Bilan 2024 et perspectives 2025 : développements majeurs en matière de cybersécurité et de protection des renseignements personnels

28 janvier 2025

A l'occasion de la Journée internationale de la protection des données, BLG vous propose un retour sur les développements significatifs de l'année 2024 dans les domaines de la cybersécurité et de la protection des renseignements personnels au Canada.

Nous avons rassemblé nos bulletins les plus marquants de 2024 afin de vous offrir une synthèse des évolutions récentes, incluant les changements législatifs, les tendances émergentes et les meilleures pratiques. En complément, cette publication offrira un aperçu des priorités stratégiques et enjeux que les entreprises devront garder à l'esprit en ce début d'année 2025.

Rétrospective de l 'année 2024

Intelligence artificielle (IA)

Utilisation de l 'IA par les organismes publics

L'année 2024 a marqué une étape clé dans la réglementation mondiale de l'IA, notamment avec l'entrée en vigueur du Règlement sur l'intelligence artificielle de l'Union européenne, qui établit une référence internationale en la matière.

Bien que le Québec ne dispose pas encore d'un cadre juridique spécifique à l'IA, il s'inscrit dans cette dynamique globale grâce à des initiatives alignées sur les normes internationales. Parmi celles-ci, le ministère de la Cybersécurité et du Numérique (MCN) a publié un Énoncé de principes pour encadrer l'utilisation responsable de l'IA par les organismes publics qui identifie dix axes fondamentaux pour l'utilisation de l'IA, notamment le respect des droits, la transparence, la fiabilité et la durabilité. En parallèle, le MCN a introduit un Guide des bonnes pratiques pour l'utilisation de l'IA générative, offrant des recommandations pratiques sur la protection des renseignements personnels, la neutralité, l'efficacité, la diligence et la sensibilisation. Ces deux documents constituent des outils essentiels pour les organismes publics, en leur fournissant un cadre clair et opérationnel pour intégrer l'IA de manière responsable, sécurisée et conforme aux attentes légales et éthiques.

Pour en savoir plus : Utilisation responsable de l'IA par les organismes publics | BLG

Meilleures pratiques en matière d'IA pour les participants aux marchés des capitaux

Le droit encadrant l'IA est marqué par son caractère fragmenté et son évolution rapide, reflétant la diversité des secteurs qu'il impacte. Face aux attentes réglementaires toujours plus précises, l'Autorité des marchés financiers (AMF) et la Commission des valeurs mobilières de l'Ontario (CVMO) ont publié des lignes directrices pour orienter les gestionnaires d'actifs canadiens vers les meilleures pratiques à adopter pour mitiger les risques opérationnels et éthiques liés à l'IA.

Ces lignes directrices traitent de la validation et de la surveillance des systèmes d'IA pour assurer leur fiabilité, une gouvernance solide des données pour minimiser les biais et garantir leur intégrité, ainsi que la mise en place de processus d'audit et de responsabilité. En assurant la transparence des décisions automatisées et en respectant les standards éthiques, les entreprises œuvrant dans le secteur financier peuvent renforcer la confiance des parties prenantes et s'aligner sur les exigences croissantes des régulateurs en matière de gouvernance et de conformité.

En outre, les Autorités canadiennes en valeurs mobilières ont publié en décembre 2024 l'Avis 11-348 du personnel des ACVM et de consultation, Applicabilité du droit canadien des valeurs mobilières à l'utilisation des systèmes d'intelligence artificielle dans les marchés des capitaux, afin de donner des éclaircissements et des indications sur la façon dont la législation en valeurs mobilières s'applique à l'utilisation des systèmes d'IA par les participants aux marchés des capitaux.

Pour en savoir plus : Meilleures pratiques en matière d'IA pour les gestionnaires d'actifs canadiens | BLG

Loi 5 et protection des renseignements de santé au Québec

La Loi sur les renseignements de santé et des services sociaux (Loi 5), entrée en vigueur le 1er juillet 2024, instaure un nouveau cadre juridique pour la gestion des renseignements de santé au Québec. Elle s'applique aux organismes de santé, y compris les cliniques privées, et encadre le traitement des renseignements de santé et de services sociaux, incluant les renseignements permettant d'identifier une personne en lien avec son état de santé ou les services de santé reçus.

La Loi 5 impose aux organismes de santé des obligations strictes en matière de gouvernance, exigeant l'adoption de politiques détaillées qui couvrent les mesures de sécurité, le contrôle des accès et le traitement des incidents de confidentialité. Elle introduit également une obligation de protection de la vie privée par défaut pour les produits et services technologiques utilisés et exige une évaluation des facteurs relatifs à la vie privée (EFVP) avant tout projet technologique impliquant des renseignements de santé. Bien qu'elle ne prévoie pas de sanctions administratives pécuniaires, la Loi 5 introduit des sanctions pénales pouvant atteindre 150 000 $.

Pour en savoir plus : Loi 5 et protection des renseignements de santé au Québec | BLG

Nouveau pouvoir d 'imposition de sanctions administratives pécuniaires en vertu de la Loi de 2004 de l'Ontario

Depuis le 1er janvier 2024, le Commissaire à l'information et à la protection de la vie privée de l'Ontario (Commissaire) est habilité à imposer des sanctions administratives pécuniaires pour les infractions à la Loi de 2004 sur la protection des renseignements personnels sur la santé.

Ce pouvoir représente un levier supplémentaire pour renforcer la conformité dans le secteur de la santé. Les sanctions peuvent atteindre 50 000 $ pour une personne physique et 500 000 $ pour une organisation ; elles visent à dissuader des infractions graves telles que l'accès non autorisé aux dossiers médicaux, l'exploitation des renseignements personnels à des fins lucratives ou la négligence persistante des droits des patients. Dans les cas de violations particulièrement graves ou de profits illicites générés par la commission d'une infraction, le Commissaire peut demander des ajustements dépassant les plafonds réglementaires ou transmettre le dossier au Procureur général.

Ces nouvelles mesures soulignent la nécessité pour les organisations de revoir leurs politiques et leurs pratiques en matière de confidentialité afin de limiter les risques juridiques et financiers. Afin de favoriser la conformité et d'encourager des pratiques robustes et éthiques en matière de protection des

renseignements personnels, le Commissaire a également publié des lignes directrices qui précisent les modalités d'application de ces sanctions, soulignant leur rôle non seulement punitif, mais aussi éducatif.

Pour en savoir plus : PHIPA administrative monetary penalties | BLG

Règlement sur l 'anonymisation des renseignements personnels

Le 30 mai 2024, le Québec est devenu la première juridiction canadienne à adopter une réglementation spécifique sur l'anonymisation des renseignements personnels.

Le Règlement sur l'anonymisation des renseignements personnels, établit un cadre normatif précis offrant aux entreprises et organismes publics une marche à suivre pour procéder à l'anonymisation. Le Règlement vise à garantir que les données anonymisées ne permettent plus, de façon irréversible, d'identifier une personne. Le Règlement exige que l'anonymisation soit effectuée sous la supervision d'experts qualifiés et impose des analyses approfondies des risques de réidentification tout au long du processus, notamment en considérant les critères d'individualisation, de corrélation et d'inférence. Les organisations doivent également adopter des techniques d'anonymisation conformes aux meilleures pratiques reconnues, telles que la randomisation et la généralisation. Enfin, depuis le 1er janvier 2025, un registre détaillant les processus d'anonymisation, les techniques utilisées et les analyses de risques est requis.

Pour en savoir plus : Règlement sur l'anonymisation des renseignements personnels | BLG

La Loi 25 introduit le droit à la portabilité des données

Le droit à la portabilité, dernier volet de la Loi 25 est entré en vigueur au Québec le 22 septembre 2024. Ultime jalon d'une vaste réforme législative, ce droit permet aux individus de récupérer et de transférer leurs renseignements personnels informatisés dans un format technologique structuré et couramment utilisé.

Inspiré par le Règlement général sur la protection des données, le droit à la portabilité vise à renforcer le contrôle des citoyens sur leurs données. Les entreprises doivent être en prêtes à identifier les renseignements concernés, garantir leur transmission sécurisée et s'assurer de leur conformité avec les critères techniques, comme l'utilisation de formats interopérables tels que CSV, XML ou JSON.

Le droit à la portabilité est considéré comme une extension au droit d'accès. Ainsi, et bien que des distinctions existent, les entreprises devraient traiter les demandes de portabilité conformément au régime applicable aux demandes d'accès. Le gouvernement du Québec a publié un tableau explicatif pour

illustrer la distinction entre le droit d'accès aux renseignements personnels et le droit à la portabilité.

Pour en savoir plus : La Loi 25 introduit le droit à la portabilité des données | BLG

Adoption du projet de loi 194 en Ontario

La Loi de 2024 visant à renforcer la cybersécurité et la confiance dans le *secteur public* (PL 194), adoptée le 25 novembre 2024, marque une avancée majeure en matière de cybersécurité, d'intelligence artificielle et de protection des données en Ontario. Le PL 194 vise à moderniser le cadre législatif de la province en alignant ses exigences sur les normes canadiennes et internationales. Il prévoit des mesures concrètes pour renforcer la protection des renseignements personnels, y compris des obligations accrues en matière d'EFVP et de signalement des violations, tout en dotant le Commissaire à l'information et à la protection de la vie privée de pouvoirs élargis, permettant une surveillance proactive et la mise en œuvre de mécanismes pour mieux encadrer l'utilisation des technologies émergentes.

Pour en savoir plus : Bill 194 - The new Enhancing Digital Security and Trust Act, 2024 | BLG

Ratissage et attentes du Commissariat à la protection de la vie privée (CPVP) sur le consentement en ligne

Le 9 juillet 2024, le CPVP a publié son rapport sur le ratissage, mettant en lumière les résultats d'une enquête approfondie sur les mécanismes de conception trompeuse (aussi appelées « interfaces truquées ») utilisés par certains sites Web et applications pour influencer les décisions des utilisateurs concernant leurs renseignements personnels.

En complément, le CPVP a également publié un guide pratique destiné à aider les entreprises à éviter ces mécanismes et à éclairer les particuliers sur ces pratiques. Le rapport et le guide font état des attentes du CPVP à l'égard des organisations en matière de consentement éclairé en ligne.

Bien qu'ils présentent des pratiques optimales plutôt que des règles exécutoires, ces documents préparent le terrain à de potentielles mesures coercitives, puis incluent des exemples visuels concrets de ce qui est jugé acceptable ou non par le CPVP. Au regard de ces publications, les entreprises canadiennes devraient examiner leurs plateformes Web et y apporter les ajustements nécessaires, afin de se conformer dès maintenant aux attentes du CPVP sans attendre le dépôt d'une plainte ou le lancement d'une enquête formelle.

Pour en savoir plus : Ratissage et attentes du CPVP sur le consentement en ligne | BLG

Politique de confidentialité de Facebook et consentement valable

Dans la décision *Canada Privacy Commissioner v Facebook Inc.*, rendue le 9 septembre 2024, la Cour d'appel fédérale a jugé que Facebook avait enfreint les exigences de la *Loi sur la protection des renseignements personnels et les* documents électroniques (LPRPDE) en matière de consentement et de mesures de sécurité, précisant ainsi la portée de ces obligations.

La Cour a jugé que les politiques de confidentialité de Facebook, trop longues et complexes, ne répondaient pas aux exigences de transparence nécessaire pour un consentement valable. Qui plus est, la décision soulève la question quant à l'obligation pour les organisations de prendre des mesures raisonnables pour s'assurer que les tiers qui collectent des renseignements personnels en leur nom respectent leurs engagements en matière de confidentialité. Dans le cas de Facebook, le défaut de surveillance des applications tierces a été considéré comme une violation de l'obligation de protéger adéquatement les renseignements personnels.

Dans l'ensemble, la décision Facebook souligne l'importance d'une approche proactive et transparente de la protection des renseignements personnels, qui place le droit à la vie privée des individus au cœur des pratiques organisationnelles.

Le 8 novembre 2024, Facebook a demandé l'autorisation d'interjeter appel devant la Cour suprême du Canada au motif que l'appel proposé soulève deux questions d'importance publique concernant la LPRPDE, en particulier la longueur de la politique de confidentialité et le consentement valable, ainsi que l'obligation de surveiller le respect de mesures de sécurité raisonnables par les fournisseurs de service tiers. On peut s'attendre à une décision sur la demande d'autorisation d'interjeter appel en mai 2025.

Pour en savoir plus : Facebook privacy policy and breach of meaningful consent | BLG (disponible en anglais seulement)

LifeLabs LP v. Information and Privacy Commissioner (Ontario)

Dans un contexte où les incidents de confidentialité se multiplient, les organisations se trouvent confrontées à des questions cruciales sur la gestion de leurs enquêtes internes.

L'affaire LifeLabs c. Commissaire à l'information et à la protection de la vie privée de l'Ontario met en lumière les limites du privilège lié aux enquêtes menées après une atteinte à la protection des données. La Cour a confirmé que le privilège ne s'étend pas aux faits sous-jacents qui doivent être divulgués en vertu d'une obligation légale, même s'ils sont intégrés dans des documents protégés. Par exemple, le rapport d'enquête préparé par une firme de cybersécurité externe pour LifeLabs, bien qu'initié par les avocats de

l'entreprise, n'a pas été jugé privilégié, car il avait été produit principalement à des fins commerciales et non pour un litige imminent. De même, les communications sensibles, y compris les négociations de rançons entre LifeLabs et les présumés cybercriminels, n'ont pas pu bénéficier d'une protection juridique.

Cette décision rappelle que les faits sous-jacents ne constituent pas des renseignements privilégiés soumis au privilège lorsqu'ils existent indépendamment. En outre, elle souligne également l'importance pour les organisations de faire appel à des conseillers juridiques externes et de documenter clairement les objectifs de leurs enquêtes en matière de cybersécurité pour protéger efficacement leur privilège juridique tout en répondant aux obligations réglementaires.

Pour en savoir plus : LifeLabs LP v. Information and Privacy Commr. (Ontario), 2024 ONSC 2194 | BLG

Nouveau règlement sur les incidents de sécurité pour certaines institutions financières

Le Règlement sur la gestion et le signalement des incidents de sécurité de l'information de certaines institutions financières et des agents d'évaluation du crédit, qui entrera en vigueur le 23 avril 2025, impose des exigences strictes aux institutions financières et aux agents d'évaluation du crédit afin de garantir une gestion proactive et efficace des incidents de confidentialité.

Le Règlement contraint les organisations à élaborer une politique complète de gestion des incidents, à désigner un responsable pour superviser leur gestion, à signaler tout incident à l'AMF dans un délai de 24 heures après notification aux dirigeants, et à tenir un registre détaillé des incidents pour une période minimale de cinq ans. Par ailleurs, les sanctions pour non-conformité incluent des amendes pouvant atteindre 500 $ pour les personnes physiques et 2 500 $ pour les personnes morales.

Ce Règlement vise à garantir des pratiques exemplaires de gestion et de signalement des incidents, permettant aux organisations visées de mieux les anticiper et les gérer, minimisant ainsi les impacts potentiels sur leur réputation, leur solvabilité et la confiance de leurs clients.

Pour en savoir plus, demeurez à l'affût : BLG devrait publier une analyse du nouveau Règlement environ un mois avant son entrée en vigueur.

Encadrement de l 'IA et projet de loi C-27

Le 6 janvier 2025, le Parlement a été prorogé jusqu'au 24 mars 2025, par une proclamation du gouverneur général sur l'avis du premier ministre, mettant ainsi fin à la session parlementaire et à tous les travaux parlementaires. Trois projets de loi inscrits au Feuilleton étaient censés transformer de manière

significative l'environnement réglementaire au Canada après leur adoption, dont le projet de loi C-27, le projet de loi C-26 et le projet de loi C-63.

Le projet de loi C-27 aurait remplacé la LPRPDE, vieille de 25 ans, par la *Loi* sur la protection de la vie privée des consommateurs (LPVPC) et édicté la *Loi* sur l'intelligence artificielle et les données (LIAD), qui aurait établi un encadrement réglementaire pour les systèmes d'intelligence artificielle utilisés dans le cadre d'activités commerciales au Canada.

Après la prorogation, il est peu probable que le projet de loi C-27 renaisse de ses cendres en raison de la controverse entourant la LIAD, et ce, même s'il existe un vaste consensus sur la nécessité d'une réforme du régime fédéral de protection des renseignements personnels dans le secteur privé.

Loi sur l'IA au Québec ?

Le 5 février 2024, le Conseil de l'innovation du Québec a déposé le rapport Prêt pour l'IA : Répondre au défi du développement et du déploiement responsables de l'IA au Québec. Ce rapport recommande, entre autres, que le Québec adopte une loi-cadre spécifiquement dédiée à encadrer le développement et le déploiement de l'IA, s'inspirant des principes de la Déclaration de Montréal.

À l'instar de l'approche préconisée par le fédéral et l'Union européenne, cette législation serait basée sur la sévérité des risques associés aux systèmes d'IA. Cette loi viserait à établir des normes pour l'utilisation des systèmes d'IA tant dans le secteur privé que dans le secteur public. Elle serait gérée par une autorité indépendante, qui aurait également le rôle de conseiller et d'élaborer des règlements pour sa mise en œuvre.

Pour en savoir plus : Prêt pour l'IA : Le Conseil de l'innovation du Québec propose l'adoption d'une loi sur l'IA | BLG

Orientation sur la biométrie

La CAI et le CPVP ont tous deux publié des lignes directrices sur la biométrie en 2023 : les lignes directrices sur les horodateurs et pointeuses biométriques de la CAI et le « Document d'orientation provisoire à l'intention des organisations sur le traitement des données biométriques » du CPVP (ouvert à des fins de consultation jusqu'au 16 février 2024). Les organismes de réglementation ont recommandé de minimiser la collecte de données biométriques à des fins de commodité et ont souligné que ces renseignements sensibles devraient être recueillis uniquement en cas de besoin urgent, réel, important et/ou légitime de le faire.

Dans la même veine, la CAI a récemment rendu une décision concernant la nécessité d'utiliser un système de reconnaissance faciale par une entreprise. Cette décision démontre, une fois de plus, les attentes très élevées de la CAI lorsqu'il est question de mettre en place un système biométrique dans un milieu de travail.

Nouvelles de la CAI

L'Assemblée nationale du Québec a procédé à la nomination de Me Lise Girard à titre de présidente de la CAI. Son entrée en fonction était le 8 novembre 2024. Auparavant, Me Girard était sous-ministre adjointe à la sécurité de l'information gouvernementale et à la cybersécurité au ministère de la Cybersécurité et du Numérique ainsi que chef gouvernemental de la sécurité de l'information.

Par ailleurs, après une année consacrée à la publication de lignes directrices sur la Loi 25, nous pouvons désormais nous attendre à ce que la CAI soit plus proactive dans l'application de la loi et dans l'imposition de sanctions administratives pécuniaires.

Actions collectives en matière de protection de la vie privée

Le 4 juillet 2024, la Cour d'appel de la Colombie-Britannique a rendu deux jugements d'appel en matière d'actions collectives dans des contextes de fuite de données. Ce faisant, la Cour d'appel a clarifié la portée potentielle des recours fondés sur le droit à la vie privée à l'encontre des consignataires de données qui subissent des cyberattaques, et ce, que ces recours soient prévus par la loi ou en vertu de la common law.

Dans chacune des affaires *G.D. v. South Coast British Columbia Transportation Authority* (l'affaire G.D.) et *Campbell v. Capital One Financial Corporation* (l'affaire Campbell), la Cour d'appel a confirmé la possibilité de faire valoir diverses causes d'action à l'encontre de consignataires de données qui n'ont pas commis d'acte répréhensible intentionnel, y compris le délit civil d'atteinte à la vie privée en vertu de la *Privacy Act* de la Colombie-Britannique. Les parties dans l'affaire G.D. ont demandé l'autorisation d'interjeter appel devant la Cour suprême du Canada et une décision à cet effet est encore attendue.

De plus, la Cour suprême de la Colombie-Britannique a accordé la demande de certification de l'action collective contre Home Depot Canada alléguant la violation des lois provinciales sur la protection des renseignements personnels lors de la collecte et du partage des renseignements personnels des clients après l'envoi par courriel des reçus d'achat. Par ailleurs, la Cour a rejeté les allégations selon lesquelles Home Depot aurait violé d'autres devoirs et obligations contractuelles.

Rapport de l'enquête du CPVP sur OpenAI

En 2023, le CPVP ainsi que les autorités provinciales de protection de la vie privée de la Colombie-Britannique, de l'Alberta et du Québec ont lancé une enquête sur OpenAI à la suite d'une plainte selon laquelle des renseignements personnels ont été recueillis, utilisés et communiqués sans consentement. Le CPVP n'a pas encore fourni de détails sur les conclusions

de l’enquête, mais il est probable que le rapport d’enquête soit rendu public en 2025.

Par

Cléa Jullien, Hélène Deschamps Marquis, Frédéric Wilson, Daniel J. Michaluk, Eric S. Charleston, Cassandre Legault

Services

Cybersécurité, respect de la vie privée et protection des renseignements personnels, Intelligence artificielle (IA)

BLG | Vos avocats au Canada

Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG) est le plus grand cabinet d’avocats canadien véritablement multiservices. À ce titre, il offre des conseils juridiques pratiques à des clients d’ici et d’ailleurs dans plus de domaines et de secteurs que tout autre cabinet canadien. Comptant plus de 725 avocats, agents de propriété intellectuelle et autres professionnels, BLG répond aux besoins juridiques d’entreprises et d’institutions au pays comme à l’étranger pour ce qui touche les fusions et acquisitions, les marchés financiers, les différends et le financement ou encore l’enregistrement de brevets et de marques de commerce.

blg.com

Bureaux BLG

Calgary

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

T 403.232.9500
F 403.266.1395

Ottawa

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

T 613.237.5160
F 613.230.8842

Vancouver

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

T 604.687.5744
F 604.687.1415

Montréal

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

T 514.954.2555
F 514.879.9015

Toronto

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

T 416.367.6000
F 416.367.6749