LE TEMPS

FILE PHOTO: Commuters pass a British Airways advert on the tube at Canary Wharf station in London, Britain September 7, 2018. REUTERS/Kevin Coombs -/File Photo

OPINION

Les données personnelles: de l'eldorado à la marée noire

OPINION. Les sanctions prononcées contre British Airways et Marriott forcent à revoir la manière dont la possession des données personnelles doit être conçue: au-delà d'un actif, c'est une charge, un passif pour les entreprises, affirme Alexandre Jotterand, avocat, étude id est avocats Sàrl

4 minutes de lecture

Forum **Technologies**

Alexandre Jotterand, avocat, étude id est avocats Sàrl
Publié jeudi 11 juillet 2019 à 15:36, modifié jeudi 11 juillet 2019 à 15:38. **ABONNÉ**

L'autorité anglaise de contrôle en matière de données personnelles – l'ICO – frappe fort, en annonçant à quelques jours d'intervalle vouloir imposer des amendes record à British Airways d'abord, pour 183 millions de livres (226 millions de francs suisses), puis à Marriott International, pour 99 millions de livres (122 millions de francs suisses).

Au-delà de leur montant (qui doit encore être confirmé), ces deux amendes ont en commun de ne pas sanctionner la manière dont ces entreprises ont collecté les données, ni la manière dont elles les ont traitées, mais l'insuffisance des mesures qui ont été prises pour les sécuriser.

La sécurité des données

La réglementation européenne sur la protection des données (le fameux RGPD) impose en effet aux entreprises de mettre en œuvre «les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque». Cette obligation n'est certes pas nouvelle, mais le RGPD impose désormais aux entreprises victimes d'une fuite de données d'en informer l'autorité compétente dans les 72 heures qui suivent la découverte de l'incident, et donc d'annoncer la potentielle violation de leur obligation de sécurité, avec à la clé des amendes pouvant atteindre 4% du chiffre d'affaires annuel.

essage envoyé par les autorités est clair: les entreprises
responsables des données personnelles qu'elles
nnent et ont l'obligation de les protéger »

Si les sanctions annoncées par l'ICO sont à ce jour les plus lourdes, elles ne sont pas les premières prononcées à la suite d'une fuite de données. Début juin 2019, l'autorité française de protection des données – la CNIL – a en effet prononcé une amende de 400 000 euros (445 000 francs suisses) contre SERGIC, après la découverte d'une faille de sécurité affectant le site web de cette régie immobilière française. Si le montant est d'apparence plus modeste, il reste important en proportion du chiffre d'affaires de l'entreprise (plus de 0,9%, contre 1,5% pour British Airways et 3% pour Marriott).

Le message aux entreprises

Le message envoyé par les autorités de contrôle avec ces amendes est clair: les entreprises sont responsables des données personnelles qu'elles détiennent et ont l'obligation de les protéger en y affectant les ressources nécessaires. Il s'agit là d'un changement de paradigme. Les données personnelles – souvent qualifiées «d'or noir du XXIe siècle» – sont en effet généralement conçues comme un actif bon marché. La raison: les données brutes sont abondantes, gratuites ou presque, et une fois amassées en quantité, raffinées, puis agrégées, peuvent être commercialisées.

Les sanctions prononcées par les autorités de contrôle forcent à revoir la manière dont la possession des données personnelles doit être conçue par les entreprises: au-delà d'un actif, c'est une charge, un passif pour les entreprises. Leur détention doit ainsi être conçue selon une approche basée sur le risque – risque juridique, économique et réputationnel, contre lequel il faut se prémunir – et qui se matérialise souvent en cas de fuite de données. Pour reprendre l'image de «l'or noir», les fuites de données sont aujourd'hui ce que les marées noires sont au pétrole, à la différence près que les entreprises dont la cargaison contient des données doivent naviguer dans un océan truffé de pirates souvent sophistiqués et disposant de ressources importantes, le tout dans un cadre légal rigoureux.

Un changement de paradigme

Protéger les données stockées de manière appropriée (vision sécurité) devient, dans cette perspective, aussi important que de les collecter et les utiliser conformément aux exigences légales (vision réglementaire). Dans ce cadre, respecter ses obligations après la survenance d'une fuite de données est certes nécessaire d'un point de vue réglementaire, mais insuffisant d'un point de vue sécurité si la fuite de données pouvait (ou devait) être évitée. Ainsi, dans le cas de British Airways, la compagnie aérienne a notifié sans délai l'incident après l'avoir constaté, puis a pleinement collaboré avec l'ICO et adapté ses systèmes de sécurité, conformément aux exigences réglementaires. Cela n'a pas retenu l'ICO d'annoncer son intention d'infliger cette amende record au motif que British Airways n'avait pas appliqué le soin et la rigueur nécessaires à la protection des données de ses clients.

Lire aussi: Le RGPD, la révolution du consentement

Le RGPD (et ses sanctions) peut sembler une problématique lointaine pour les entreprises suisses (à tort ou à raison suivant lesquelles). Cela étant, le changement de paradigme concernant la conception des données personnelles – d'une ruée vers l'or à la crainte d'un scandale à l'image de la survenance d'une marée noire – dépasse les frontières de l'Union européenne. Pour les entreprises suisses également, il n'est plus envisageable de concevoir les données personnelles simplement comme un actif, ou d'approcher la protection des données comme un problème réglementaire uniquement. Il faut repenser la manière dont les données personnelles sont conçues et prendre en compte le risque associé à leur possession.