La LPRPDE prévoit qu'une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances[49]. Cette exigence générale, qui se retrouve également dans les lois provinciales de protection des renseignements personnels[50], suppose un test de raisonnabilité qui ne peut être écarté même lorsqu'une organisation a obtenu un consentement valable[51].

Sur la base d'une analyse de la jurisprudence, le Commissariat à la protection de la vie privée du Canada (ci-après « CPVP ») a identifié certains facteurs clés à prendre en considération pour déterminer si une collecte, une utilisation ou une communication de

46. *Id.*, par. 21.
47. *Id.*, par. 22.
48. *Id.*, par. 13.
49. LPRPDE, préc., note 7, art. 5(3).
50. Voir la Loi sur le privé, préc., note 2, art. 4 et 5 ; *Personal Information Protection Act*, SA 2003, c. P-6.5, art. 11 (ci-après « PIPA de l'Alberta ») ; *Personal Information Protection Act*, SBC 2003, c. 63, art. 11 (ci-après « PIPA de la C.-B. »).
51. CPVP, *Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3)* ; voir également *X. et Pharmaprix*, 2014 QCCAI 1003352, par. 18 et *Société de transport de la Ville de Laval* c. *X.*, [2003] C.A.I. 667, par. 64 à 70.

renseignements personnels est à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances :

- le caractère sensible des renseignements personnels en question ;
- le besoin ou les intérêts commerciaux légitimes des fins visées par l'organisation ;
- l'efficacité de la collecte, de l'utilisation et de la communication pour répondre au besoin de l'organisation ;
- l'existence de moyens portant moins atteinte à la vie privée qui permettent d'atteindre les mêmes fins pour un coût et des avantages comparables ; et
- la proportionnalité de l'atteinte à la vie privée par rapport aux avantages[52].

Appliquant ce cadre d'analyse, les Commissaires ont conclu que la collecte en continu de données de localisation détaillées en arrière-plan à des fins de publicité ciblée n'était pas une finalité acceptable dans les circonstances.

Premièrement, les Commissaires ont qualifié les données de localisation recueillies via l'application de la chaîne de restauration rapide de renseignements personnels sensibles considérant la possibilité, pour Tim Hortons, d'utiliser l'information sur les déplacements d'un utilisateur pour générer des connaissances intimes à son sujet. En effet, puisque l'application recueillait des données de localisation toutes les quelques minutes et parvenait à déduire le lieu du domicile et le lieu de travail de l'utilisateur, les Commissaires ont jugé que Tim Hortons serait également en mesure de générer des inférences plus sensibles comme une visite à un lieu de culte, à un cabinet médical ou à un rassemblement politique. Il est intéressant de souligner que bien que la preuve indique que Tim Hortons n'avait pas utilisé les données de localisation pour générer de telles inférences, les Commissaires sont parvenus à cette conclusion considérant la « possibilité réelle » que les renseignements soient utilisés de cette façon[53]. Les Commissaires mentionnent également que les lieux de résidence et de travail peuvent s'avérer particulièrement sensibles dans certains contextes, par exemple pour les personnes vivant dans des refuges

52. CPVP, *Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3)*.
53. CPVP *et al.*, préc., note 43, par. 43.

qui viennent en aide aux victimes de violence conjugale ou pour les employés d'établissement correctionnel.

Deuxièmement, tout en reconnaissant que la publicité ciblée peut constituer une fin acceptable de traitement des données[54], les Commissaires ont jugé que Tim Hortons n'avait pas un besoin commercial légitime de recueillir les données de localisation considérant que celles-ci n'ont, dans les faits, jamais été utilisées aux fins de marketing mentionnées aux utilisateurs en raison du changement de priorités internes de l'entreprise. En effet, Tim Hortons a continué de recueillir une importante quantité de données de localisation pendant près d'un an après sa réorientation stratégique. En d'autres termes, Tim Hortons ne pouvait justifier la collecte des renseignements en l'absence d'une finalité précise d'utilisation.

Troisièmement, les Commissaires ont examiné la proportionnalité entre l'atteinte à la vie privée des utilisateurs que représente la collecte de leurs données de localisation et les avantages obtenus par Tim Hortons. À cet égard, les Commissaires soulignent l'importance de la notion de proportionnalité dans l'interprétation du test de raisonnabilité :

> La collecte et l'analyse des données de localisation détaillées des consommateurs par les entreprises sans égard à la notion de proportionnalité créent un risque important que les renseignements personnels ne soient plus utilisés à des fins acceptables, mais plutôt qu'ils soient amassés et traités comme de simples biens, de la marchandise à exploiter ou comme outil de surveillance pour les entreprises.[55]

Ainsi, les Commissaires sont d'avis que la collecte en arrière-plan de données de localisation toutes les quelques minutes et l'analyse en continu de ces données pour déduire le domicile et le lieu de travail constitue une atteinte importante à la vie privée des utilisateurs qui n'est pas proportionnelle aux avantages que Tim Hortons aurait pu espérer tirer de la possibilité de mieux promouvoir ses produits. Les Commissaires précisent d'ailleurs qu'il aurait été beaucoup plus transparent et moins intrusif de demander aux utili-

54. CPVP, *Résultats de l'enquête sur le Programme de publicité pertinente de Bell lancée par le commissaire*, Rapport de conclusions d'enquête en vertu de la LPRPDE nº 2015-001.
55. CPVP *et al.*, préc., note 43, par. 46.

sateurs de fournir leur domicile ou leur lieu de travail directement via l'application afin de bénéficier d'offres personnalisées.

À notre avis, l'application du test de raisonnabilité par les Commissaires dans la décision Tim Hortons ne saurait être interprétée comme une interdiction générale au traitement de données de localisation. En effet, les Commissaires ont confirmé que les fonctions GPS peuvent être utilisées à des fins acceptables, notamment pour la sécurité et la gestion des employés[56], et pour fournir et améliorer les produits et services[57]. Il importe toutefois de s'assurer que les données de localisation sont effectivement utilisées aux fins pour lesquelles elles ont été recueillies et qui ont été mentionnées aux individus au moment de la collecte.

### *2.2.2 L'obtention d'un consentement valable à la géolocalisation sur une application mobile*

Les Commissaires ont ensuite examiné la validité du consentement obtenu par Tim Hortons pour le traitement des données de localisation des utilisateurs tout en prenant soin de préciser que l'obtention d'un consentement n'a pas pour effet de rendre acceptable une collecte, une utilisation ou une communication qui ne passe pas le test de raisonnabilité.

À cet égard, les *Lignes directrices pour l'obtention d'un consentement valable* prévoient que les organisations doivent généralement obtenir un consentement explicite lorsque les renseignements recueillis sont sensibles ou lorsque leur collecte, leur utilisation ou leur communication ne répond pas aux attentes raisonnables des personnes concernées ou crée un risque résiduel important de préjudice grave[58]. Ces lignes directrices prévoient également que les

56. CPVP, *Examen de l'utilisation des renseignements personnels recueillis au moyen d'un système mondial de localisation*, Résumé de conclusions d'enquête en vertu de la LPRPDE nº 2006-351.

57. CPVP, *Le fait qu'un utilisateur accorde des « autorisations » à une application ne signifie pas, en soi, qu'il consent à la collecte, à l'utilisation et à la communication de renseignements personnels – Nous encourageons Google à donner plus de précisions aux utilisateurs pour éviter toute interprétation erronée*, Rapport de conclusions en vertu de la LPRPDE nº 2014-008, par. 92 ; CPVP, *Microsoft va obtenir le consentement exprès, améliorer la transparence pour les paramètres de confidentialité de Windows 10*, Rapport de conclusions d'enquête en vertu de la LPRPDE nº 2018-004, par. 62.

58. CPVP, « Lignes directrices pour l'obtention d'un consentement valable », mai 2018 (révisée le 13 août 2021), en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-

organisations doivent mettre l'accent sur les éléments suivants au moment de la collecte :

- Les renseignements personnels qui sont recueillis, détaillés avec suffisamment de précision pour permettre aux individus de bien comprendre ce à quoi ils consentent ;
- Les tiers auxquels les renseignements personnels seront communiqués ;
- Les fins auxquelles les renseignements sont recueillis, utilisés ou communiqués, détaillées avec suffisamment de précision pour permettre aux individus de bien comprendre ce à quoi ils consentent ; et
- Les risques de préjudice et les autres conséquences liés à la collecte, à l'utilisation ou à la communication des renseignements.

En l'espèce, les Commissaires ont conclu que Tim Hortons n'avait pas obtenu un consentement valable pour la collecte des données de localisation via l'application mobile (dans l'éventualité où les finalités de traitement auraient été acceptables) puisque les utilisateurs n'ont pas été informés adéquatement de l'étendue de la collecte et des conséquences de leur consentement. En effet, le libellé des demandes de permission sous iOS et Android n'informait pas les utilisateurs du fait que l'application recueillerait leurs données de localisation même lorsqu'elle était fermée ; au contraire, la FAQ indiquait que la collecte de données de localisation se produisait *seulement* lorsque l'application était ouverte[59]. En outre, les utilisateurs n'étaient pas informés que l'activation des fonctions de localisation de l'application allait se traduire par une collecte de données à quelques minutes d'intervalle chaque jour, peu importe l'endroit où ils se déplaçaient, dès lors que leur appareil était allumé. Comme les utilisateurs ne pouvaient raisonnablement s'attendre à une telle collecte de données de localisation en arrière-plan, Tim Hortons aurait dû fournir ces renseignements importants aux utilisateurs, de façon évidente, dans sa demande d'autorisation lors du téléchargement de l'application.

Ayant conclu que Tim Hortons n'avait pas obtenu un consentement valable des utilisateurs en raison de ce manque de transparence,

---

protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gl_omc_201805/>.

59. CPVP *et al.*, préc., note 43, par. 21 et 64.

les Commissaires ne se sont pas prononcés sur la forme appropriée du consentement pour la collecte des données de localisation. Cela dit, vu la qualification des données de localisation à titre de renseignement sensible et la remarque énonçant que les utilisateurs n'auraient pu raisonnablement s'attendre à ce que l'application recueille leurs données de localisation en arrière-plan, on peut affirmer qu'un consentement explicite aurait été requis.

Cette interprétation illustre l'importance du niveau de détail des données de localisation et de la fréquence de leur collecte dans la détermination de la forme appropriée du consentement pour une utilisation à des fins de marketing. En effet, dans des décisions antérieures, le CPVP a conclu qu'un consentement explicite était nécessaire pour utiliser la géolocalisation précise d'un visiteur d'un centre commercial afin de diffuser de la publicité ciblée sur des affichages, mais il a également reconnu qu'un consentement implicite était acceptable lorsque l'adresse IP du visiteur d'un site Web était utilisée pour déterminer son emplacement approximatif afin de lui présenter des publicités pertinentes[60].

### *2.2.3 L'importance des clauses de limitation dans un contrat avec un fournisseur de services*

Étant donné le rôle central du fournisseur de services responsable du développement de la fonctionnalité de localisation de l'application mobile dans cette affaire, les Commissaires ont examiné l'entente de service entre Tim Hortons et Radar afin de déterminer si celle-ci assurait une protection adéquate aux données des utilisateurs. Ces quelques commentaires, rédigés sous la forme d'un *obiter*, fournissent un éclairage pratique sur le type de dispositions contractuelles auxquelles s'attendent les Commissaires lorsqu'une organisation confie à un fournisseur un mandat qui implique un traitement de renseignements personnels.

Une entreprise est responsable des renseignements personnels qu'elle détient, y compris lorsque ceux-ci sont transférés ou

60. Voir CPVP, *Enquête conjointe sur La Corporation Cadillac Fairview limitée par le commissaire à la protection de la vie privée du Canada, la commissaire à l'information et à la protection de la vie privée de l'Alberta et le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique*, Conclusions en vertu de la LPRPDE nº 2020-004 ; CPVP, *Enquête sur les pratiques de traitement des renseignements personnels de Ganz Inc.*, Rapport de conclusions en vertu de la LPRPDE nº 2014-011.

confiés à un fournisseur de services dans le cadre d'un mandat[61]. Par conséquent, une entreprise qui confie à un tiers la tâche de recueillir, d'utiliser, de conserver ou de communiquer des renseignements personnels pour son compte doit prendre des moyens, notamment par voie contractuelle, afin d'assurer un niveau de protection adéquat aux renseignements pendant qu'ils sont traités par le fournisseur. Cette obligation se traduit généralement par une entente qui prévoit certaines mesures de sécurité raisonnables et appropriées, compte tenu notamment de la sensibilité des renseignements personnels impliqués[62]. La Loi 25 prévoit justement qu'une entreprise peut communiquer des renseignements personnels à un fournisseur de services, sans le consentement des personnes concernées, à condition de conclure une entente écrite qui prévoit des mesures pour assurer la protection du caractère confidentiel des renseignements, pour que ceux-ci ne soient utilisés que dans le cadre de l'exécution du contrat et pour qu'ils ne soient pas conservés après son expiration[63].

La limitation de la portée des opérations de traitement effectuées par le fournisseur de services constitue une disposition essentielle de l'entente puisqu'elle détermine les fins selon lesquelles le mandataire est autorisé à traiter les renseignements personnels pour le compte de l'entreprise, et ce, sans le consentement des personnes concernées. Ainsi, si le fournisseur de services souhaite utiliser les renseignements transmis pour ses propres fins, les parties devront obtenir un consentement supplémentaire dans la mesure où ce traitement n'est pas visé par une autre exception au consentement prévue par la loi.

En l'espèce, l'entente entre Tim Hortons et Radar prévoyait que Radar pouvait utiliser les renseignements « pour améliorer les services [que Radar a fourni à Tim Hortons], ainsi qu'à d'autres fins de conception, de diagnostic et de rectification en lien avec les services et d'autres offres de la société »[64]. Cette même clause autorisait également Radar à communiquer les données des utilisateurs dans le cadre de ses activités, mais uniquement sous forme agrégée ou sous

61. Loi sur le privé, préc., note 2, art. 1 al. 2 et 3.1 al. 2 (telle qu'amendée par la Loi 25) ; LPRPDE, préc., note 7, Annexe 1, Principe 4.1.3 ; PIPA de l'Alberta, préc., note 50, art. 5 ; PIPA de la C.-B., préc., note 50, art. 4(2).
62. LPRPDE, préc., note 7, Principe 4.7 ; PIPA de l'Alberta, préc., note 50 ; PIPA de la C.-B., préc., note 50, art. 34 ; Loi sur le privé, préc., note 2, art. 10.
63. Loi sur l'accès, préc., note 3, art. 67.2 (telle qu'amendée par la Loi 25) ; Loi sur le privé, préc., note 2, art. 18.3 (telle qu'amendée par la Loi 25). À noter que les amendements à ces articles entrent en vigueur le 22 septembre 2023.
64. CPVP *et al.*, préc., note 43, par. 43.

une autre forme ne permettant pas d'identifier un individu. Selon l'interprétation des Commissaires, ce libellé aurait permis à Radar d'utiliser ou de communiquer les données de localisation à ses propres fins, potentiellement sans obtenir un consentement préalable valable.

Considérant ce langage vague et permissif et l'absence de définitions de concepts clés dans l'entente, notamment en ce qui concerne l'anonymisation et la dépersonnalisation des renseignements personnels[65], les Commissaires ont jugé que le niveau de protection offert par l'entente entre Tim Hortons et Radar était inadéquat. Plus précisément, les Commissaires indiquent qu'ils se seraient attendus à retrouver des protections contractuelles beaucoup plus rigoureuses compte tenu du volume et de la sensibilité des renseignements concernés, ainsi que du niveau de risque accru associé à l'« écosystème actuel de suivi de la localisation » qui augmente la possibilité que ces données soient combinées à des données d'autres sources[66].

Finalement, la décision des Commissaires concernant l'application mobile Tim Hortons illustre les enjeux importants liés à l'utilisation de technologies de localisation à grande échelle. Afin d'identifier en amont les risques en matière de protection des renseignements personnels, ce type de projet devrait faire l'objet de mesures de « protection de la vie privée dès la conception » (*privacy by design*) comme la réalisation d'une évaluation des facteurs relatifs à la vie privée.

## 3. LE DÉLIT D'INTRUSION DANS L'INTIMITÉ EN COMMON LAW : UN RETOUR SUR LA TRILOGIE D'OWSIANIK

Dans une trilogie de décisions concernant l'autorisation[67] d'actions collective en Ontario, la question de la responsabilité des détenteurs de données pour le délit d'intrusion dans l'intimité a

65. La Loi 25 prévoit qu'un renseignement personnel est « dépersonnalisé » lorsqu'il « ne permet plus d'identifier directement la personne concernée », ce qui s'apparente davantage à la pseudonymisation qu'à l'anonymisation (voir l'article 12 de la Loi sur le privée amendée). En effet, un renseignement personnel sera considéré « 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 la personne concernée » (voir l'article 23 de la Loi sur le privée amendée). Ces notions ne sont toutefois pas définies de façon uniforme dans les autres lois canadiennes de protection des renseignements personnels.
66. CPVP *et al.*, préc., note 43, par. 4 et 77.
67. Afin d'assurer une cohérence avec les articles passés des Cahiers de propriété intellectuelle, nous employons le terme « autorisation » pour le besoin de cet article, mais, dans les provinces de common law, cette étape s'appelle la « certification ».

finalement été abordée. Cette trilogie, constituée des affaires *Owsianik*[68], *Obodo*[69] et *Winder*[70] (collectivement, la « Trilogie d'Owsianik » ou la « Trilogie »), limite l'étendue du risque de responsabilité dans des actions collectives pour les entreprises qui détiennent des renseignements personnels et qui sont victimes d'incidents de confidentialité causés par des activités de pirates informatiques. En effet, dans chacun de ces arrêts, la Cour d'appel de l'Ontario (ci-après la « CA ON ») a statué que les entreprises qui recueillent et conservent des renseignements personnels dans des bases de données (ci-après les « détenteurs de données ») ne peuvent être tenues responsables en vertu du délit d'intrusion dans l'intimité lorsqu'elles ne participent pas activement à l'intrusion, y compris lorsque ce sont des pirates informatiques qui accèdent illégalement aux renseignements qu'elles détiennent.

Dans le texte qui suit, nous donnerons un aperçu du contexte juridique qui a donné lieu aux enjeux discutés dans la Trilogie d'Owsianik, des faits marquants, du raisonnement de la CA ON et de son impact sur les litiges futurs en matière de protection de la vie privée.

### 3.1 Contexte

Chacun des groupes dans la Trilogie d'Owsianik cherchait à faire autoriser une action collective qui visait ultimement à appliquer la décision de 2012 de la CA ON dans l'affaire *Jones*[71], qui a reconnue pour la première fois le délit d'intrusion en common law. Il convient de mentionner que, contrairement aux décisions de la Trilogie, l'affaire *Jones* concernait un recours *individuel* en dommages-intérêts pour atteinte à la vie privée intentée directement contre l'*intrus*, une employée d'une banque qui avait accédé à plusieurs reprises aux dossiers financiers de la nouvelle partenaire de son ex-mari.

Le délit d'intrusion dans l'intimité fut importé par la CA ON à partir de concepts de droit américain[72] alors que le juge Sharpe constatait à la fois l'importance du respect de la vie privée dans la *Charte canadienne des droits et libertés* et la jurisprudence canadienne[73]

68. *Owsianik* v. *Equifax Canada Co.*, 2022 ONCA 813.
69. *Obodo* v. *TransUnion of Canada, Inc.*, 2022 ONCA 814.
70. *Winder* v. *Marriott International, Inc.*, 2022 ONCA 815.
71. *Jones* v. *Tsige*, 2012 ONCA 32.
72. Restatement (Second) of Torts, § 652B (2010).
73. *Jones* v. *Tsige*, préc., note 71, par. 66.

et que les faits présentés devant lui ne donneraient autrement pas lieu à un recours pour la plaignante même si la situation « réclamait une réparation »[74] (notre traduction). Spécifiquement, la CA ON a examiné la raison d'être du délit, à savoir le droit à la protection des renseignements personnels de la demanderesse, et a reconnu que ce droit devait être protégé compte tenu de « l'évolution technologique »[75] (notre traduction) qui conduit de manière croissante à « la collecte et l'agrégation systématique de renseignements hautement personnels qui sont facilement accessibles sous forme électronique »[76] (notre traduction).

En reconnaissant le délit d'intrusion dans l'intimité, la CA ON a clairement assumé son rôle progressiste, notamment en ce qui consiste à développer la common law d'une manière compatible avec les besoins des entreprises, en tenant compte notamment de l'évolution technologique des pratiques d'affaires. De plus, en agissant ainsi, la CA ON nous montre également qu'elle cherchait à ce que des dommages symboliques soient accordés aux victimes d'atteinte à la vie privée, même si ces dommages n'étaient pas indemnisables en vertu d'autre délit tel que la négligence.

Dans le cadre de la décision *Jones*, la CA ON a défini les trois éléments du délit d'intrusion dans l'intimité :

(1) Le défendeur a commis une intrusion, sans justification légale, dans les affaires privées ou les préoccupations personnelles du plaignant ;

(2) Le défendeur a commis l'intrusion de manière intentionnelle ou inconsidérée ; et

(3) Une personne raisonnable considérerait l'intrusion commise par le défendeur comme étant très offensante, et causant de la détresse, de l'humiliation ou de l'angoisse[77].

La CA ON a donc ouvert la porte avec l'arrêt *Jones* à des demandes de dommages-intérêts non pécuniaires dans des cas qui n'impliquent pas de blessures graves et prolongées. Au cours de la décennie qui a suivi cette décision, les tribunaux de common law ont

74. *Id.*, par. 69.
75. *Id.*, par. 68.
76. *Id*.
77. *Id.*, par. 71.

clarifié la portée de ce délit, notamment dans le cadre de la Trilogie d'Owsianik, telle qu'expliquée ci-dessous.

### 3.2 Trois incidents de confidentialité et un délit

Dans chacune des décisions de la Trilogie d'Owsianik, les membres demandaient au tribunal d'autoriser une action collective contre des détenteurs de données – respectivement les bureaux de crédit Trans Union et Equifax, et les hôtels Starwood du groupe Marriot – qui avaient chacun subi un incident de confidentialité[78] au cours duquel des pirates informatiques avaient accédé à leurs réseaux et compromis les renseignements sous leur contrôle, y compris les renseignements personnels des membres.

Les renseignements accédés de manière illégale comprenaient l'adresse, noms, date de naissance, numéro de permis de conduire, adresse électronique, mot de passe, numéro de téléphone, numéro d'assurance sociale, numéro de passeport, et des détails sur les dossiers financiers des individus concernés, incluant l'état de leur dette, l'historique de paiement et les numéros de cartes de crédit. Pour illustrer l'ampleur que peuvent prendre les incidents de confidentialité, dans l'affaire *Owsianik*, environ 20 000 Canadiens ont été avisés par Equifax que des pirates informatiques avaient consulté leurs renseignements personnels.

#### *3.2.1 Owsianik*

Dans l'affaire *Owsianik*, le représentant des membres demandeurs a plaidé que les pratiques « inconsidérées »[79] (notre traduction) d'Equifax en matière de gestion des données constituaient une intrusion dans l'intimité qui serait très choquante pour une personne raisonnable[80]. Les membres du groupe avançaient spécifiquement qu'Equifax n'avait pas un système de sécurité adéquat pour protéger l'accès aux données, et, de plus, que l'entreprise était pleinement consciente des insuffisances de son système, notamment en raison de résultats négatifs d'audits qu'elle avait récemment obtenus sur cette

78. Pour le besoin de cet article, nous employons le terme « incident de confidentialité » comme le définit l'article 3.6 de la Loi sur le privé qui désigne l'accès, l'utilisation, et la communication non autorisés, ou la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.
79. *Agnew-Americano* v. *Equifax Canada Co.*, 2019 ONSC 7110, par. 68.
80. *Owsianik* v. *Equifax Canada Co.*, 2021 ONSC 4112, par. 5.

question[81]. Les membres du groupe soutenaient en outre qu'Equifax n'a pas réagi à l'intrusion illégale dans la base de données de manière appropriée ou efficace[82], et que le fait de ne pas prendre les mesures appropriées pour empêcher l'accès non autorisé à des renseignements financiers sensibles constituait une atteinte intentionnelle ou inconsidérée à leur vie privée[83].

*Owsianik* a été la première des trois affaires de la Trilogie à être entendue par les tribunaux inférieurs à l'automne 2019. En première instance, le tribunal a autorisé la demande pour intrusion dans l'intimité des demandeurs, estimant qu'il n'était pas clair et évident que le délit d'intrusion dans l'intimité ne pouvait être retenu au procès sur le fond[84]. Toutefois, en soulignant l'absence d'une intrusion réelle de la part d'Equifax dans le scénario présenté, la majorité de la Cour divisionnaire a déclaré que d'autres catégories de responsabilité pouvaient contrôler de manière plutôt adéquate le comportement du défendeur – à savoir le délit de négligence[85].

### *3.2.2 Obodo*

Dans l'affaire *Obodo*, le représentant des membres a déposé sans succès une requête en vue d'obtenir l'autorisation d'une action pour intrusion dans l'intimité contre le détenteur de données, dans ce cas TransUnion, qui avait subi une fuite de données importante[86]. La Cour supérieure de l'Ontario s'est notamment basée sur Owsianik pour conclure que le délit d'intrusion dans l'intimité ne pouvait s'étendre aux activités de piratages visant des renseignements personnels et pour rejeter la requête[87].

### *3.2.3 Winder*

Dans l'affaire *Winder*, le représentant des membres a tenté de faire valoir que le comportement de Marriott, qui avait obtenu leurs renseignements personnels de manière trompeuse par de fausses prémisses, faisait de lui un intrus « imprudent »[88] (notre traduction) et non un simple détenteur de données. Alors que le tribunal consi-

81. *Agnew-Americano* v. *Equifax Canada Co.*, préc., note 79, par. 63.
82. *Id.*, par. 66.
83. *Id*.
84. *Id*.
85. *Owsianik* v. *Equifax Canada Co.*, préc., note 80, par. 57.
86. *Obodo* v. *Trans Union of Canada, Inc.*, préc., note 69.
87. *Id.*, par. 22.
88. *Winder* v. *Marriott International, Inc.*, 2022 ONSC 390, par. 9.

dérait, tout au plus, que le comportement de Marriott aurait pu en faire un intrus « constructif »[89] (notre traduction), il a finalement décidé que le délit d'intrusion dans l'intimité devait avoir un champ d'application étroit. Se référant à l'arrêt *Jones*, la Cour supérieure a conclu que l'extension du délit d'intrusion dans l'intimité aux intrus « constructifs »[90] (notre traduction) entraînerait une multiplication des litiges et attribuerait une responsabilité à un comportement déjà adéquatement contrôlé par d'autres causes d'action, comme la négligence ou la rupture de contrat[91]. Par conséquent, la Cour a déterminé que le demandeur n'avait pas invoqué une cause d'action juridiquement viable à l'encontre de Marriot pour le délit d'intrusion[92].

### 3.3 Raisonnement de la Cour d'appel de l'Ontario

En juin 2022, la CA ON a entendu les appels dans chacune des trois affaires de la Trilogie de manière consécutive et a rejeté chacun d'eux dans une décision commune en novembre 2022, convenant que les détenteurs de données ne pouvaient être tenus responsables du délit d'intrusion dans l'intimité des demandeurs dans ces circonstances. Ce faisant, la CA ON a apporté d'importantes clarifications sur la portée et l'application au délit d'intrusion dans l'intimité. Notamment, elle a profité de l'occasion pour réitérer les trois éléments de délit, comme ils sont définis dans l'arrêt *Jones* mentionné plus haut, et les a appliqués aux affaires dont elle était saisie.

Dans chacune des trois affaires, la demande des plaignants n'a pas satisfait à la condition du délit d'intrusion dans l'intimité relative à la performance du défendeur d'une intrusion, sans justification légale, dans les affaires privées ou les préoccupations personnelles du plaignant, et par conséquent, aucun des détenteurs de données n'a été accusé d'avoir porté atteinte à la vie privée des plaignants. La Cour estimait en effet que les détenteurs n'avaient pas commis l'action requise par le délit, car les accès illégitimes aux données qui ont eu lieu n'avaient rien à voir avec les actions des détenteurs de données[93]. Le tort causé par les détenteurs de données découlait plutôt du fait qu'ils n'avaient pas respecté leurs obligations envers les membres en ce qui concerne la protection de leurs intérêts en matière de vie

89. *Id.*, par. 16.
90. *Id.*, par. 15.
91. *Id.*, par. 13-16.
92. *Id.*, par. 18.
93. *Owsianik* v. *Equifax Canada Co.*, préc., note 68, par. 54.

privée[94]. À cet égard, le tribunal conclut que les actions n'étaient pas recevables et ne pouvaient procéder, car elles ne présentaient pas de comportement susceptible de constituer une intrusion ou une atteinte à la vie privée des membres.

Le juge David Doherty, écrivant pour une cour unanime, résuma le raisonnement de la CA ON sur la question de responsabilité des détenteurs de données pour l'intrusion dans l'intimité des demandeurs dans l'ensemble de la Trilogie :

> Sur la base des faits invoqués, les défendeurs n'ont rien fait qui puisse constituer un acte d'intrusion ou d'atteinte à la vie privée des plaignants. Les intrusions alléguées ont été commises par des pirates informatiques tiers inconnus, agissant indépendamment des intérêts des détenteurs de données et au détriment de ceux-ci.[95] (Notre traduction)

La CA ON a également rejeté l'argument selon lequel la prétendue « insouciance »[96] des détenteurs de données quant aux conséquences d'une conservation négligente des données pouvait engager leur responsabilité. La CA ON précise que l'exigence comportementale et l'exigence d'état d'esprit du délit d'intrusion dans l'intimité étaient des éléments distincts du délit, qui doivent tous deux être satisfaits séparément pour établir la responsabilité des défendeurs. En l'espèce, il n'y avait pas de comportement allégué de la part de l'un ou l'autre des défendeurs susceptibles d'équivaloir à une intrusion dans la vie privée des membres, et l'imprudence alléguée dans l'exécution d'une autre obligation ne pouvait pas à elle seule satisfaire aux éléments du délit.

### *3.3.1 Responsabilité du fait d'autrui*

Bien que les trois groupes de la Trilogie aient soumis une demande commune pour étendre le champ d'application du délit d'intrusion dans l'intimité au-delà des intrus réels (ex. : les pirates informatiques), c'est-à-dire à ceux qui n'ont pas protégé correctement les renseignements personnels dont ils ont la charge (ex. : les détenteurs de données), la CA ON a rejeté cette demande, estimant que

94. *Id.*, par. 61 ; *Winder* v. *Marriott International, Inc.*, préc., note 70, par. 20.
95. *Owsianik* v. *Equifax Canada Co.*, préc., note 68, par. 7.
96. *Id*.

cela créerait un fondement juridique trop large pour l'établissement de la responsabilité en cas de délit intentionnel[97].

Dans le même sens, il convient de souligner la demande soumise par les membres dans l'affaire *Obodo* en vertu de laquelle les détenteurs de données pourraient être tenus responsables des actes intrusifs commis par des tiers. Cette demande a également été rejetée par la CA ON, qui a déclaré que la responsabilité du fait d'autrui repose sur l'existence d'une relation employeur-employé et sur des raisons de principe qui justifient l'extension de la responsabilité à l'employeur pour les actes accomplis en son nom par son employé[98]. Dans cette affaire, les pirates informatiques à l'origine de l'incident de confidentialité n'entretenaient pas de relation employeur-employé avec les détenteurs de données. Par conséquent, ce dernier ne pouvait être tenu responsable des actions des cybercriminels.

En somme, la CA ON a jugé que, comme aucun des groupes n'a pu démontrer qu'un des détenteurs de données s'était directement immiscé dans la vie privée des membres, élément central du délit d'intrusion dans l'intimité, les détenteurs de données ne peuvent être tenus responsables dans ces circonstances. Toutefois, la CA ON a noté que cette conclusion n'exclut pas la possibilité que, dans d'autres circonstances, des détenteurs de données soient tenus responsables en cas de négligence s'ils ne prennent pas les mesures nécessaires pour protéger les renseignements personnels, causant ainsi des dommages réels aux individus concernés, plutôt que symboliques[99].

97. *Obodo* v. *Trans Union of Canada, Inc.*, préc., note 69, par. 65.
98. *Id.*, par. 25 ; Il est intéressant de noter le raisonnement de la Cour dans une affaire connexe, l'affaire *Broutzas*, dans laquelle le tribunal a examiné si les organismes de planification de l'épargne-études devaient être tenus responsables du délit d'intrusion dans l'intimité pour avoir acheté des renseignements personnels de patients auprès d'employés malhonnêtes d'hôpitaux. La Cour divisionnaire a conclu que les organismes de planification ne pouvaient pas être considérés comme étant des « intrus » dans les affaires personnelles des patients, car ils n'avaient pas accédé aux dossiers hospitaliers. Pour les tenir responsables, il faudrait étendre la portée du délit, en faisant la preuve que les organismes de planification savaient ou auraient dû savoir que les renseignements étaient obtenus de manière illicite, et qu'à ce titre, ils étaient devenus parties prenantes de la violation (*Broutzas* v. *RVHS*, 2023 ONSC 540, par. 48-54).
99. *Owsianik* v. *Equifax Canada Co.*, préc., note 68, par. 79.

## 3.4 Observations

### *3.4.1 Distinguer le délit d'intrusion dans l'intimité et le délit de négligence*

Les conclusions de la Trilogie d'Owsianik semblent limiter les recours disponibles aux victimes d'atteinte à la vie privée, particulièrement en réduisant les scénarios où des demandes d'intrusion dans l'intimité et de négligence peuvent être soumises conjointement avec succès. En effet, en raison de la Trilogie, de telles victimes ne peuvent compter sur ces deux recours que lorsqu'elles poursuivent une partie qui a participé activement à l'accès illégal de leurs renseignements personnels. À la lumière de ce changement, il est important de distinguer ces deux délits afin de correctement conseiller les parties susceptibles d'être impliquées dans une action collective intentée à la suite d'un incident de confidentialité.

Tout d'abord, le délit de négligence présente l'avantage considérable de ne pas exiger du demandeur qu'il prouve l'existence des trois éléments de l'intrusion de l'intimité établis dans *Jones* : une intrusion dans l'intimité du demandeur par le défendeur, commise de manière intentionnelle ou inconsidérée, et considérée comme étant très offensante et causant de la détresse, de l'humiliation ou de l'angoisse[100]. La combinaison de ces éléments requiert des circonstances particulières, limitant les situations permettant le succès de ce recours, illustrant ainsi l'intention du juge Sharpe de la CA ON d'éviter d'ouvrir « les vannes »[101] (notre traduction) de l'action collective avec sa décision dans l'arrêt *Jones*. Il est particulièrement plus facile de prouver le critère de l'état d'esprit dans le cas de la négligence, où il suffit de démontrer que le défendeur n'a pas fait preuve du degré de diligence qu'une personne raisonnable aurait exercé, alors que le délit d'atteinte à la vie privée nécessite de démontrer l'intentionnalité ou l'inconsidération.

Un recours pour délit d'intrusion dans l'intimité peut toutefois présenter plusieurs avantages pour le demandeur, car, contrairement au délit de négligence, ce délit n'exige pas la preuve d'une relation de proximité entre le défendeur et le plaignant suffisante pour donner lieu à une obligation de diligence. En outre, le délit d'intrusion dans l'intimité ne requiert pas d'établir la présence d'un préjudice économique réel. La raison de ce fardeau de preuve allégé est que la

100. *Jones* v. *Tsige*, préc., note 71, par. 71.
101. *Id.*, par. 71.

demande pour intrusion dans l'intimité vise à réparer l'humiliation et le préjudice émotionnel subis par une intrusion personnelle dans des situations où d'autres recours sont impossibles parce que le préjudice subi ne peut être facilement quantifié[102]. Il en suit alors que les plaignants peuvent obtenir des dommages symboliques non pécuniaires, sans avoir à atteindre le seuil de préjudice grave et prolongé applicable aux actions pour négligence, en vertu de la décision de la Cour suprême *Mustapha* c. *Culligan of Canada Ltd.*[103].

Cet avantage du délit d'intrusion dans l'intimité est particulièrement important dans les affaires d'atteinte à la vie privée, puisque comme l'ont remarqué les auteurs Anne Merminod, Karine Chênevert et Markus Kremer[104], la preuve des dommages et intérêts indemnisables, que requiert le délit de négligence, constitue un enjeu important dans ce type d'affaires.

Il convient enfin de mentionner ici l'arrêt *Lamoureux*[105], une décision de la Cour supérieure du Québec confirmée par la Cour d'appel du Québec (ci-après la « CA QC ») et la première décision rendue sur le fond au Canada en matière de perte de renseignements personnels qui retient que les troubles et inconvénients subis par les membres à la suite de la perte des renseignements personnels ne peuvent constituer des dommages susceptibles d'être indemnisés. En effet, même alors que l'Organisme canadien de réglementation du commerce des valeurs mobilières, le défendeur dans cette affaire, a admis qu'il n'avait pas protégé les données de manière adéquate[106], la CA QC a tout de même refusé d'octroyer des dommages aux membres parce que, entre autres, ces derniers n'avaient pu démontrer que les dommages causés par l'incident de confidentialité dépassaient les conséquences raisonnables ou les inconvénients quotidiens, ou qu'ils étaient suffisamment graves ou indemnisables au sens de la jurisprudence établie en matière du délit de négligence[107].

---

102. Anne MERMINOD, Karine CHÊNEVERT et Markus KREMER, « Two Solitudes of Privacy: Privacy Class Actions in Quebec and the Rest of Canada », dans S.F.C.B.Q., vol. 480, *Colloque national sur l'action collective Développements récents au Québec, au Canada et aux États-Unis*, Montréal, Éditions Yvon Blais, 2020, p. 67-96.
103. *Mustapha* v. *Culligan of Canada Ltd.*, 2008 CSC 27, par. 9.
104. A. MERMINOD, K. CHÊNEVERT et M. KREMER, préc., note 102, p. 86.
105. *Lamoureux* c. *OCRCVM*, 2021 QCCS 1093.
106. *Id.*, par. 43.
107. *Id.*, par. 23.

### *3.4.2 Conséquences de la Trilogie sur les litiges en vie privée et les actions collectives*

Alors que plusieurs provinces de common law, notamment l'Ontario, avaient adopté une approche plus libérale en matière d'indemnisation dans les actions pour atteinte à la vie privée, la Trilogie d'Owsianik apporte des clarifications importantes au champ d'application du délit d'intrusion dans l'intimité et rapproche le droit applicable en Ontario à celui du Québec. Notamment, cette Trilogie limite les risques, auxquels s'exposent les entreprises qui recueillent des renseignements personnels, des manières suivantes :

- Leur responsabilité en cas de piratage de données pourrait être réduite et se limiter aux dommages économiques réels ayant été démontrés de manière satisfaisante à un tribunal.

- Leur responsabilité pour un délit d'intrusion dans l'intimité d'un individu ne peut être engagée que si elles participent activement à l'accès illicite aux renseignements personnels d'autrui.

### *3.4.3 Une tendance en faveur des défendeurs*

La Trilogie d'Owsianik s'inscrit dans une tendance plus large de décisions[108] rendues au courant des trois dernières années favorables aux entreprises victimes de piratage informatique et qui limitent la portée des délits d'intrusion dans l'intimité et de négligence dans des contextes d'action collective.

Par exemple, dans l'affaire *Setoguchi* c. *Uber B.V.*[109], la Cour d'appel de l'Alberta (la « CA AB ») a rendu une décision dans la même veine que l'arrêt *Lamoureux* mentionné plus haut et en se référant plusieurs fois à la Trilogie pour justifier son refus d'autoriser une action collective intentée par des clients d'Uber à la suite d'un vol des données des utilisateurs et chauffeurs de la compagnie effectué par des pirates informatiques. Les membres du groupe demandeur avaient intenté une action collective contre Uber pour rupture de contrat et négligence, ainsi que pour avoir manqué à son obligation de diligence envers les membres du groupe, en ne prenant pas les

---

108. Voir *Del Giudice* c. *Thompson*, 2021 ONSC 5379 ; *Kaplan* c. *Casino Rama*, 2019 ONSC 2025, d'un intérêt particulier au paragraphe 21 « la possibilité que les membres du groupe soient victimes d'un vol d'identité ou d'une fraude à l'avenir ne donne pas lieu à des dommages-intérêts indemnisable » (notre traduction) ; et *Stewart* c. *Demme*, 2022 ONSC 1790.
109. *Setoguchi* v. *Uber B.V.*, 2023 ABCA 45.

mesures adéquates pour protéger leurs renseignements personnels. Alors que la CA AB était à la recherche d'un « préjudice réel »[110] (notre traduction) et indemnisable afin de justifier l'action en négligence et de statuer sur l'autorisation de l'action, mais ne trouvant aucune preuve de celle-ci, la CA AB a conclu qu'elle ne pouvait autoriser la demande d'action en négligence.

La CA AB explique son raisonnement en déclarant que tout dommage subi par les membres de groupe demandeur lors de la fuite des données, incluant sous la forme de perte de renseignements personnels accessibles au public (comme les coordonnées), et d'un risque accru de fraude ou de vol d'identité, s'il est récupérable, est négligeable ou insignifiant, et n'est donc pas indemnisable en droit, ce dernier point notamment faisant écho aux propos de la Cour d'appel du Québec dans l'arrêt *Lamoureux*[111].

Le raisonnement de la CA AB selon lequel la perte de renseignements déjà accessibles au public limite le préjudice potentiel se retrouve également dans un nombre croissant de décisions relatives à des recours collectifs portant sur des questions de protection de la vie privée. Notamment, la Cour divisionnaire de l'Ontario applique le même raisonnement dans l'affaire *Broutzas*[112] pour justifier son refus d'autoriser des recours collectifs intentés la découverte d'employés d'hôpitaux qui vendaient les coordonnées de nouveaux parents à des organismes de planification de l'épargne-études[113]. Reprenant des conclusions de l'affaire *Stewart* c. *Demme*[114], la Cour dans *Broutzas* confirma que le délit d'intrusion dans l'intimité requiert une intrusion dans la vie privée très grave, un seuil qui n'est pas automatiquement atteint par toutes les intrusions[115]. En effet, même si les renseignements en question relèvent du domaine de la santé, ce seuil ne sera probablement pas atteint lorsque l'intrusion a été évanescente, que les renseignements n'étaient pas particulièrement sensibles, qu'ils étaient par ailleurs disponibles et que l'intrusion n'a pas eu d'effet perceptible sur les demandeurs[116].

110. *Id.*, par. 58.
111. *Lamoureux* c. *OCRCVM*, préc., note 105, par. 88.
112. *Broutzas* v. *RVHS*, préc., note 98.
113. *Id*.
114. *Stewart* v. *Demme*, 2022 ONSC 1790, par. 22 et 27.
115. *Broutzas* v. *RVHS*, préc., note 98, par. 40.
116. *Broutzas* v. *Rouge Valley Health System*, 2018 ONSC 6315, par. 152 ; *Broutzas* v. *RVHS*, préc., note 98, par. 31-33.

Il semble que, alors que les entreprises doivent continuer à respecter les lois applicables en matière de protection de la vie privée, les décisions rendues au cours des dernières années dans des juridictions de common law comme de droit civil dans le cadre d'actions collectives fondées sur des atteintes au droit à la vie privée montrent que les entreprises défenderesses ont plus souvent gain de cause lorsque les membres des groupes en demande ne peuvent pas prouver qu'ils ont subi des dommages indemnisables.

## CONCLUSION

Il est évident que les tribunaux à travers le Canada sont confrontés à des défis considérables en raison de l'évolution rapide des technologies. Les décisions commentées dans le présent article mettent en évidence les difficultés et les enjeux liés à l'application des lois de protection des renseignements personnels à des technologies sophistiquées comme l'intelligence artificielle et la géolocalisation et à des pratiques intrusives causées par des pirates informatiques.

En réponse à ces complexités engendrées par l'application du droit aux nouvelles technologies, les législateurs provinciaux et fédéraux semblent avoir adopté une approche centrée sur la modernisation des lois de protection des renseignements personnels assistée par la publication de lignes directrices par les autorités règlementaires. Cette approche encourage le dialogue entre les décideurs et les parties prenantes impliquées dans le développement et l'application des nouvelles technologies, tout en reconnaissant une certaine flexibilité dans l'interprétation du droit nouveau.

Cependant, il importe de prendre conscience des conséquences significatives que ces changements règlementaires auront sur les pratiques des organisations, à commencer par les entreprises et les organismes publics québécois, qui devront relever le défi de taille que constitue l'application de la quasi-totalité des obligations introduites par la Loi 25 à compter du 22 septembre 2023. Les entreprises assujetties à la législation fédérale en matière de protection des données pourraient aussi bientôt devoir se soumettre à l'exercice advenant l'adoption du projet de loi C-27, qui vise notamment de remplacer la LPRPDE par la *Loi sur la protection de la vie privée des consommateurs*.

Dans ce même sens, en se fiant sur la récente communication de la CAI aux médias[117] selon laquelle elle a été notifiée par plus de 30 organisations d'un incident de confidentialité en moins de deux mois suivant l'entrée en vigueur des premiers changements apportés à la Loi sur le privé, ce type d'enjeux n'est pas près de disparaître. Au contraire, il semble impératif que les entreprises abordent la question de la cyberresponsabilité dans le cadre de leurs activités, car ces enjeux sont susceptibles d'attirer de plus en plus l'attention du public et des médias, et par conséquent, pourraient potentiellement mener à une augmentation des actions collectives soulevant des enjeux de vie privée.

En outre, les différents acteurs impliqués dans le cycle de vie des systèmes d'intelligence artificielle (ci-après « IA ») pourraient éventuellement avoir à se conformer à un tout nouveau cadre juridique prévu par la *Loi sur l'intelligence artificielle et les données*, une autre proposition du projet de loi C-27 et la première tentative du gouvernement fédéral de légiférer sur l'IA. D'ailleurs, le gouvernement fédéral semble avoir inspiré le gouvernement québécois dans cette voie, car ce dernier a récemment annoncé qu'il chercherait également à réglementer l'utilisation de l'IA afin de mieux encadrer les activités dans ce milieu et afin d'adresser les enjeux éthiques qui s'y trouven[t118]. Les développements récents dans le domaine de l'IA, marqués notamment par le déploiement de l'algorithme ChatGPT développé par OpenAI, pourraient donc annoncer une nouvelle vague de changements législatifs.

117. Hugo JONCAS, « Une trentaine d'entreprises ont déclaré des fuites en deux mois », *La Presse*, 8 décembre 2022, en ligne : <https://www.lapresse.ca/affaires/2022-12-08/protection-des-renseignements-personnels/une-trentaine-d-entreprises-ont-declare-des-fuites-en-deux-mois.php>.

118. Alexandre ROBILLARD, « Fitzgibbon veut éviter les dérapages de l'intelligence artificielle », *Le Devoir*, 6 avril 2023, ligne : https://www.ledevoir.com/politique/quebec/788254/technologie-fitzgibbon-veut-eviter-les-derapages-de-l-intelligence-artificielle.