POINTS DE VUE D'AUDIT INTERNE

PROTECTION DES RENSEIGNEMENTS PERSONNELS

IAI Canada Montréal

Introduction

Avec la collecte et le traitement des renseignements personnels qui se multiplient à un rythme sans précédent, la protection de la vie privée est devenue une préoccupation majeure pour les individus et les organisations. Les auditeurs internes jouent un rôle essentiel en s'assurant que leurs organisations respectent les lois et les réglementations en matière de protection des renseignements personnels, et maintiennent la confiance numérique de leurs parties prenantes.

Nous avons interviewé Florian Strich, co-président du chapitre Montréal Knowledge Network de l'IAPP pour discuter de ces enjeux et des meilleures pratiques en matière de gestion de la vie privée dans les organisations.

BIOGRAPHIE

Biographie

Florian a démarré sa carrière il y a 10 ans comme juriste spécialisé en droit de l'internet après des études à la Sorbonne. Il travaille sur des enjeux de vie privée notamment le droit à l'oubli et le cyberharcèlement, dans des cabinets d'avocats spécialisés, avant de retourner aux études pour se former en informatique et commerce (ESSEC/ Telecom Paris). Cofondateur de la chaire en gouvernance de l'information à l'ESSEC, il se tourne ensuite vers le conseil, aidant depuis huit ans des entreprises à conjuguer protection de la vie privée et gouvernance des données. Rejoignant PwC il y a cinq ans, il s'installe au Québec deux ans plus tard pour développer la pratique francophone en vie privée.

Entrevue

01 Qu'entend-on exactement par protection des renseignements personnels et quel est le lien avec la confiance numérique?

La protection des renseignements personnels vise à préserver la confidentialité et la sécurité des renseignements personnels des individus. À l'ère numérique, chaque action que nous effectuons en ligne laisse un sillage de renseignements personnels, que ce soit en utilisant une carte de crédit ou un GPS ou en interagissant sur les réseaux sociaux. Ces données sont précieuses pour les entreprises, qui s'engagent dans ce que la chercheuse Shoshana Zubov appelle le «capitalisme de surveillance»[1], et pour les gouvernements qui peuvent surveiller certaines personnes pour des raisons de sécurité intérieure.

La définition des renseignements personnels est très large, englobant tout renseignement qui identifie directement ou indirectement une personne. Certains de ces renseignements sont considérés comme sensibles en raison de leur nature ou du contexte dans lequel elles sont utilisées. Par exemple, les informations financières, l'orientation sexuelle, l'appartenance politique, la santé, etc. La gestion de ces données nécessite généralement le consentement exprès des personnes concernées pour garantir transparence accrue.

La protection de la vie privée vise à redonner aux citoyens le contrôle sur leurs renseignements personnels. Cela comprend le droit d'être informé sur l'utilisation de leurs données, de consentir librement à cette utilisation et de s'assurer que les données sont utilisées conformément aux annonces faites.

Finalement, la confiance numérique est étroitement liée à la protection des renseignements personnels. Elle représente la confiance que les individus accordent aux entreprises quant à leur capacité et leur volonté de respecter leur consentement et de protéger leurs renseignements personnels. Lorsqu'une entreprise ou une organisation est transparente dans ses pratiques de collecte et d'utilisation des données, respecte les droits des individus et met en place des mesures de sécurité adéquates, elle contribue à renforcer la confiance numérique.

[1]Shoshana Zuboff, L'Âge du capitalisme de surveillance, éd. ZULMA, 2020

02 Comment évolue la réglementation en matière de protection des renseignements personnels?

Au Canada, la protection des renseignements personnels dans le secteur privé est principalement régie par la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). Cependant, il y a eu des développements récents visant à moderniser et à renforcer la réglementation en matière de protection des renseignements personnels.

Le projet de loi C-27, également connu sous le nom de Loi sur la protection de la vie privée des consommateurs (LPVC), vise à renforcer le contrôle des individus sur leurs renseignements personnels, à exiger davantage de transparence de la part des entreprises et à introduire des sanctions plus sévères pour les violations de la vie privée. Le projet de loi a été introduit en novembre 2020 et est en cours d'examen.

Au niveau du secteur public fédéral, la loi de 1985 sur la protection des renseignements personnels s'applique et le gouvernement est en train de mener des consultations pour éventuellement la réformer.

Au Québec, la législation pour les secteurs privés et publics a été réformée par le projet de loi 64, adopté en septembre 2021 et devenue loi 25. Cette loi a positionné le Québec comme étant un leader en matière de protection des renseignements personnels, en établissant des normes rigoureuses comparables à celles du Règlement général sur la protection des données (RGPD) de l'Union européenne. Elle renforce les pouvoirs de contrôle de la Commission d'accès à l'information (CAI) et introduit des sanctions financières dissuasives.

03 Pourquoi la gestion des renseignements personnels est-elle essentielle pour une entreprise ou une organisation aujourd'hui?

La confiance dans les données qui englobe la protection de la vie privée, la sécurité et la gouvernance des données, est devenue un enjeu stratégique majeur pour les organisations, bien au-delà des obligations réglementaires. Si des lois comme le RGPD ou la Loi 25 encouragent la conformité grâce à des sanctions significatives (ex. 5 % du chiffre d'affaires ou 20 M$), leur véritable importance réside dans leur rôle de catalyseurs pour la résilience organisationnelle et la gestion des risques, notamment face aux rançongiciels ou aux crises géopolitiques.

Dans un contexte où les fuites de données sont inéluctables, l'enjeu est d'assurer la continuité des activités tout en évitant des violations pouvant entraîner des conséquences graves, tant pour les entreprises que pour les individus. Par ailleurs, l'émergence de l'IA générative illustre à quel point des données fiables et bien gouvernées sont essentielles. Sans elles, les technologies innovantes peuvent produire des résultats erronés, comme l'a démontré un récent cas canadien où un chatbot a halluciné un rabais qu'une entreprise a dû honorer.

Enfin, les données, et en particulier les renseignements personnels, sont désormais au cœur de la plupart des modèles d'affaires. Une information fiable est indispensable pour innover, comprendre les besoins des clients et s'adapter aux marchés. En ce sens, un programme de protection des renseignements personnels bien conçu peut devenir un levier pour instaurer une gouvernance et une protection des données robuste. Je pense à un de mes clients qui a su créer un programme intégré de confiance numérique et qui a ainsi réalisé des économies d'échelle significatives en alignant ses équipes, ses processus et ses technologies. Investir dans des données de confiance, c'est donc payant.

04 Comment se déroule la mise en place d'un programme de protection des renseignements personnels et est-ce que l'audit interne a un rôle à jouer ?

La mise en conformité ou la création d'un programme de protection des renseignements personnels est un processus complexe. Il y a deux grandes étapes : la définition d'une structure de gouvernance et la mise en place des programmes visant à informer les utilisateurs de manière transparente, à respecter leur consentement et leurs autres droits, tels que le droit d'accès, et à gérer le cycle de vie des données de manière responsable. Tout cela contribue à établir la confiance numérique.

Pour ce qui est de la définition d'une structure de gouvernance, la première étape consiste à nommer un responsable de la protection des renseignements personnels, agissant sous la délégation du dirigeant de l'entreprise qui est personnellement responsable devant la loi. Ensuite, des comités multidisciplinaires sont formés, regroupant les responsables des opérations, des technologies de l'information, de la cybersécurité, de la gouvernance des données et de la gestion des risques. Ces comités travaillent ensemble pour définir la politique de vie privée de l'entreprise, en traduisant les exigences légales en requis d'entreprise.

L'enjeu central de gouvernance en matière de protection des renseignements personnels réside dans la mise en place d'une première ligne de défense robuste. Cela implique que les ressources opérationnelles manipulant quotidiennement des renseignements personnels (Ligne 1A) aient une compréhension claire des exigences et des pratiques à adopter. Il est tout aussi essentiel que leurs superviseurs (Ligne 1B) partagent cette compréhension et jouent un rôle actif dans la supervision et la sensibilisation.

Avec une première ligne bien formée et engagée, le bureau de la vie privée (Ligne 2) peut se concentrer sur ses fonctions de coordination, de contrôle et de pilotage, tout en déléguant certains contrôles à d'autres fonctions clés comme le contrôle interne ou la gestion des risques.

La fonction d'audit interne (Ligne 3) possède le savoir-faire et occupe une position privilégiée pour réaliser des revues de gouvernance. Elle est en mesure de poser des questions clés telles que : les rôles et responsabilités sont-ils clairement définis? Les comités disposent-ils de chartes adéquates? Les personnes ayant un rôle de supervision, ont-elles accès aux bonnes informations en temps opportun pour prendre les bonnes décisions ? La stratégie mise en place est-elle en adéquation avec les objectifs fixés par la structure de gouvernance? Les risques ont-ils été identifiés, rapportés et le processus de surveillance est-il suffisamment solide pour s'assurer que les mesures d'atténuation des risques sont mises en œuvre? etc.

05 Une fois la structure de gouvernance établie, comment est établie la gestion du cycle de vie des données? Quel rôle peut jouer l'audit interne dans cette gestion du cycle de vie des données?

Le processus de mise en conformité se poursuit par un état des lieux, qui peut être réalisé par l'audit interne ou d'autres acteurs, pour évaluer la conformité aux exigences légales. Cela permet d'identifier les écarts et de concevoir un programme de remédiation.

L'entreprise doit ensuite comprendre comment elle utilise les renseignements personnels (« traitements »), et son niveau de conformité. Pour ce faire, elle réalise une cartographie de ses traitements (appelée aussi « inventaire » ou « registre »). Cette cartographie peut être obtenue par des entretiens et des analyses techniques, afin de retracer le cycle de vie des données au travers des différentes couches de l'architecture (processus, applications, infrastructures). Une fois l'inventaire établi et les écarts identifiés, l'entreprise peut fonder ses décisions de priorisation sur des données fiables et suivre son avancement de manière précise.

Les processus clés, tels que la gestion du consentement, les droits des personnes ou la vie privée dès la conception, sont ensuite définis et mis en œuvre. Pour les industrialiser, de nombreuses entreprises adoptent des outils spécialisés (Privacy Enhancing Technologies), qui automatisent certaines tâches et facilitent la documentation et le partage d'informations. Une attention particulière est portée à la sensibilisation et à la formation de l'ensemble des employés, car la protection des données est une responsabilité collective.

L'audit interne peut intervenir pour s'assurer que l'entreprise maintient son niveau de conformité dans le temps. Par des audits récurrents, il évalue à la fois les aspects organisationnels (application des processus, documentation, leadership) et techniques (scans et contrôles d'environnements). Ces audits permettent favorisent l'établissement de programmes solides et durables, évitant une conformité superficielle limitée à des politiques et processus théoriques.

06 Quels sont certains des contrôles clés qu'un auditeur interne devrait observer lors d'un audit?

Chaque organisation devrait définir ses contrôles clés, mais en général, le niveau de maturité d'une organisation peut être estimé en vérifiant l'existence de rôles ou de comités dédiés à la vie privée, leur influence auprès de la haute direction, la présence d'un programme de vie privée, un inventaire des traitements, une approche de protection de la vie privée dès la conception pour les nouveaux projets, ainsi que des processus tels que la gestion du consentement, les droits des personnes, la suppression des données après leur durée de conservation, la gestion des incidents, et surtout, l'application pratique de ces processus.

07 Quels conseils donnerais-tu aux auditeurs internes pour s'informer sur le sujet de la protection des renseignements personnels?

Je recommande vivement aux équipes d'audit interne de veiller à ce qu'au moins un membre soit formé sur les questions de vie privée, ce qui peut être réalisé via les formations CIPM ou CIPP proposées par l'IAPP. Ces formations offrent une compréhension approfondie de l'opérationnalisation de la vie privée, le CIPM se concentrant sur l'aspect opérationnel tandis que le CIPP aborde les enjeux réglementaires. De plus, le site de la Commission d'accès à l'information offre des ressources précieuses, étant donné que la CAI est l'entité chargée de l'interprétation et de l'application de la loi au Québec.

Le chapitre Knowledge Network de Montréal de l'IAPP organise des conférences bimensuelles sur des sujets d'actualité liés à la vie privée, et je vous encourage vivement à y participer, car ces événements ne sont pas exclusifs aux membres. De plus, les sites web des différents régulateurs (provinciaux, fédéraux, européens, etc.) disposent d'excellentes «salles de presse» en ligne où vous pouvez trouver toutes les nouvelles importantes. Le site de l'IAPP offre également une salle de presse virtuelle de grande qualité, où l'on peut se tenir informé des dernières évolutions dans le domaine de la vie privée.

Le chapitre de Montreal de l'IAIM offre aussi des formations à ce sujet.

08 Finalement, comment perçois-tu le futur de la gestion des renseignements personnels?

Je pense que la gestion de la vie privée va devenir une composante intégrale des opérations courantes des entreprises, similaire à ce qui s'est produit en Europe environ trois ans après l'entrée en vigueur du RGPD.

Le rôle émergent de l'ingénieur de la vie privée est particulièrement crucial, car ces professionnels de la TI sont capables d'identifier des solutions techniques pour assurer le respect de la vie privée et l'intégrer de manière transparente à l'expérience utilisateur ainsi que dans le cycle de projet de l'entreprise.

De plus, l'avènement de l'IA soulève des défis fascinants en matière de respect de la vie privée, notamment en ce qui concerne les algorithmes qui peuvent agir comme des «boîtes noires». Il est essentiel de pouvoir expliquer et contrôler l'utilisation des Renseignements Personnels (RP) par ces systèmes afin de fournir des informations transparentes, gérer le consentement et les droits des individus.

Entrevue réalisée par
Maelle Gillet pour l'Institut des auditeurs internes – Section Montréal

À propos de l'IAPP

L'IAPP (International Association of Privacy Professionals) est la plus grande et la plus complète communauté mondiale sur la protection de la vie privée et une ressource essentielle, aidant les praticiens à développer et à faire progresser leur carrière, et les organisations à gérer et protéger leurs données. Fondée en 2000 avec seulement une poignée de professionnels dévoués et seulement 2 membres corporatifs, l'organisation a grandi pour compter plus de 75 000 membres dans plus de 100 pays. L'IAPP est devenue le leader reconnu de l'industrie de la vie privée, facilitant les conversations/débats et la collaboration entre les principaux leaders et organisations

À propos de l'IAIM

Fondé en mars 1945, l'Institut des auditeurs internes, Section Montréal (IAI Montréal) est un organisme à but non lucratif constitué en vertu de la loi sur les compagnies du Québec. Il regroupe près de 900 membres et est dirigé par un conseil d'administration, supporté par des comités.

Notre chapitre a pour mission de soutenir et développer les professionnels de l'audit interne tout au long de leur carrière, ainsi que de promouvoir le rôle et la valeur de la profession. Sa vision est d'être reconnu comme un partenaire de choix par la communauté d'affaires, qui veille à la pertinence et l'innovation au sein de la profession.

Notre slogan? Le partenaire par excellence pour la croissance de nos membres!

IAI
Canada
Montréal