Les sociétés, protectrices de la vie privée

« Il n'est pas nouveau de constater que la Constitution protège parfois quelques criminels pour préserver la vie privée de tous. »

– Antonin Scalia, ancien juge à la Cour suprême des États-Unis

On pourrait croire que ce dernier commentaire du juge Scalia résume judicieusement la querelle très médiatisée survenue aux États-Unis au cours des derniers mois, opposant Apple et le U.S. Federal Bureau of Investigation (FBI). La capacité du gouvernement d'accéder à des renseignements personnels est au cœur de ce débat. Cette confrontation a soulevé des questions fondamentales sur l'équilibre entre les droits de la personne et la sécurité collective. Elle souligne également que les questions de confidentialité constituent un risque réel très important pour plusieurs sociétés. Il est opportun d'examiner quels sont ces risques et quelle est l'incidence de la vie privée, ou de l'absence de celle-ci, sur les sociétés et les produits et services qu'elles offrent.

La vie privée est-elle un droit?

Le « droit » à la vie privée varie grandement selon l'endroit où vous vivez. Les États-Unis, par exemple, abordent la vie privée d'une manière différente de la plupart des autres développés. La Constitution des États-Unis ne prévoit aucun droit particulier à la vie privée, bien qu'elle fasse allusion à certains aspects de celle-ci, par exemple en empêchant les perquisitions et saisies abusives. En matière de renseignements personnels, les États-Unis se distinguent par l'absence de loi qui protège globalement leur confidentialité. Ils ont tout au plus mis en vigueur diverses mesures législatives qui protègent la confidentialité de l'information dans certains secteurs. Dans l'ensemble, cela signifie que la protection des renseignements personnels aux États-Unis n'est pas aussi rigoureuse que dans certains autres pays développés.

L'Europe offre un bon exemple de protection rigoureuse des renseignements personnels. Les gouvernements européens ont reconnu collectivement le droit à la vie privée en l'intégrant de manière précise dans la Convention européenne des droits de l'homme, adoptée en 1950. L'Union européenne (UE) a harmonisé la protection des renseignements personnels dans tous les États membres en adoptant, en 1995, la Directive sur la protection des données personnelles. Tous les États membres, en plus de la Suisse, ont édicté des lois pour se conformer à cette directive de l'UE.

Le Canada dispose de sa propre loi sur la vie privée, celle-ci étant aussi conforme à la directive de l'UE. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) est entrée en vigueur le 1er janvier 2001. Dès lors, la plupart des provinces ont elles aussi adopté des lois complémentaires. La LPRPDE définit clairement les droits des personnes et les obligations des sociétés qui collectent des renseignements personnels. Cette loi prévoit notamment l'obligation d'obtenir un consentement avant de collecter, d'utiliser ou de divulguer des renseignements. Elle comprend aussi l'obligation de préserver toute l'information recueillie.

Celle-ci exige que les sociétés agissent comme gardiens des renseignements personnels et protecteurs de la vie privée, ce qui soulève certains risques pour elles. Un manquement à ces obligations peut entraîner des conséquences très graves pour leurs marques, et même des pertes financières. Pour les investisseurs, le risque d'atteinte à la vie privée est devenu un risque d'investissement. Certains cas récents l'ont démontré.

Une pomme pourrie

Le cas récent qui opposait Apple inc. au FBI, aux États-Unis, a illustré à quel point les problèmes de protection des renseignements personnels peuvent être importants. Le FBI a ordonné à Apple de permettre l'accès au iPhone utilisé par l'auteur de la tuerie à San Bernardino, en Californie, en décembre 2015. Le chiffrement du iPhone, son mot de passe et sa fonction qui permet d'effacer le contenu posaient au FBI un obstacle insurmontable sans l'aide d'Apple. Apple a collaboré avec la police et les services de sécurité sur plusieurs cas dans le passé, mais cette fois, c'était différent. Le FBI ne demandait

pas seulement de l'aide, il exigeait qu'Apple crée une porte dérobée dans le iPhone. Apple était mal à l'aise avec cette demande parce qu'elle ne facilitait pas l'accès uniquement à ce téléphone, mais à tous les iPhone, et à quiconque pouvait obtenir cette technologie, plutôt que seulement Apple et le FBI. Le PDG d'Apple, Tim Cook, a résumé les inquiétudes de la société en déclarant « cette porte dérobée ne pourra pas être réservée seulement aux bonnes gens ».

Le FBI a fait appel aux tribunaux et a obtenu une ordonnance obligeant Apple à se plier à sa demande. Apple a fait appel de cette décision, mais le FBI a annoncé qu'il n'avait plus besoin d'elle après avoir réussi à accéder au téléphone avec l'aide d'un tiers. Ce débat se déplace maintenant sur un terrain nouveau et incertain, puisque le FBI connaît désormais une faille de sécurité qui, en théorie, affaiblit les appareils d'Apple partout dans le monde.

Apple n'est pas le seul fabricant de téléphones à être confronté à ce problème. Vers la fin de 2015, BlackBerry faisait face à des demandes du gouvernement pakistanais pour accéder aux données d'un utilisateur de BlackBerry, y compris ses courriels et ses messages du BBM. BlackBerry a déclaré préférer se retirer du marché du Pakistan plutôt que permettre un accès de ce type. Finalement, le gouvernement pakistanais a reculé et BlackBerry pourra continuer à mener ses activités au Pakistan.

Les cas d'Apple et de BlackBerry mettent l'accent sur le fait que ces sociétés de technologie sont très réticentes à accepter des compromis sur les questions de confidentialité. Ces sociétés de technologie, y compris Apple, prennent même des mesures pour ne plus avoir accès aux appareils de leurs propres clients, rendant volontairement plus difficile la tâche de se plier aux demandes officielles d'accès. Bien qu'elles considèrent probablement cette décision comme la plus juste, leur plus grande motivation pour adopter de telles mesures est sans doute qu'elles reconnaissent l'importance de leur engagement envers le respect de la vie privée, le succès de leurs produits et la valeur de la marque. Compromettre cet engagement à respecter la vie privée pourrait en revanche nuire à la confiance envers le produit. Ceci pourrait provoquer une baisse du volume de ventes et des recettes qui, à leur tour, auraient une incidence directe sur le rendement de l'action. Ce lien direct entre la protection de la vie privée et le cours de l'action explique pourquoi les investisseurs devraient être informés des conséquences possibles de ce que représente le cas opposant Apple et le FBI.

Encore une intrusion

L'autre aspect du risque d'atteinte à la vie privée que doivent gérer les sociétés concerne les renseignements confidentiels fournis par leurs clients et qu'elles doivent conserver. Il peut s'agir d'un nom et d'une adresse, des données de carte de crédit et d'information sur la santé et le style de vie. Comme mentionné précédemment, les sociétés ont l'obligation de protéger les renseignements personnels qu'elles collectent, mais malheureusement, il arrive de plus en plus souvent que ces renseignements soient dévoilés, soit parce qu'une société les a divulgués par mégarde ou plus souvent, parce que des pirates ont pénétré les systèmes de la société. Nous sommes tous très préoccupés, en tant que particuliers, par le vol d'identité notamment, mais les sociétés s'inquiètent aussi, car une violation de données confidentielles peut porter atteinte à la marque et aux ventes et donner lieu à des coûts directs importants.

À titre d'exemple récent, le détaillant Target a montré à quel point une telle violation peut nuire à l'avenir d'une société. En décembre 2013, en pleine saison des fêtes, Target a découvert une intrusion dans ses systèmes qui exposait les données détaillées sur environ 40 millions de cartes de crédit et de débit. Les conséquences pour la société ont été immédiates et elles se font encore sentir après deux ans. Target a dépensé 61 millions de dollars au cours des deux premiers mois pour couvrir les dommages causés par cette intrusion et les ventes étaient de 46 % inférieures à celles de la même période l'année précédente. Target a réglé une réclamation de Visa au montant de 67 millions de dollars pour compenser une partie des coûts de réémission des cartes et elle versera sans doute la même somme à MasterCard. De nombreuses autres réclamations de la part d'émetteurs de cartes sont encore en suspens.

Bien qu'il soit relativement simple de déterminer les coûts directs d'une société victime d'une telle intrusion, il est plus difficile de quantifier les effets sur la réputation et la marque d'une entreprise. Ils sont souvent établis par la manière dont la société gère ce type de violation et par l'initiative dont elle fait preuve pour répondre aux inquiétudes de ses clients. Une enquête[1] menée en 2015 a révélé que l'événement le plus préjudiciable pour la réputation d'une marque était la violation de données; viennent ensuite un mauvais service à la clientèle et un désastre environnemental. Pour une société comme Target, qui évolue dans le secteur extrêmement compétitif de la vente au détail, une violation de renseignements personnels peut être désastreuse. Target n'est toutefois pas la seule victime. Des sociétés telles que Home Depot, Sony, Sears, JP Morgan Chase et plusieurs autres ont subi des

[1] The Aftermath of a Mega Data Breach: Consumer Sentiment, Enquête menée par le Ponemon Institute et commanditée par la Experian's Data Breach Resolution Unit.

violations similaires. Elles sont si nombreuses, en fait, que les spécialistes de la sécurité considèrent aujourd'hui qu'il existe deux types de sociétés : celles qui savent avoir été victimes d'une intrusion et celles qui l'ignorent. Certains signes laissent croire que le préjudice d'une intrusion dans les systèmes d'une société sur le cours de son action s'atténue à mesure que les cas se multiplient. Il semble qu'à chaque nouvelle annonçant une autre violation de la vie privée, le public en général et les actionnaires réagissent de moins en moins; ce n'est plus tant un « événement » qu'un simple coût associé à l'exploitation d'une entreprise.

En plus des exigences réglementaires et des enjeux de sécurité nationale, un engagement à protéger la vie privée est devenu un élément important de la marque et de la réputation de toutes les sociétés. Quand le lien de confiance entourant la vie privée est brisé, il peut être bien difficile et coûteux de le rétablir. Il est important de souligner que pour les investisseurs, ceci peut avoir des conséquences directes sur la performance d'une société.

Date de publication : le 15 avril 2016

Gestion mondiale d'actifs