Les affaires - website
August 23, 2018
URL: http://www.lesaffaires.com/dossier/nouvelles-frontieres-en-regulation-financiere/protection-des-donnees-personnelles-comment-eviter-les-derives/604471

Protection des données personnelles: comment éviter les dérives?

Offert par Les Affaires

Édition du 25 Août 2018

PAR RICHARD CLOUTIER

Twitter | Courriel

Les entreprises consiste à satisfaire leur obligation d'énoncer clairement ce qu'elles vont faire des renseignements personnels récoltés. [Photo: 123RF]

L'évolution technologique et l'émergence de nouveaux acteurs dans le secteur financier obligent les législateurs et les régulateurs à remettre en question les pratiques traditionnelles en matière de gestion, d'utilisation et de protection des données personnelles.

À mesure que l'écosystème financier adopte les technologies, il se concentre sur les données, tant dans leur valeur stratégique que dans la façon dont elles sont traitées et protégées.

Ainsi, « la fourniture de produits de paiement, de crédit, d'assurance et d'investissement dépend du stockage, du traitement et de la transmission d'éléments de données qui représentent des actifs et des passifs financiers, ainsi que des informations sensibles sur les clients », constate l'Institute of International Finance (IIF), dans un rapport publié le 6 juillet 2018.

À cet égard, le défi pour les entreprises consiste à satisfaire leur obligation d'énoncer clairement ce qu'elles vont faire des renseignements personnels récoltés.

« Historiquement, beaucoup de clauses de consentement étaient : "ou pour toute autre utilisation en lien avec la recherche, l'optimisation de nos services, l'amélioration de nos processus », donc étaient des fourre-tout permettant d'englober beaucoup d'utilisations qui, au moment de la collecte, demeuraient ésotériques et indéterminées », indique Jean-François de Rico, associé chez Langlois avocats.

Aujourd'hui, cette réalité pose un défi aux institutions financières désirant faire affaire avec une *fintech*. Par exemple, si elle veut lui communiquer des renseignements personnels tirés de sa base de données afin d'alimenter le développement d'un algorithme propulsé par l'intelligence artificielle dans le but de faire du profilage, est-ce que le consentement des clients obtenu au départ est suffisant ?

De même, comment l'obligation de la durée de conservation des données, qui doit prendre fin au moment où il n'y a plus d'utilisation requise, se matérialise-t-elle si les données sont anonymisées pour nourrir des algorithmes de l'intelligence artificielle ? D'autant plus, signale Jean-François de Rico, qu'il y a beaucoup de démonstrations dans l'histoire récente selon lesquelles il est impossible d'anonymiser les données de façon complète.

Quant à la *blockchain*, il estime que « si le principe d'un registre distribué est son caractère indélébile et le maintien de son intégrité, il faut que le développement des couches applicatives utilisées permette d'isoler les renseignements personnels afin de se prémunir d'une atteinte à la confidentialité ou à la disponibilité ».

Que dit la réglementation ?

À la suite du scandale Facebook/Cambridge Analytica, l'Europe a remplacé en mai 2018 sa directive sur la protection des données personnelles, qui datait de 1995, par le Règlement général sur la protection des données (RGPD).

En plus de reprendre les principes de protection des renseignements personnels déjà en vigueur, y compris le consentement de la personne concernée ou le droit d'accéder à ses données personnelles, le RGPD a créé de nouveaux droits, dont « le droit au déréférencement et le droit à la portabilité des données », selon la Commission d'accès à l'information du Québec.

Aux États-Unis, la Californie a emboîté le pas en adoptant le California Consumer Privacy Act, qui vise à protéger les données personnelles collectées par les entreprises et à permettre aux consommateurs de refuser qu'on les utilise à des fins commerciales.

Au Canada, la protection des renseignements personnels est encadrée par deux régimes, le fédéral et le provincial, alors que trois provinces, dont le Québec, ont adopté leur propre loi.

« Les deux niveaux de régime prévoient des règles bien précises liées à la collecte, à l'utilisation, à la communication, à la sécurité et à la destruction des renseignements personnels, mais sans avoir toujours le même degré d'obligations », précise Nicolas Vermeys, professeur agrégé à la faculté de droit de l'Université de Montréal.

Pour leur part, les régulateurs comme l'Autorité des marchés financiers (AMF) précisent dans leurs règlements les attentes particulières qu'ils ont envers les entreprises qu'ils encadrent concernant, par exemple, la cybersécurité et l'utilisation des médias sociaux.

« Les inscrits ont une responsabilité de mettre en place une politique et des procédures qui correspondent de façon proportionnelle au niveau de risque que la cybersécurité représente pour eux », confirme Moad Fahmi, directeur fintech et innovation, à l'AMF.

Selon lui, toutefois, la question de la protection des données est présente dans toutes les sphères de la société, et si pour l'AMF, « en matière financière, la cybersécurité est une question vraiment cruciale, elle transcende notre mandat et soulève des questions qui deviennent sociétales et qui méritent des discussions plus larges sur ce que l'on veut dans notre futur à mesure que notre vie se numérise ».

Jean-François de Rico constate une tendance forte vers la reconnaissance d'un droit de déréférencement, « une tendance qui va être difficile à renverser et qui va créer des défis technologiques significatifs ».