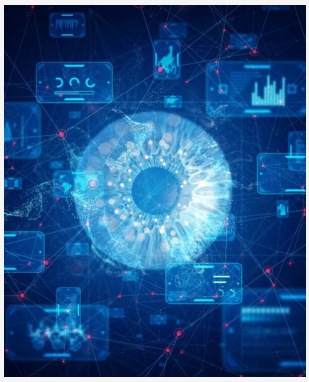
OSLER

Cybersécurité et protection de la vie privée : ce qu'il faut retenir de notre 2e Conférence annuelle

21 NOVEMBRE 2025 8 MIN DE LECTURE



Expertises Connexes

- Gestion de risques et réponse aux crises
- Gouvernance d'entreprise
- Intelligence artificielle
- Litiges
- Respect de la vie privée et gestion de l'information
- Technologie

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

Key Takeaways

- La 2e Conférence annuelle sur la protection de la vie privée organisée par Osler s'est concentrée sur les amendements proposés par la loi 25, la cybersécurité, les tendances récentes en protection de la vie privée, l'évolution du rôle de responsable en protection des données et la gouvernance de l'IA.
- Guillaume Clément, expert en cybersécurité chez KPMG, a souligné que la cybersécurité est une responsabilité partagée à l'échelle de l'entreprise, et non plus une question de technologie.

Le bureau de Montréal d'Osler a récemment accueilli en octobre dernier 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.

L'un des moments forts de l'événement a été la discussion entre Eloïse Gratton, associée et cochef du groupe national Respect de la vie privée et gestion de l'information d'Osler et Guillaume Clément, associé, Services en cybersécurité, KPMG et président de KPMG Egyde Conseils. Voici les faits saillants de cet entretien, riche en perspectives pratiques pour les entreprises canadiennes.

Guillaume Clément : un regard d'expert sur les menaces de cybersécurité modernes

Fort de plusieurs années d'expérience terrain auprès d'organisations de divers secteurs, Guillaume Clément conseille régulièrement des entreprises confrontées à des attaques de cybersécurité sophistiquées. Son message : les menaces évoluent très rapidement, et la capacité d'y faire face repose autant sur la technologie que sur la culture, les processus et l'engagement de la haute direction.
« La cybersécurité n'est plus seulement l'affaire du CISO ou du CIO : c'est une responsabilité partagée à l'échelle de l'entreprise. »

1. Données biométriques : un risque pas toujours là où on l'attend

Les données biométriques (empreintes, reconnaissance faciale, voix, iris) sont souvent perçues comme *les plus sensibles* des renseignements personnels. Pourtant, toutes ne présentent pas le même risque. Selon Guillaume Clément, le danger augmente surtout lorsque ces données sont centralisées et liées à d'autres identifiants personnels, comme des noms ou des identifiants d'appareils.

« Une donnée biométrique isolée est difficilement exploitable. C'est la combinaison avec d'autres bases de données qui crée le risque. »

Lorsqu'elles sont stockées séparément et sous la forme d'un gabarit biométrique, ces données deviennent beaucoup plus difficiles à réutiliser. Même dans les rares cas de vol de bases biométriques, la réutilisation pratique reste techniquement complexe. En vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé* **(** LPRPSP) et de la *Loi concernant le cadre juridique des technologies de l'information,* récemment modifiées par la loi 25, les organisations sont néanmoins assujetties à une série d'obligations accrue en lien avec la collecte de renseignements biométrique. Elles doivent en justifier la nécessité, renforcer leurs mécanismes de consentement et effectuer une déclaration à la Commission d'accès à l'information du Québec.

2. Assurance cyber : partenaire stratégique ou nouveau risque ?

Les compagnies d'assurance jouent désormais un rôle essentiel et de plus en plus structurant dans la gestion des incidents de cybersécurité. Plusieurs ont mis en place des équipes spécialisées capables d'appuyer les assurés lors des enquêtes techniques ou des échanges avec les cybercriminels.

Selon Guillaume, il s'agit d'une évolution naturelle du marché, qui témoigne d'une professionnalisation croissante du secteur. Il souligne toutefois que la coordination entre les différents intervenants (assureur, entreprise et experts techniques) peut parfois soulever des enjeux de gouvernance, de confidentialité et d'alignement stratégique, qu'il convient de gérer avec attention.

Autre tendance : la restriction des conditions de couverture. Les assureurs refusent de plus en plus de réclamations lorsque les entreprises n'ont pas mis en place les mesures de sécurité minimales exigées. Afin de gérer ce risque, les entreprises devraient:

- Relire attentivement les clauses techniques de leurs polices d'assurance;
- Documenter leurs pratiques de conformité et mesures de sécurité en place
- Et surtout, préserver la maîtrise de leur plan de réponse aux incidents

3. Informatique quantique : menace future, risque présent

L'informatique quantique n'est pas encore une menace immédiate, mais elle pourrait à terme bouleverser les fondements actuels de la cryptographie et rendre obsolètes plusieurs standards utilisés pour protéger les données sensibles.

Selon Guillaume, le principal enjeu actuel réside dans la stratégie dite *store now, decrypt later* :

« Certains acteurs — notamment étatiques — stockent déjà des volumes massifs de données chiffrées, dans l'attente de pouvoir les décrypter grâce à la puissance quantique. »

Pour se préparer sans tomber dans l'alarmisme, les organisations peuvent dès aujourd'hui

identifier où leurs mécanismes de chiffrement sont utilisés, cartographier les données et communications sensibles, et intégrer le risque quantique dans leurs feuilles de route technologiques et de sécurité. Une approche progressive, basée sur la crypto-agilité et le suivi des travaux de normalisation (par exemple ceux du NIST), permet déjà de réduire le risque de “harvest now, decrypt later” sans sur-investir ni perturber les opérations.

4. Fraudes à l’IA : l’ère de l’hypertrucage et de la désinformation ciblée

La montée de l’IA générative a transformé la fraude numérique. Les hypertrucages (*deepfakes*) visuels et vocaux et les campagnes d’hameçonnage multicanal deviennent plus crédibles, plus rapides et plus difficiles à détecter.

« L’IA donne aux fraudeurs une arme de persuasion massive. Elle exploite la confiance et l’urgence, deux leviers humains universels. »

Guillaume cite un exemple frappant : un cadre supérieur a reçu un ensemble coordonné de courriels, textos et appels vocaux imitant parfaitement un supérieur hiérarchique. L’attaque, entièrement générée par IA, semblait authentique jusque dans les moindres détails.

Pour contrer ces menaces

- certaines entreprises testent l’authentification « à triple facteur «, combinant validation technique, comportementale et humaine;
- la segmentation des accès et les protocoles de double vérification deviennent des standards essentiels
- et la formation des employés doit désormais inclure la reconnaissance des contenus synthétiques

Malgré les outils, l’erreur humaine reste la première cause d’incident. La formation demeure la première ligne de défense, mais elle doit être accompagnée de mécanismes automatiques de détection et de vérification.

5. Sécurité organisationnelle : repenser les défenses humaines

Les lois sur la protection des renseignements personnels imposent aux organisations des mesures physiques, techniques et organisationnelles adéquates pour protéger les renseignements personnels.

Dans la pratique, cette exigence est technologiquement neutre, mais de plus en plus précisée par les autorités. Les décisions réglementaires récentes définissent plus clairement ce qu’on entend par « sécurité adéquate ».

Or, Guillaume constate que sur le terrain :

- la majorité des incidents proviennent de vulnérabilités logicielles non corrigées, d’accès distants mal sécurisés, d’hameçonnage, de pièces jointes malveillantes, d’erreurs de configuration ou humaines
- les outils de sécurité sont souvent mal configurés ou sous-utilisés ;
- et les incidents détectés augmentent, pas forcément parce qu’ils sont plus nombreux, mais parce que nous avons plus de visibilité et de capacité de détection.

« Les cyberattaques exploitent des failles techniques et humaines nécessitant une cybersécurité multicouche : mises à jour, authentification forte, formation, vigilance et bonne

gouvernance. »

Les bonnes pratiques recommandées incluent notamment de former en continu les employés, avec des scénarios concrets, mesurer la résilience humaine par des tests de simulation et intégrer la cybersécurité dans les décisions de gestion dès la conception des projets.

6. Gouvernance et leadership : la cybersécurité comme enjeu d'affaires

Pour Guillaume, la cybersécurité dépasse le cadre technique : c'est aussi un enjeu stratégique de gouvernance et de stratégie. « Les PDG et conseils d'administration doivent maîtriser les risques numériques pour poser les bonnes questions et guider les décisions. »

Or, malgré son classement parmi les trois principaux risques des organisations, la cybersécurité reste sous-financée et mal priorisée. Les CISO et CIO, souvent surchargés, peinent à obtenir les moyens nécessaires.

L'écart persiste entre la perception du risque et l'action concrète. La solution ? Un leadership engagé, soutenu par une culture de cybersécurité intégrée à tous les niveaux.

Conclusion : bâtir la confiance numérique

Les échanges avec Guillaume confirment que juridique, technologique et stratégique forment un tout indissociable. Dans un Canada où réglementations, technologies et menaces s'accélèrent, la réponse tient en trois mots : préparation, coordination, gouvernance.

Les leaders doivent anticiper et transformer la cybersécurité en levier de confiance et de performance.

 Citation à retenir

« La cybersécurité n'est pas un coût, c'est un investissement essentiel pour préserver et renforcer la confiance de toutes les parties prenantes. »
— *Guillaume Clément*

À propos de l'événement

La 2e Conférence annuelle sur la protection de la vie privée d'Osler s'est tenue le 21 octobre 2025 à Montréal. Organisée par l'équipe Respect de la vie privée et gestion de l'information, cette demi-journée a rassemblé des professionnels du droit, des technologies et de la gouvernance pour échanger sur les enjeux stratégiques de la protection des renseignements personnels au Canada.

Pour toute question sur la conformité aux lois en matière de protection de renseignements personnels, la gestion des incidents de cybersécurité ou la gouvernance des données, notre équipe se tient à votre disposition.