Le rapport 2020 de la *Federal Trade Commission* américaine en matière de *Privacy and Data Security*

Célian Hirsch, le 14 septembre 2021

Dans son rapport 2020 sur la *privacy and data security*, la *Federal Trade Commission* américaine offre un aperçu de ses récentes décisions en la matière.

La *Federal Trade Commission* américaine (FTC) a notamment pour mandat de surveiller le respect de la *Section 5* du *Federal Trade Commission Act*, lequel interdit les « *unfair or deceptive practices in the marketplace* ». Pour cela, elle doit vérifier le respect de diverses législations fédérales, à défaut de l'existence d'une seule législation en la matière. La FTC a dû modifier son approche d'*enforcement* afin de prendre en compte la *privacy and data security* en raison des développements de nouvelles technologies et de nouveaux modèles d'entreprises.

Dans son rapport 2020 sur la *Privacy and Data Security*, la FTC livre notamment des résumés de ses affaires relatives à la protection de la vie privée et à la cybersécurité. Nous en évoquons ci-dessous quelques-uns.

En avril 2020, un accord entre la FTC et Facebook a été confirmé judiciairement. Il s'agit de l'amende la plus importante jamais imposée en matière de *privacy* : Facebook a dû payer USD 5'000'000'000.-. En violation d'un ordre de la FTC de 2012, la firme californienne a non seulement communiqué de fausses informations à ses utilisateurs sur leur capacité de contrôler leurs données, mais elle n'a également pas mis en place de garanties suffisantes en faveur de la protection des données. Par ailleurs, le réseau social n'a pas indiqué qu'il utiliserait les numéros de téléphone fournis par ses utilisateurs pour l'authentification à deux facteurs afin de les cibler avec de la publicité.

En novembre 2020, la FTC s'en est prise à Zoom. Cette société, bien connue depuis mars 2020, affirmait de manière trompeuse que les communications entre utilisateurs étaient cryptées. Par ailleurs, l'installation de Zoom sur un ordinateur Mac entraînait l'installation d'un programme annexe permettant de déjouer la protection offerte par Safari. Ce programme tiers demeurait installé, même si le logiciel Zoom était par la suite désinstallé. En raison de ces manquements, Zoom doit demander à un tiers indépendant d'établir un rapport d'audit bisannuel sur son programme sécurité et notifier à la FTC tout *data breach*.

En plus de ces deux cas importants, la FTC a ouvert plusieurs procédures contre des sociétés qui certifiaient, de manière erronée, disposer d'une bonne sécurité des données. À titre exemplatif, *Tapplock* prétendait que ses serrures intelligentes connectées à Internet étaient incassables. *SkyMed Internionall Inc.* a affirmé, à tort, que des données médicales de 130'000 clients n'étaient pas librement accessibles, alors qu'elles avaient été déposées sur un *cloud* non sécurisé. Pour sa part, *Ascension Data & Analytics LLC* a transmis les données de ses clients à un sous-traitant, lequel avait également mal configuré ses accès *cloud*. Or, en vertu du droit financier américain, la société devait s'assurer que son sous-traitant protégeait de manière appropriée les données qui lui étaient confiées.

D'autres procédures de la FTC concernent l'application du *Fair Credit Reporting Act*. Cette législation établit des exigences pour les entreprises qui utilisent des données pour déterminer la solvabilité, l'éligibilité à l'assurance, l'aptitude à l'emploi et pour sélectionner les locataires. *Mortgage Solutions FCS* a par exemple été amendée pour avoir révélé des données clients dans ses réponses aux posts critiques publiés sur Yelp. *National Landmark Logisitics* utilisait des *robocalls* pour laisser des messages trompeurs indiquant aux personnes qu'elles faisaient l'objet d'un audit ou d'une procédure et qu'elles allaient recevoir des documents à leur domicile ou à leur travail. Les *robocalls* menaçaient les personnes de poursuites judiciaires s'ils n'effectuaient pas immédiatement un paiement. Une autre société de recouvrement de créances (*Midwest Recovery Systems*) a également été amendée pour avoir ajouté des dettes fictives ou très douteuses dans les dossiers de crédit des clients afin de les contraindre à les payer.

Enfin, en matière de *privacy and data security,* la FTC s'occupe également de vérifier la bonne mise en œuvre des mécanismes internationaux de transfert de données, tels que le *EU-U.S. Privacy Shield Framework*, le *Swiss-U.S. Privacy Shield Framework* et le *Asia-Pacific Economic Cooperation Cross-Border Privacy Rules System* (cf. swissprivacy.law/17/). Elle a ainsi sanctionné diverses entreprises pour n'avoir pas respecté ces mécanismes ou avoir allégué à tort de les avoir rejoints.

Rompu au RGPD, le lecteur européen sera toujours étonné de la diversité des lois et des règles américaines en matière de *privacy and data security*. Il devrait néanmoins garder un œil attentif aux développements outre-Atlantique. En effet, même si les règles divergent, nos préoccupations en matière de protection et de sécurité des données sont proches. Les décisions de la FTC peuvent ainsi être d'une précieuse aide afin de mieux respecter et répondre aux attentes des consommateurs européens.

Proposition de citation : Célian HIRSCH, Le rapport 2020 de la *Federal Trade Commission* américaine en matière de *Privacy and Data Security*, 14 septembre 2021 *in* www.swissprivacy.law/90

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.