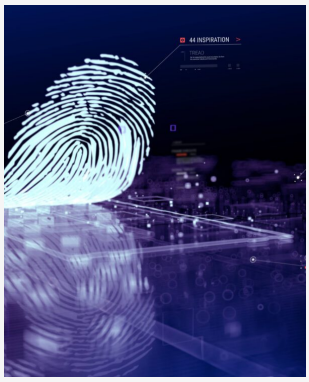
OSLER

Les 10 grandes tendances en matière de protection de la vie privée en 2025



Il s'agit du troisième article de la série consacrée aux éléments marquants de la 2e Conférence annuelle sur la protection de la vie privée à Montréal.

Accéder aux cinq bulletins d'actualités de cette série

9 DÉCEMBRE 2025 18 MIN DE LECTURE

Expertises Connexes

- Gouvernance d'entreprise
- Intelligence artificielle
- Litiges
- Litiges relatifs à la protection de la vie privée et des données
- Respect de la vie privée et gestion de l'information
- Technologie

Auteurs(trice): Éloïse Gratton, Ad. E., François Joli-Coeur

Le 21 octobre 2025, le bureau de Montréal d'Osler, Hoskin & Harcourt S.E.N.C.R.L./s.r.l. a accueilli la 2e Conférence annuelle sur la protection de la vie privée, organisée par le groupe Respect de la vie privée et gestion de l'information. Cette demi-journée, suivie d'un lunch de réseautage, a réuni des experts de l'industrie et des juristes d'entreprise pour explorer les enjeux actuels : mise en œuvre des amendements proposés par la **Loi 25**, tendances récentes en litige, gouvernance de l'intelligence artificielle (IA), technologies émergentes et cybersécurité.

La conférence s'est ouverte avec une revue des 10 des tendances les plus importantes de la dernière année en protection de la vie privée selon Eloïse Gratton, associée et cochef du groupe Respect de la vie privée et gestion de l'information d'Osler et François Joli-Coeur, associé.

Nous avons déjà publié les deux articles suivants : « Cybersécurité et protection de la vie privée : ce qu'il faut retenir de notre 2e Conférence annuelle » et « L'évolution du rôle du responsable de la protection de la vie privée à l'ère de l'innovation et de l'intelligence artificielle ».

Dans les prochaines semaines, nous ferons paraître des articles sur les deux autres grands sujets abordés lors de la conférence :

- *Revue de l'année sur les litiges en matière de vie privée*
- *Intelligence artificielle : gouvernance et autres enjeux émergents*

Voici les tendances à noter de la dernière année et les enseignements à retenir pour votre entreprise.

1. Biométrie : hausse continue de l'adoption et risques accrus

Les systèmes biométriques se déploient rapidement dans tous les secteurs : du contrôle d'accès et horodateurs en milieu de travail à la prévention des pertes dans le commerce de détail, en passant par la vérification d'identité numérique. Les autorités réglementaires canadiennes demeurent particulièrement actives dans ce secteur.

Au Québec, la Commission d'accès à l'information (CAI) a reçu plus de 100 déclarations biométriques en 2024-2025[1] en vertu de la *Loi concernant le cadre juridique des technologies de l'information*, une hausse de 206 % sur une période de trois ans. Cette croissance témoigne de la popularité des méthodes d'authentification et d'identification biométriques.

Les entreprises qui déclarent à la CAI qu'elles utilisent un système biométrique reçoivent souvent des lettres de réponse suggérant une utilisation possiblement non-conforme (par exemple, consentement non valide, test de nécessité/proportionnalité non rencontré, manque de mesure alternative, etc.). Bien que ces lettres ne constituent pas des décisions officielles ou contraignantes, elles relèvent généralement des violations *potentielles* sur la base de l'examen préliminaire par la CAI de la documentation.

Au sujet des enquêtes officielles, la CAI a, dans les décisions *Métro* (2025) et *Transcontinental* (2024), réaffirmé son scepticisme quant à la nécessité et à la proportionnalité des systèmes biométriques en vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé* (la Loi sur le privé). Cette approche s'explique en partie par le fait que la CAI considère les renseignements biométriques comme des renseignements personnels particulièrement sensibles en raison de leur caractère unique et immuable. Ainsi, la CAI exige des entreprises qu'elles présentent des preuves tangibles démontrant que la collecte répond à un objectif légitime, important et réel et que l'atteinte à la vie privée est proportionnelle à l'objectif poursuivi.

Au niveau fédéral, le Commissariat à la protection de la vie privée du Canada (CPVP) a publié son Document d'orientation à l'intention des entreprises sur le traitement des renseignements biométriques. Ces nouvelles lignes directrices présentent les principaux facteurs et principes que les organisations doivent prendre en compte lors de la conception et du déploiement d'initiatives biométriques, notamment :

- La nécessité d'établir que le but de l'initiative est légitime, approprié et proportionné aux risques pour la vie privée;
- Les exigences relatives à l'obtention d'un consentement valide;
- L'importance de la minimisation des données, de la transparence, de mesures robustes de protection et du maintien de l'exactitude des systèmes biométriques.

Contrairement à la position de la CAI, le CPVP évoque la possibilité que la biométrie puisse être une condition de service (c'est-à-dire qu'une alternative ne soit pas offerte).

Par ailleurs, les autorités élargissent également la notion de « donnée biométrique ». Dans leurs conclusions conjointes suivant leur enquête sur le réseau social TikTok, les commissaires provinciaux et fédéral ont traité certains traits non identifiants comme biométriques, suggérant que toute technologie capable d'analyser des caractéristiques physiologiques ou comportementales peut déclencher des obligations accrues. Les entreprises utilisant ces technologies devraient réévaluer si leurs traitements relèvent de la biométrie et ajuster leur gouvernance interne.

À retenir : Entre l'interprétation stricte de la CAI et l'encadrement plus nuancé du CPVP en

matière de biométrie, les organisations doivent déterminer où elles souhaitent se situer sur le spectre du risque et de la conformité, tout en documentant rigoureusement la nécessité et la proportionnalité de leurs usages biométriques.

2. Incidents de confidentialité : explosion des signalements et évolution des menaces

Depuis l'entrée en vigueur des obligations de signalement des incidents de confidentialité au Québec en 2022[2], la CAI a connu une augmentation de 559 % du nombre d'avis, soit un total de 514 en 2024-2025[3]. Du côté fédéral, le CPVP a reçu 615 déclarations d'atteinte à la sécurité des données au cours du même exercice, un volume semblable à celui de l'année précédente.[4]

L'amélioration des outils de détection des incidents et la sensibilisation accrue aux enjeux de protection des renseignements personnels au sein des entreprises, souvent encouragées par les autorités réglementaires elles-mêmes, peuvent en partie expliquer l'augmentation des déclarations. Or, cette transparence accrue s'accompagne d'une attention réglementaire plus soutenue, créant une dynamique où le respect des attentes réglementaires en matière de prévention et de signalement conduit paradoxalement à un risque plus élevé d'enquête. Les autorités de la protection des renseignements personnels canadiennes, y compris la CAI et le CPVP, effectuent désormais davantage de suivis post-signalement d'incidents, notamment pour évaluer si les entreprises ont mis en place des mesures pour éviter des incidents similaires dans le futur. Toutefois, pour l'instant, les autorités concentrent leurs activités de surveillance sur les incidents majeurs.

Quant aux attaques, elles sont plus complexes et souvent ciblées sur les chaînes d'approvisionnement et les infrastructures critiques. Le projet de loi C-8, déposé en juin 2025, vise d'ailleurs à édicter la *Loi sur la protection des cybersystèmes essentiels* qui prévoit un cadre de protection des cybersystèmes essentiels liés aux services et systèmes qui sont d'une importance critique pour la sécurité nationale ou la sécurité publique. Nous constatons également une augmentation des attaques provenant de l'interne (*insider threat*), forçant les entreprises à redoubler d'ardeur pour développer des systèmes de détection sophistiqués.

Face à l'évolution des menaces, les organisations se préparent par le biais d'exercices de simulation (« *table top* ») et par le biais de procédures de réponse aux incidents.

À retenir : Avec la multiplication des enquêtes et des suivis déclenchés par les signalements d'incidents, les organisations ont tout intérêt à renforcer leurs pratiques de prévention, en consolidant leurs mesures de protections physiques, organisationnelles et administratives afin de réduire les risques d'incident à la source et d'éviter d'éventuelles enquêtes. Une vigilance accrue s'impose également face aux menaces internes, encore trop souvent sous-estimées.

3. Demandes d'accès : de la conformité à la stratégie contentieuse

Nous constatons que les demandes d'accès en vertu des lois sur la protection des renseignements personnels deviennent des outils stratégiques pour préparer des litiges contre les entreprises ou des plaintes à différentes autorités réglementaires. Cette tendance s'explique en partie par l'utilisation croissante d'outils d'IA générative pour la rédaction automatisée de ces demandes, ce qui entraîne une hausse notable de leur volume et de leur sophistication, renforçant ainsi leur pertinence dans un contexte contentieux. Ces requêtes visent désormais un éventail beaucoup plus large de renseignements, avec des descriptions

extrêmement détaillées des informations recherchées, notamment les métadonnées, journaux, scores internes et autres données dérivées.

Face à la croissance des demandes, certaines organisations font appel à des processus de triage et de réponses automatisées. Ces processus peuvent toutefois connaître des défaillances. Par exemple, ces systèmes automatisés produisent parfois des réponses trop génériques qui ne répondent pas aux exigences spécifiques de la loi applicable. Lorsque la réponse est incomplète ou tardive, les personnes concernées peuvent être incitées à déposer une plainte auprès des autorités réglementaires. Pour éviter une telle situation, les organisations doivent adopter une approche juridiquement défendable à l'égard des réponses générées par ces processus automatisés, ce qui suppose notamment d'indiquer clairement aux utilisateurs les objectifs de ces processus, qui ne visent pas nécessairement à donner accès à l'ensemble des renseignements détenus par l'organisation, mais plutôt à faciliter un accès autonome à certaines informations, tout en précisant les moyens d'obtenir des renseignements supplémentaires. Il est également essentiel que les équipes juridiques collaborent étroitement avec les équipes techniques afin d'extraire efficacement les données pertinentes, tout en assurant la cohérence des communications.

À retenir : Avec l'augmentation du volume et de la complexité des demandes d'accès, les organisations doivent renforcer la maturité et la capacité de leurs programmes de gestion des demandes d'accès. Les processus automatisés peuvent améliorer l'efficacité, mais ils doivent être conçus et supervisés de façon à demeurer juridiquement défendables, transparents et conformes aux exigences légales applicables.

4. Vie privée des enfants : une priorité nationale

La vie privée des enfants s'impose de plus en plus comme une priorité à la fois réglementaire et politique.

Sur le plan législatif, le ministre de l'Innovation, Evan Solomon, a affirmé que la protection des jeunes sera au cœur de la réforme fédérale à venir[5]. Cette évolution s'inscrit dans une tendance internationale plus large : plusieurs juridictions, dont l'Union européenne, imposent déjà des exigences accrues en matière de protection des données des mineurs.

L'enquête conjointe sur le réseau social TikTok a d'ailleurs mis en lumière les pratiques de collecte, d'utilisation et de communication de renseignements personnels de mineurs. Le CPVP considère désormais les renseignements personnels des enfants comme étant des renseignements sensibles par défaut[6] et mène une consultation sur un Code sur la protection des renseignements personnels des enfants. Le CPVP a également récemment conclu une consultation sur le contrôle de l'âge. Dans ce contexte, les organisations doivent aussi composer avec des seuils d'âge du consentement différents selon les juridictions : au Québec, ce seuil est fixé à 14 ans, alors que le reste du Canada s'oriente plutôt vers un âge de 13 ans, créant ainsi des obligations de conformité différentes.

Dans ce contexte de vigilance accrue, les risques juridiques se multiplient : au Québec, des dizaines de développeurs de jeux vidéo font actuellement l'objet d'une action collective alléguant leur violation de la vie privée des enfants.

À retenir : Alors que la protection de la vie privée des enfants prend une place grandissante sur les plans réglementaires et politiques, les entreprises offrant des services numériques destinés aux jeunes devraient se préparer à une surveillance accrue des mécanismes de contrôle de l'âge, ainsi qu'à des exigences plus strictes de validation du consentement et de transparence.

5. Souveraineté des données : enjeux politiques et choix d'infrastructure

Le débat sur la localisation des données et l'accès étranger aux données se concrétise de plus en plus. En 2025, les gouvernements et grandes entreprises exigent un meilleur contrôle de la localisation des données canadiennes.

Les inquiétudes liées au CLOUD Act américain alimentent la prudence à l'égard de l'hébergement transfrontalier. Plusieurs organisations privilégient désormais des fournisseurs d'hébergement établis au Canada ou, lorsqu'ils traitent avec des entreprises étrangères, exigent que seules les juridictions canadiennes aient compétence sur les données domestiques. Parallèlement, certains organismes publics ajoutent des clauses de localisation à leurs appels d'offres.

La Stratégie fédérale en matière d'informatique souveraine pour l'IA démontre que la souveraineté numérique devient un pilier de la politique industrielle et de l'IA.

Pour le secteur privé, cela impose de concilier efficacité et conformité — souvent au moyen de solutions de nuages souverains ou hybrides.

À retenir : Alors que la souveraineté numérique s'impose à la fois comme enjeu politique et contractuel, les entreprises devraient l'intégrer à leur planification stratégique et à leur cartographie des risques, afin d'anticiper les attentes croissantes des autorités réglementaires et des clients institutionnels.

6. Application de la loi : plus d'enquêtes, pas encore d'amendes

Malgré les pouvoirs accrus de la CAI découlant des amendements introduits par la Loi 25, la CAI n'a pas encore imposé de sanctions administratives pécuniaires, mais son activité d'enquête s'intensifie. Les récentes décisions couvrent un éventail plus large d'entreprises, y compris des acteurs québécois dans le commerce de détail ou la fabrication. Les enquêtes conjointes avec d'autres autorités canadiennes se multiplient, et les autorités réglementaires s'intéressent davantage aux menaces internes et aux usages abusifs de données à l'interne.

À retenir : le fait qu'aucune amende n'ait été imposée ne doit pas être interprété comme de la clémence. Les attentes en matière de programmes de gestion de la vie privée continuent de croître.

7. Technologies de surveillance : entre sécurité et conformité

Face à la hausse des risques de sécurité, les organisations adoptent des technologies d'observation — analyses en magasin, suivi des employés, détection comportementale. La décision *Métro* a illustré la tension entre la prévention des pertes et la nécessité de protéger la vie privée : les objectifs légitimes de sécurité doivent rester proportionnés et appuyés par une évaluation rigoureuse de la nécessité des mesures déployées.

En milieu de travail, la surveillance à distance, les caméras et le suivi de productivité posent des défis similaires. Dans ce contexte, la transparence, la minimisation et des politiques internes claires sont essentielles.

En ligne, les outils d'analyse comportementale alimentés par l'IA brouillent la frontière entre

sécurité, profilage et consentement. Les organisations doivent documenter leurs fins et évaluer les risques, notamment lorsque les décisions automatisées ont des impacts sur les droits ou l'emploi des individus. La réalisation d'évaluations des facteurs relatifs à la vie privée (ÉFVP) et la mise en place d'un cadre de gouvernance algorithmique deviennent ainsi des composantes incontournables d'une gestion responsable de la surveillance numérique.

À retenir : Alors que les organisations multiplient l'usage de technologies de surveillance pour renforcer la sécurité, leur déploiement doit être soigneusement planifié en évaluant la nécessité et la proportionnalité des mesures, en intégrant la protection de la vie privée dès la conception et en assurant une documentation rigoureuse.

8. Profilage et confidentialité par défaut : la prochaine frontière interprétative

Au Québec, les nouvelles règles sur la prise de décision automatisée et la confidentialité par défaut instaurent un cadre de mise en œuvre complexe, surtout pour les systèmes d'IA en constante évolution. Les entreprises doivent revoir leurs interfaces utilisateurs, leurs paramètres par défaut et leurs mécanismes de révision internes pour garantir une personnalisation transparente et équitable. Elles devraient également être en mesure d'expliquer la logique de leurs systèmes et de documenter la nature des inférences produites.

Par ailleurs, les complexités propres au contexte québécois se révèlent dans la décision rendue en vertu de la Loi sur le privé par la CAI, exposée dans le rapport d'enquête conjoint 2025-003. Cette dernière précise que les obligations de confidentialité par défaut au Québec ne sont pas identiques à celles du RGPD en raison des différences de formulation entre l'article 9.1 de la Loi sur le privé et l'article 25 du RGPD. Cette distinction ajoute une couche supplémentaire d'incertitude quant à l'étendue concrète des obligations de confidentialité par défaut et aux attentes pratiques des autorités réglementaires.

À retenir : Le profilage et la confidentialité par défaut constituent un terrain encore incertain, tant au niveau fédéral qu'au Québec, ce qui oblige les entreprises à naviguer avec prudence. Elles doivent suivre de près l'évolution des normes, anticiper les zones grises dans leurs pratiques de personnalisation et être prêtes à adapter rapidement leurs systèmes et processus aux orientations futures des autorités réglementaires.

9. Conception trompeuse : le consentement sous la loupe

Le rapport 2024 du CPVP sur les pratiques de conception manipulatrices ouvre un nouveau front d'application. Les autorités réglementaires s'intéressent désormais non seulement au fait qu'un utilisateur ait consenti, mais à la manière dont le consentement est obtenu.

Des pratiques comme les cases précochées, les formulations trompeuses, les incitations répétées ou les obstacles artificiels peuvent invalider le consentement. Le CPVP a identifié plusieurs catégories problématiques (interférence, obstruction, contrainte, harcèlement), alignées sur les normes internationales telles que le *Digital Services Act* européen.

À retenir : Face à une attention accrue des autorités réglementaires à l'égard de la manière dont le consentement est obtenu, les entreprises canadiennes gagneraient de revoir leurs interfaces et paramètres de confidentialité. Le consentement devient une question de gouvernance du design, autant que de conformité juridique.

10. Intelligence artificielle : le nouveau test de résistance du droit à la vie privée

L'IA transforme la conformité en matière de vie privée en profondeur. Les enquêtes conjointes sur OpenAI et X (Twitter) illustrent l'attention croissante portée par les autorités réglementaires à la réutilisation des données, aux fins secondaires et à l'entraînement des modèles, ce qui démontre que même des acteurs internationaux de premier plan ne sont pas à l'abri d'une surveillance réglementaire rigoureuse.

Les questions clés dominent le paysage canadien :

- Les organisations peuvent-elles utiliser les données clients ou internes pour entraîner des modèles d'IA sans consentement explicite?
- Comment limiter contractuellement l'utilisation des données clients par les fournisseurs pour entraîner leurs propres systèmes?
- Quand les « assistants » ou « scribes » d'IA déclenchent-ils les obligations de divulgation liées à la prise de décision automatisée (article 12.1 de la Loi sur le secteur privé au Québec)?

Ces questions révèlent l'importance croissante de la transparence, de l'explicabilité et de la limitation des fins dans l'utilisation de l'IA. En 2026, les programmes de conformité en matière de vie privée ne pourront plus être envisagés séparément de la gouvernance de l'IA.

À retenir : Face à l'attention croissante des autorités réglementaires portée sur l'utilisation des données pour entraîner les systèmes d'IA, les entreprises devront établir des processus intégrés de gestion des données et des algorithmes, en favorisant une collaboration étroite entre juristes, techniciens et experts en éthique, afin d'assurer une utilisation responsable de l'IA et de renforcer la confiance des clients et des partenaires.

Conclusion : une année placée sous le signe de la responsabilité

Derrière ces dix tendances se profile un fil conducteur : les autorités réglementaires s'attendent à ce que les organisations ne se contentent plus de respecter la loi, mais démontrent une véritable responsabilité — en documentant la nécessité de leurs initiatives, en expliquant leurs choix et en intégrant la protection des renseignements personnels dans leurs opérations quotidiennes.

L'intersection entre vie privée, cybersécurité et intelligence artificielle se densifie rapidement. Au cours des prochains mois, l'équipe AccessPrivacy d'Osler publiera des analyses de suivi sur plusieurs thèmes de la conférence, notamment la gouvernance de l'IA, la protection des enfants et les risques émergents de recours collectifs.

Pour les professionnels de la vie privée, 2025 ne marque pas seulement une année d'adaptation, mais aussi le début d'une nouvelle ère de gouvernance intégrée et fondée sur les risques au Canada.

---

[1] CAI, Rapport annuel d'activités et de gestion 2024-2025.

[2] Loi sur le privé, article 3.5.

[3] CAI, « Rapport annuel d'activités et de gestion 2024-2025 ». (octobre 2025)

[4] CPVP, « Rapport annuel au Parlement 2024-2025 concernant la Loi sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels et les documents électroniques » (5 juin 2025).

[5] Toronto Star, « Evan Solomon says lessons from TikTok privacy probe will help shape new Canadian AI laws » (24 septembre 2025).

[6] Commissaires fédéral, provinciaux et territoriaux à la protection de la vie privée et des ombuds responsables de la protection de la vie privée, « Mettre l'intérêt supérieur des jeunes à l'avant-plan en matière de vie privée et d'accès aux renseignements personnels » (4-5 octobre 2023) .