LES RÈGLES CANADIENNES EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE EN LIGNE SONT À REVOIR

Anatoliy Gruzd | 19 août, 2020

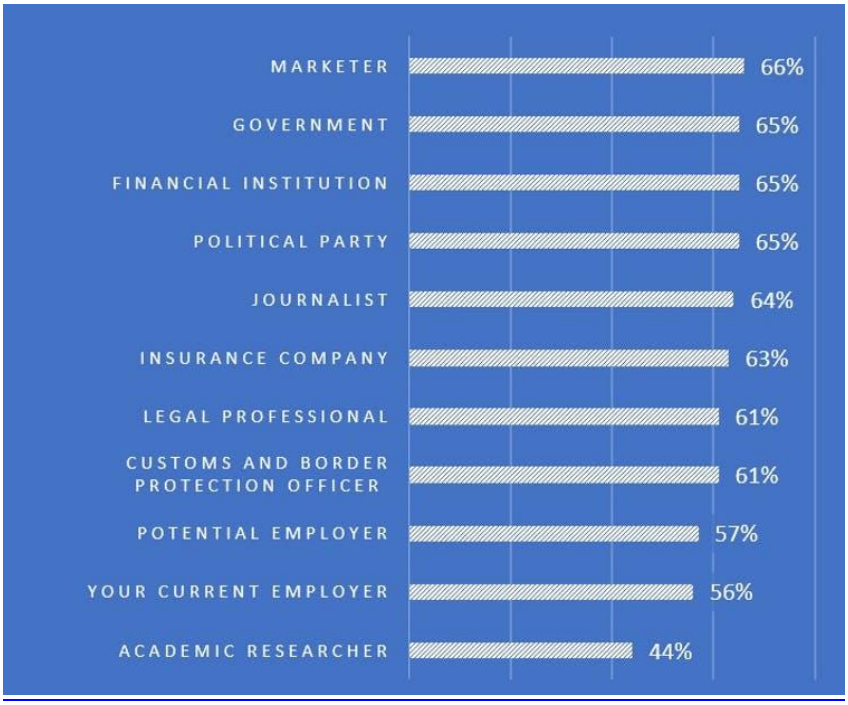
Avec la pandémie, on est davantage coincé à la maison et on a tendance à passer beaucoup plus de temps en ligne en général et sur les médias sociaux en particulier.

Ce n'est pas surprenant, si l'on considère que 99 pour cent des ménages canadiens ont accès à l'Internet à large bande et que 94 pour cent des adultes canadiens en ligne ont un compte sur au moins une plate-forme de médias sociaux, ce qui fait du Canada l'un des pays les plus connectés au monde.

Cependant, plus nous nous servons de ces plates-formes pour aller en ligne et rester en contact avec les gens, plus nous créons de données sur nos intérêts et nos habitudes. Cette mine d'informations sur nous et les personnes de notre réseau peut être utilisée par beaucoup d'organismes, comme les plates-formes de médias sociaux et de nombreuses tierces parties.

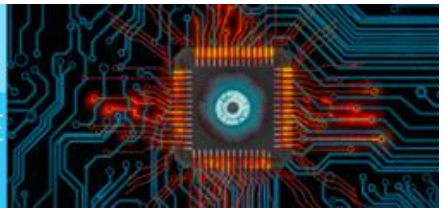
Un malaise croissant

Dans ce contexte, il n'est pas surprenant de voir que les utilisateurs de médias sociaux sont de moins en moins à l'aise avec la quantité de données recueillies à leur sujet et la manière dont on peut les exploiter. Dans notre enquête auprès de 1 500 Canadiens, de 65 à 66 % des répondants ont déclaré ne pas être à l'aise avec le fait que des spécialistes du marketing, le gouvernement, des institutions financières et des partis politiques accèdent à des informations publiques les concernant ou qu'ils ont publiées sur les médias sociaux.



Pourcentage des 1 500 personnes interrogées qui déclarent ne pas être à l'aise avec le fait que des tiers aient accès aux données des médias sociaux qu'elles ont publiées elles-mêmes ou qu'on a publiées à leur sujet. Ryerson University Social Media Lab's Social Media Privacy in Canada Report, 2018, Author provided

RSC SRC



Ce malaise est l'un des signes nous indiquant que les données en ligne des Canadiens ne sont pas suffisamment protégées en vertu de l'actuelle Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE).

La LPRPDE a 20 ans, et son harmonisation avec les principes de la nouvelle Charte numérique du Canada est l'une des priorités énoncées par notre gouvernement. Cependant, le processus a été retardé d'abord par les élections fédérales et ensuite par la pandémie. Par ailleurs, la pandémie a accéléré le développement et le déploiement de nouveaux outils et techniques numériques qui reposent sur une grande quantité de données, telles que la recherche de contacts et la reconnaissance faciale, rendant la révision de la LPRPDE plus pressante que jamais.

Une nouvelle réglementation sur la protection de la vie privée et des données devra tenir compte des technologies émergentes et de leurs applications qui seront le moteur de notre économie numérique dans un avenir proche.

Et ailleurs ?

Lorsque l'Union européenne a adopté le règlement général sur la protection des données (RGPD) en 2018, toute une classe de technologies émergentes basées sur la chaîne de blocs s'est retrouvée en conflit avec celui-ci. La chaîne de blocs est la même technologie que celle utilisée pour créer les bitcoins, mais elle ne se limite pas aux cryptomonnaies. Des sites de médias sociaux comme Steemit, Minds et Memo reposent sur la chaîne de blocs et permettent aux utilisateurs d'avoir davantage de contrôle sur leurs données personnelles.

La nature décentralisée de ces sites rend difficile le respect de la RGPD, qui présume qu'il existe un seul responsable du traitement des données (personne physique ou morale) qui collecte les données des individus et veille à leur protection. Dans les réseaux de chaînes de blocs « pair-à-pair », le registre qui stocke toutes les données est distribué sur plusieurs nœuds et n'est pas contrôlé par une entité unique.

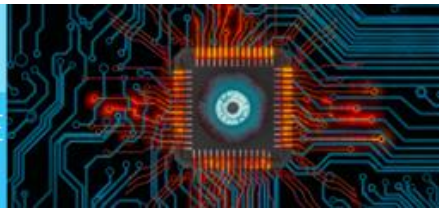
En réalité, cela engendre une « responsabilité conjointe », qui n'est pas évidente à appliquer et à interpréter dans le cadre de la RGPD. La conception décentralisée entre également en conflit avec le principe de minimisation des données de la RGPD, qui exige des responsables du traitement des données qu'ils minimisent la quantité et les types de données collectées sur les individus et stockées.

Une autre caractéristique de la chaîne de blocs, qui vise à protéger contre la modification ou la suppression de données, contredit l'article de la RGPD sur le « droit à l'effacement », qui attribue aux personnes le droit de demander la suppression de leurs données personnelles « dans les meilleurs délais ».

Protections futures

La réglementation actuelle nécessite de nouvelles lignes directrices portant sur les groupes de données décentralisées et axées sur l'utilisateur, comme les sites de médias sociaux basés sur la chaîne de blocs. Mais même si la RGPD requiert encore des améliorations, le Canada pourrait tirer quelques leçons de son exemple.

D'abord, il est crucial que la mise à jour de la LPRPDE ne se concentre pas seulement sur les technologies qui existent déjà, mais aussi sur celles que l'on voit poindre à l'horizon. Des technologies émergentes



telles que la chaîne de blocs modifient les rapports de force entre les responsables du traitement des données et les utilisateurs en concevant de nouvelles façons de créer, de collecter et de partager leurs données.

Deuxièmement, il est important de comprendre que pour garantir la flexibilité et la reddition de comptes nécessaires pour apaiser les préoccupations des Canadiens concernant l'utilisation de leurs données, il faudra faire preuve de créativité dans la façon d'établir la collaboration entre les utilisateurs, les gouvernements, les fournisseurs de plates-formes, les courtiers en données, les industries axées sur les données, les concepteurs d'applications, les chercheurs et les groupes de la société civile.

Ce faisant, le Canada pourra soutenir la prochaine vague d'innovation numérique tout en protégeant et en renforçant les droits des Canadiens en matière de données.

La SRC a créé un groupe de travail sur l'infoveillance en charge de l'examen des répercussions de la surveillance, des données, de la vie privée et de l'égalité. Le groupe de travail a commencé à analyser la transition des notions individualistes de « protection de la vie privée » à l'arrivée du capitalisme de surveillance, qui désigne un système économique d'accumulation fondé sur la marchandisation des données personnelles. Le capitalisme de surveillance présente de nombreuses caractéristiques, notamment la mise en données (action sociale transformée en données quantifiées), le dataïsme (croyance naïve en la capacité des données à résoudre les problèmes humains), la surveillance des données (utilisation des données pour la surveillance des populations et des individus) et le profilage discriminatoire (avec des implications particulières pour les personnes issues de communautés déjà marginalisées).

Les membres du groupe de travail sont : Jane Bailey (Université d'Ottawa) ; Benoît Dupont (Université de Montréal) ; Anatoliy Gruzd (Ryerson University) ; et David Lyon (Queen's University).