

Cultiver la confiance

Dans la foulée du scandale impliquant Facebook et Cambridge Analytica, les entreprises doivent (re)gagner la confiance des consommateurs et la cultiver. Votre entreprise interagit directement avec le public ? La protection des renseignements personnels et de la vie privée est plus que jamais un levier pour vous démarquer de la concurrence.

Le débat sur le « paradoxe de la vie privée » ne date pas d'hier. En effet, les spécialistes du numérique se penchent sur la question depuis plus d'une décennie, mais le débat a certainement pris le devant de la scène ces derniers mois. Les consommateurs se disent soucieux de protéger leurs renseignements personnels, mais leurs comportements en ligne ne reflètent pas toujours cette préoccupation. « Les gens affirment qu'ils se préoccupent grandement de leur vie privée. Cependant, en réalité, ils sont prêts à échanger leurs données ou même les adresses de courriel d'amis pour quelque chose d'aussi banal qu'une pointe de pizza », ironise le journaliste techno Chris Ip. Du côté des entreprises, les positions sont tout aussi contradictoires. « Elles [les entreprises] sont prises entre utiliser des données pour offrir une meilleure expérience aux consommateurs et empiéter sur le droit à la vie privée de ceux-ci », conclut Rani Molla, chroniqueuse données pour Recode, à la lecture du dernier rapport sur les tendances Internet de Mary Meeker.



Le scandale Facebook-Cambridge Analytica, mis au jour par le *Guardian* et le *New York Times* en mars 2018, a incontestablement remis le paradoxe de la vie privée à l'avant-plan du débat public.

Près de 90 millions d'utilisateurs de Facebook auraient été touchés par cette collecte illégitime de données personnelles à des fins de profilage électoral pendant les présidentielles américaines de 2016.

Au printemps 2018, on a aussi dévoilé que Facebook aurait communiqué des données sur ses clients à Apple, à Samsung et à des douzaines d'autres fabricants d'appareils et que l'entreprise aurait approché des hôpitaux américains dans l'optique d'accéder à des données médicales. Quelques mois plus tard, en septembre, Facebook était victime d'une cyberattaque qui aurait exposé les données de 29 millions de ses utilisateurs.

Si la dernière année s'est avérée éprouvante pour Facebook, bien d'autres entreprises — dont Google et sa plateforme vidéo YouTube, Yahoo, Twitter et Grindr — ont été plongées dans des controverses liées à une utilisation douteuse, voire illégale, de renseignements personnels. Par ailleurs, une étude de l'Université de Californie à Berkeley publiée en avril 2018 avance que plus de la moitié des applications Android destinées aux enfants de moins de 13 ans pourraient contrevenir à la loi américaine COPPA (*Children's Online Privacy Protection Act*) en raison de pratiques de collecte et de partage de données non conformes.



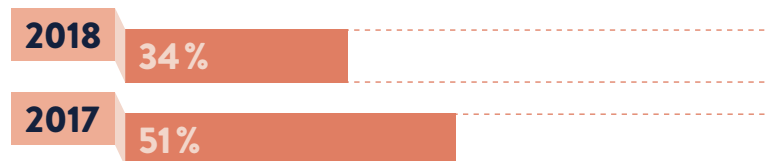


La perspective des consommateurs à l'ère de la personnalisation

Certes, les consommateurs sont de plus en plus méfiants. Un sondage réalisé par GlobalWebIndex en octobre 2018 révèle que 65 % des répondants nord-américains (62 % parmi les Canadiens) s'inquiètent de la manière dont les entreprises exploitent leurs renseignements personnels.

En 2018, seulement 34 % des Canadiens affirment avoir confiance en Facebook, selon les chiffres de la firme Proof Inc. Il s'agit d'un recul de 17 points de pourcentage par rapport à l'année précédente. **Malgré tout, 84 % des répondants au pays demeurent des utilisateurs actifs de la plateforme.** « Nous sommes très préoccupés par la façon dont Facebook se comporte comme organisation, explique Josh Cobden, premier vice-président de Proof Inc. Nous continuons néanmoins d'utiliser la plateforme, car elle livre ce que nous attendons d'elle. »

Canadiens affirmant avoir confiance en Facebook



Le partage de renseignements personnels n'est donc pas un frein à l'utilisation d'une plateforme si celle-ci répond aux besoins des utilisateurs et leur offre une expérience pertinente et personnalisée.

Au total, 53 % des Canadiens accepteraient de partager leurs renseignements personnels en échange de produits et de services adaptés à leurs attentes selon un sondage mené par CROP en mai 2018. Cette proportion grimpe à 67 % parmi les 25-34 ans et à 79 % parmi les 18-24 ans. « Les jeunes sont plus friands de consommation et sont donc fort enthousiastes à l'idée de partager leurs renseignements pour mieux en profiter », conclut la firme de sondage.

Canadiens acceptant de partager leurs renseignements personnels





Là où une entreprise s'adressant directement aux consommateurs peut réussir à se démarquer, c'est en offrant à ses clients l'assurance d'une utilisation responsable de leurs données personnelles et du respect de leur droit à la vie privée.

« La réputation d'une entreprise et la confiance qu'elle inspire dépendent de sa crédibilité et de sa transparence en matière de données personnelles. »

— Chase Buckle, analyste chez GlobalWebIndex, 2018

Le phénomène est loin d'être nouveau. Le laboratoire *Regards sur le numérique* de Microsoft France, par exemple, observait en 2015 que la protection des données personnelles était appelée à devenir un important « élément de différenciation concurrentielle ». Toutefois, l'impératif d'une saine gestion des données se fait aujourd'hui plus pressant en raison notamment d'une évolution marquée de la réglementation.





La perspective des entreprises à l'heure du RGPD

Plus que toute autre mesure législative à ce jour, le *Règlement général sur la protection des données (RGPD)* de l'Union européenne (UE) incite les entreprises à mieux utiliser et protéger les renseignements personnels de leurs clients. En gestation depuis 2012, le RGPD est entré en vigueur en mai 2018, soit quelques semaines après l'éclatement du scandale Facebook-Cambridge Analytica.

Entre autres mesures, le RGPD introduit des obligations de consentement explicite à la collecte de données personnelles, le droit pour les internautes de l'UE d'exiger l'effacement des renseignements qui les concernent, des sanctions plus sévères contre les entreprises prises en défaut et l'obligation pour les sociétés étrangères de se conformer aux mesures législatives.

« Désormais, les consommateurs de l'UE auront la liberté d'adhérer [à la collecte de données personnelles] plutôt que le fardeau de demander une exemption. L'importance accordée au consentement crée un incitatif financier à gagner la confiance du consommateur. »

— Nitasha Tiku, journaliste pour Wired, 2018





Les géants de la Silicon Valley ont rapidement emboîté le pas. Facebook a mis sur pied une nouvelle équipe chargée du développement d'outils de gestion des données personnelles, dont une nouvelle fonctionnalité permettant d'effacer l'historique de navigation. Pour sa part, Google a renforcé ses fonctionnalités d'effacement sur l'ensemble de ses plateformes à l'automne.

Apple exige désormais que toute application proposée dans l'App Store soit accompagnée d'une politique relative aux renseignements personnels et à la vie privée. Le PDG d'Apple, Tim Cook, a d'ailleurs fait les louanges du RGPD en octobre dernier, félicitant l'UE pour son initiative et invitant les États-Unis à renforcer leurs propres mesures réglementaires en matière de protection de la vie privée. « Les appareils et les logiciels d'Apple — tout comme l'éthos de la compagnie — sont désormais axés sur des mesures de protection de la vie privée des utilisateurs que d'autres sociétés technologiques n'auraient jamais pensé adopter », fait remarquer l'auteur et journaliste Michael Grothaus.

C'est précisément là où résident les inquiétudes de plusieurs observateurs. **À terme, un encadrement de plus en plus serré des données personnelles avantagera-t-il une poignée de colosses comme Google, Apple, Facebook et Amazon au détriment d'entreprises aux moyens (financiers et technologiques) plus modestes ?** Aux États-Unis, de grands médias écrits comme le *Los Angeles Times* et le *Chicago Tribune* ont dû bloquer leur site Web aux internautes européens, car ils ne pouvaient pas en garantir la conformité aux exigences du RGPD. Une autre mesure actuellement à l'étude en Europe, soit le projet de règlement ePrivacy, suscite une vive controverse au sein même de l'UE. Cinquante entreprises médiatiques européennes s'y sont publiquement opposées en mars dernier : « Les entreprises médiatiques prétendent que, dans sa forme actuelle, le projet de règlement ePrivacy exigerait qu'elles obtiennent toutes le consentement explicite des consommateurs à l'utilisation de témoins (cookies) et qu'une telle mesure rendrait Google, Facebook et Amazon encore plus puissantes », rapporte Jessica Davis dans Digiday.





Quelle sera l'incidence à long terme de ces initiatives réglementaires sur le marché européen ? Quelle influence auront-elles sur la réglementation et la conduite des affaires ailleurs dans le monde ? Les mesures adoptées par l'UE ont certainement influencé les débats législatifs au Canada. En février 2018, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique recommandait de modifier la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) en vue d'y introduire ou d'y renforcer des mesures relatives entre autres au consentement, au déréférencement ainsi qu'à l'effacement et la destruction de renseignements personnels. Le comité invitait par ailleurs le gouvernement canadien à s'assurer que la LPRPDE « conserve son caractère adéquat » au regard du RGPD.

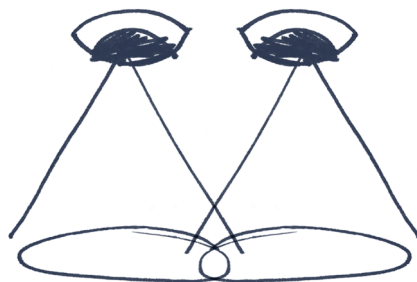
Le Ministre de l'Innovation, des Sciences et du Développement économique a accueilli ces recommandations favorablement, mais il a toutefois insisté sur la nécessité de les examiner davantage — notamment dans le cadre de consultations publiques lancées en juin 2018 — et d'envisager une harmonisation raisonnable de la loi canadienne avec le RGPD : « Reconnaissant l'importance de l'interopérabilité des régimes de protection de la vie privée, l'UE a adopté le concept d'équivalence essentielle plutôt qu'égale [...] En ce sens, il n'est pas clair que les exigences de la LPRPDE doivent refléter l'ensemble des droits et des mesures de protection du RGPD pour conserver à la Loi son caractère adéquat. »



Dans ce contexte d'incertitude réglementaire, les entreprises peuvent néanmoins être assurées de deux choses : l'exploitation des mégadonnées (*Big Data* en anglais) demeurera un facteur de succès clé dans l'économie numérique et les consommateurs, aujourd'hui mieux conscientisés, seront vraisemblablement plus sensibles aux enjeux qui touchent le respect de leur vie privée.

Les entreprises médiatiques ont tout à gagner d'une approche plus proactive et plus préventive, comme le souligne Dre Ann Cavoukian, ancienne commissaire à l'information et à la protection de la vie privée de l'Ontario et pionnière du principe de protection de la vie privée dès la conception (*Privacy by Design*) à la fin des années 1990 :

«Allant de l'avant, la protection de la vie privée ne peut être assurée seulement par la conformité aux cadres réglementaires. L'assurance de protection de la vie privée devra plutôt — dans un monde idéal — devenir le mode de fonctionnement par défaut de toute organisation.»



Outils en matière de vie privée à l'intention des entreprises canadiennes

Selon le dernier *Sondage sur la cybersécurité* (automne 2018) de l'Autorité canadienne pour les enregistrements Internet,

59 %

des entreprises répondantes ont dit stocker des données personnelles, mais

38 %

ont avoué ne pas bien connaître la LPRPDE.

Quelles sont vos obligations en vertu de la LPRPDE ? Des lois provinciales s'appliquent-elles également à vous ? Innovation, Sciences et Développement économique Canada vous propose une trousse d'outils pour bien comprendre vos responsabilités en matière de protection des renseignements personnels. Le Commissariat à la protection de la vie privée du Canada vous offre également des conseils sur comment rédiger une politique de confidentialité : « une bonne politique de confidentialité explique — dans un langage clair et simple — pourquoi une organisation recueille des renseignements personnels, ce qu'elle va en faire, comment ils seront protégés et à qui elle les communiquera. »

