

---

**Forum étudiant 2019****LES RÉSEAUX SOCIAUX ET LA PROTECTION DES DONNÉES PERSONNELLES**

---

Préparé par Pierre Skilling

Septembre 2018

Au cours des dernières années, la multiplication des réseaux sociaux et la rapidité toujours croissante de la circulation de l'information ont posé des défis complètement nouveaux aux citoyens comme aux institutions gouvernementales. Le récent scandale Cambridge Analytica – cette entreprise britannique qui a récolté des données personnelles sur des millions d'utilisateurs de Facebook à leur insu et qui est soupçonnée d'avoir joué un rôle dans l'issue de la campagne présidentielle américaine de 2016 – illustre à lui seul l'immense influence des réseaux sociaux et les répercussions que peut avoir une protection défailante des données personnelles, sur la vie privée comme sur le plan politique.

Dans ce contexte, comment assurer une protection adéquate des données personnelles ou en reprendre le contrôle? Jusqu'à quel point les entreprises technologiques telles que Facebook, Google, Twitter, Apple ou Amazon devraient-elles mettre en place des mesures de protection des données de leurs utilisateurs? Quel rôle les gouvernements et les États devraient-ils jouer dans le contrôle de ces entreprises et de l'utilisation qu'elles font des données auxquelles elles ont accès? Ces questions sont maintenant plus urgentes que jamais.

En 2013, Edward Snowden, un ancien employé des services secrets des États-Unis (National Security Agency – NSA), avait révélé que cette agence et des agences alliées pratiquaient une surveillance de masse des communications numériques, en interceptant les métadonnées<sup>1</sup>. L'étendue et l'intensité de cette surveillance, touchant tout le monde, avaient provoqué de très larges réactions sur la planète.

Puis, en mars 2018, *The New York Times* et *The Observer* (une publication sœur du quotidien *The Guardian* à Londres) ont révélé que la société Cambridge Analytica a obtenu, sans leur consentement, les données de 87 millions d'utilisateurs du réseau Facebook pour les vendre à des personnalités politiques cherchant à influencer le choix des électeurs américains à l'occasion des élections présidentielles de 2016.

---

<sup>1</sup> « Les métadonnées indiquent l'expéditeur et le(s) destinataire(s) d'un message, la date et l'heure de l'envoi, la durée d'un appel, etc. » (Raphaëlle Derome, « Tous surveillés? », *Curium*, n° 27, février 2017, p. 13)

Qu'est-ce que Cambridge Analytica? Il s'agit d'une entreprise britannique spécialisée dans le profilage psychographique<sup>2</sup>. Elle récupère des données sur les réseaux sociaux afin de tenter de prédire les comportements électoraux. Elle aide les partis politiques à cerner les portions de la population pour lesquelles il serait profitable de déployer des efforts afin de les convaincre de voter pour eux. La société a travaillé avec l'équipe de Donald Trump lors de l'élection de 2016 ainsi qu'avec d'autres candidats républicains, comme Ted Cruz et Ben Carson. Certes, 270 000 personnes avaient accepté de participer à un test sur une application de Facebook et consenti à donner des informations personnelles. Mais ladite application a également collecté les données des « amis » de ces utilisateurs, c'est-à-dire de l'information à propos plus de 50 millions de personnes, sans leur autorisation. En outre, Cambridge Analytica a aussi travaillé pour la campagne du « *Leave* » au moment du référendum sur le Brexit au Royaume-Uni, plus tôt la même année.

Canadien d'origine et cofondateur de Cambridge Analytica, Christopher Wylie est le lanceur d'alerte dans cette histoire. Il raconte avoir participé à l'élaboration du stratagème avec des chercheurs de l'Université de Cambridge afin d'obtenir des données pour cibler des électeurs avec des publicités politiques personnalisées. C'est la victoire de Donald Trump qui l'aurait poussé à remettre en question les pratiques de son entreprise, tout en considérant que Facebook a sa part de responsabilité.

En avril 2018, à la suite de ces révélations, le PDG de Facebook, Mark Zuckerberg, a été entendu en audition devant le Congrès des États-Unis, s'excusant et promettant plus de sécurité sur sa plateforme. Il s'est ensuite présenté en mai devant le Parlement européen s'excusant de nouveau pour les lacunes du réseau social dans la protection des données de ses utilisateurs.

### **La valeur, la portée et le risque du partage des données personnelles**

Les données personnelles collectées et enregistrées par les puissants GAFA (Google, Amazon, Facebook, Apple, auxquels on peut ajouter Microsoft et tous les autres sites Internet) « disent tout de notre vie : la musique que l'on écoute au réveil ou qui nous berce avant de dormir, la marque de céréales que nous achetons pour nos enfants, le fait que l'on baisse le son (ou qu'on le monte...) lorsqu'on entend [un] podcast, le nombre de kilomètres courus dans le week-end, le nom de la voiture de nos rêves dont nous avons vu la vidéo 14 fois en moins de vingt-quatre heures, la fréquentation ou non des sites de rencontres, etc.<sup>3</sup> ».

---

<sup>2</sup> « Tout ce que vous devez savoir sur le scandale Facebook-Cambridge Analytica ». *Ici Radio-Canada*, 19 mars 2018.

<http://ici.radio-canada.ca/nouvelle/1090159/facebook-cambridge-analytica-donnees-personnelles-election-politique-campagne-marketing-politique>

<sup>3</sup> Guillaume Grallet et autres, « Données personnelles et vie privée : comment reprendre le contrôle », *Le Point*, n° 2369, 25 janvier 2018.

Ces données cédées gratuitement par le citoyen-consommateur sont analysées et revendues à des fins publicitaires ciblées. Elles sont la base du modèle économique de Facebook, qui en échange offre son service de réseautage social.

Outre une vie privée qui le devient de moins en moins, le partage des données personnelles comporte plusieurs risques, dont celui qu'elles soient piratées par des *hackers*, ou encore qu'elles soient vendues à des *data brokers* (courtiers et revendeurs de données). Ce trafic de données, présent notamment aux États-Unis, peut entre autres nuire au dossier de crédit d'un individu, nuire à sa réputation et à sa recherche d'emploi, et même (dans le cas américain) mener à des pratiques problématiques dans les hôpitaux et les cabinets médicaux (trafic de données sur la santé et informations médicales<sup>4</sup>). Les *data brokers* sont au cœur d'un marché économique évalué en 2015 à 200 milliards de dollars<sup>5</sup>.

### **Comment assurer une protection des données personnelles? Deux conceptions de la vie privée en Amérique du Nord et en Europe**

Comment reprendre le contrôle sur ses données? En France, l'auteur et fondateur du think-tank GenerationLibre, Gaspard Koenig, propose que soit institué « un droit de propriété sur les données personnelles ». Ainsi, le producteur de données reprendrait possession de ce qui est sien et pourrait être rémunéré pour les informations qu'il crée et qu'il partage<sup>6</sup>.

Y a-t-il des exemples d'une pratique semblable ? On peut penser au domaine agricole aux États-Unis, où une « ferme de serveurs coopérative » pour mutualiser le stockage des données agricoles a été mise sur pied par l'Agricultural Data Coalition en 2016, à la suite d'une entente entre prestataires informatiques et représentants des fermiers sur des principes de sécurité et de confidentialité pour des données agricoles<sup>7</sup>.

Parmi les autres pistes, on trouve l'idée d'une rémunération des producteurs de données que sont les internautes contribuant aux bases de données des géants du Web (donc presque tout le

---

<sup>4</sup> Frank Pasquale, « Mettre fin au trafic des données personnelles : après l'affaire Facebook-Cambridge Analytica », *Le Monde diplomatique*, n° 770, mai 2018, p. 16-17.

<sup>5</sup> « Ces entreprises, totalement inconnues du grand public, récupèrent, analysent et revendent des données de tous horizons. Elles fleurissent essentiellement aux États-Unis, où le croisement des fichiers est beaucoup moins limité qu'en Europe. Facebook explique [...] ne vendre aucune donnée à ces spécialistes. Mais, souvent, ces derniers se servent eux-mêmes. Ainsi, pour déterminer si une personne a droit à un emprunt, la société allemande Kreditech passe au peigne fin l'activité sur les réseaux sociaux du demandeur, ainsi que ses comptes Amazon ou eBay. » *Ibid.*

<sup>6</sup> Gaspard. Koenig, « Ne donnons plus nos données », *Le Nouveau magazine littéraire*, n° 4, avril 2018, p. 48.

<sup>7</sup> Pierre Rimbet, « Données personnelles, une affaire politique : se réapproprié une ressource d'utilité publique », *Le Monde diplomatique*, n° 750, septembre 2016, p. 3.

monde!), ou encore de taxer les entreprises technologiques sur la valeur générée par les données personnelles<sup>8</sup>.

La vision même de la vie privée diffère entre les États-Unis et l'Europe. Cette dernière s'en préoccupe de façon plus stricte. L'Union européenne (UE) a adopté le Règlement général sur la protection des données (RGPD), entré en vigueur le 25 mai 2018. Le RGPD renforce les droits des citoyens européens concernant leurs données personnelles. Toutes les entreprises des 28 États membres, ainsi que celles issues des pays hors UE, mais collectant et traitant des données de résidents européens (comme Google, Facebook ou Amazon), y sont soumises. Le RGPD repose sur trois grands principes : la transparence, le droit des utilisateurs, et enfin la responsabilité des entreprises.

En vertu du RGPD, le citoyen doit exprimer son consentement de manière explicite et a un accès renforcé à ses données. Il devra savoir ce que l'entreprise compte en faire, et celle-ci devra l'en informer de façon claire et compréhensible. Le RGPD consacre aussi, notamment, un « droit à l'oubli » numérique. Le droit à l'effacement des données auprès du responsable du traitement vient compléter le droit au déréférencement d'une information ou d'un lien sur un moteur de recherche. En Europe, les entreprises qui manquent à leurs obligations édictées dans le RGPD encourent de lourdes pénalités, soit jusqu'à 4 % du chiffre d'affaires<sup>9</sup>.

Par contraste, la législation américaine permet aux entreprises de médias sociaux de conserver le contenu du profil des utilisateurs dans la sphère numérique même quand cette personne ne le désire plus, pouvant même mener à une sorte d'immortalité dans l'univers numérique. Alors que l'Europe privilégie le droit des individus à contrôler leurs données personnelles, la législation américaine, reposant largement sur le consentement, privilégie la capacité de diffuser des informations, en raison entre autres du premier amendement de la Constitution des États-Unis qui protège la liberté de parole et la liberté de presse<sup>10</sup>. Par ailleurs, il est à noter que la Californie a adopté en juin 2018 une législation sur les données personnelles largement inspirée du RGPD européen.

Au Canada (*Loi sur la protection des renseignements personnels et les documents électroniques*) et au Québec (*Loi sur la protection des renseignements personnels dans le secteur privé*), les lois actuelles touchant ces questions fonctionnent selon un système de plaintes et sont basées sur un cadre général de consentement, contrairement à l'approche européenne.

Dans un rapport présenté à la Chambre des communes, le Comité permanent de l'accès à

---

<sup>8</sup> *Ibid.*

<sup>9</sup> Guillaume Grallet, *op. cit.*

<sup>10</sup> Cayce Myers, « Digital Immortality vs. “The Right to be Forgotten”: A Comparison of U.S. and E.U. Laws Concerning Social Media Privacy », *Romanian Journal of Communication & Public Relations*, vol. 16, no. 3 décembre 2014, p. 48.

l'information, de la protection des renseignements personnels et de l'éthique a recommandé en juin 2018 que le gouvernement du Canada mette en œuvre des mesures pour veiller à la mise en place de protections semblables à celles du RGPD au Canada<sup>11</sup>. Au Québec, dans un communiqué publié en mars 2018, la Commission d'accès à l'information s'est dite préoccupée par les révélations voulant que les renseignements personnels de milliers d'utilisateurs de Facebook aient été récupérés sans leur consentement, et a rappelé que dans son dernier rapport quinquennal (2016), l'une des recommandations portait justement sur la durée de conservation des renseignements personnels par les entreprises privées<sup>12</sup>.

### **Pistes de réflexion**

- Serait-il souhaitable et envisageable que soit institué un droit de propriété des citoyens sur leurs données personnelles au Canada et au Québec ? Si oui, quels en seraient les conditions et les paramètres ?
- Au Québec, les partis politiques ont-ils recours aux données personnelles sur les réseaux sociaux afin d'influencer les électeurs ? Dans quelle mesure ?
- Faudrait-il aménager la *Loi sur la protection des renseignements personnels dans le secteur privé* afin de l'adapter aux nouvelles réalités du partage des données personnelles sur les réseaux sociaux ? De quelle façon ?
- Le Québec devrait-il s'inspirer du Règlement général sur la protection des données de l'Union européenne afin d'offrir aux usagers québécois des réseaux sociaux une meilleure protection de leurs données personnelles ?
- Des compétences de base en informatique, et particulièrement en codage, devraient-elles faire partie du programme scolaire au Québec ?
- Dans le même ordre d'idées, le programme scolaire québécois offre-t-il suffisamment d'outils aux élèves pour comprendre les enjeux liés à la vie privée et au traitement des informations personnelles par les entreprises et par les autorités publiques ?

---

<sup>11</sup> <http://www.noscommunes.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-f.pdf>

<sup>12</sup> <http://www.cai.gouv.qc.ca/fuite-de-donnees-personnelles-de-milliers-dutilisateurs-de-facebook/>

## Bibliographie

Commissariat à la protection de la vie privée au Canada. *Aperçu des lois sur la protection des renseignements personnels au Canada*, [En ligne].  
[https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/02\\_05\\_d\\_15/](https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/02_05_d_15/) (Page consultée le 6 août 2018).

Commission européenne. *Réforme des règles de l'UE en matière de protection des données 2018*, [En ligne].  
[https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules\\_fr](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_fr) (Page consultée le 6 août 2018).

Commission nationale Informatique et libertés (CNIL). *Comprendre le RGPD*, [En ligne].  
<https://www.cnil.fr/fr/comprendre-le-rgpd>

Derome, Raphaëlle. « [Dossier] Tous surveillés? », *Curium*, n° 27 (février 2017), p. 11-21.

Eggleton, Art; Saint-Germain, Raymonde. « Améliorer la protection des données personnelles au Canada », *Policy Options/Options politiques*, 2 juillet 2018.  
<http://policyoptions.irpp.org/fr/magazines/july-2018/ameliorer-la-protection-des-donnees-personnelles-au-canada>

Galloway, Scott, *The Four – Le règne des quatre : la face cachée d'Amazon, Apple, Facebook et Google*, Montréal, Édito, 2018, 372 p.

Grallet, Guillaume; Poncet, Gueric; Pons, Héloïse; Durand-Parenti, Chloé; Parrino, Béatrice. « Données personnelles et vie privée : comment reprendre le contrôle », *Le Point*, n° 2369, 25 janvier 2018, p. 34-48.

Kerry, Cameron F. « Why protecting privacy is a losing game today—and how to change the game », *Brookings Institution*, 12 juillet 2018.  
<https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game>

Koenig, Gaspard. « Ne donnons plus nos données », *Le Nouveau magazine littéraire*, n° 4, avril 2018, p. 48-49.

Lestavel, Thomas. « Vos données personnelles valent-elles de l'or? », *OInet*, n° 858 (1<sup>er</sup> février 2017), p. 30-32.

<https://thomaslestavel.files.wordpress.com/2017/03/donnecc81es-persos.pdf>

Pasquale, Frank. « Mettre fin au trafic des données personnelles : après l'affaire Facebook-Cambridge Analytica », *Le Monde diplomatique*, n° 770 (mai 2018), p. 16-17.

Pathmasiri, Saminda. « L'Internet n'oublie jamais! dit-on. Est-ce toujours vrai? », *Développements récents en droit du divertissement*, Montréal : Service de la formation continue du Barreau du Québec, 2015, p. 3-29.

Rimbet, Pierre. « Données personnelles, une affaire politique : se réapproprier une ressource d'utilité publique », *Le Monde diplomatique*, n° 750 (septembre 2016), p. 3.

« Tout ce que vous devez savoir sur le scandale Facebook-Cambridge Analytica ». Ici Radio-Canada, 19 mars 2018.

<http://ici.radio-canada.ca/nouvelle/1090159/facebook-cambridge-analytica-donnees-personnelles-election-politique-campagne-marketing-politique>

Trudel, Brigitte. « Perdre le contrôle de sa vie privée », *Le Fil*, vol. 52, n° 20 (23 février 2017).

<https://www.lefil.ulaval.ca/perdre-contrôle-de-vie-privée>

Trudel, Pierre, « Vie privée – Demander des comptes à Big Brother », *Le Devoir*, 20 décembre 2016.