Condamnation de Marriott pour une fuite de données

Célian Hirsch, le 9 avril 2021

Dans sa *Penalty Notice*, l'*Information Commissioner's Office* anglais sanctionne le groupe hôtelier Marriott pour n'avoir pas pris les mesures de sécurité adéquate (art. 32 RGPD). Ses manquements ont permis à des pirates d'obtenir les données d'environ 339 millions de clients.

Information Commissioner's Office, Penalty Notice COM0804337 du 30 octobre 2020 contre Marriott International Inc.

En septembre 2018, Marriott découvre que le système informatique de Starwood, l'une de ses filiales, a été infiltré par des pirates. Cette société avait été acquise en 2016. Or, grâce à un *web shell*, les pirates ont pu accéder en 2014 déjà au système de Starwood et y installer un *remote access trojan*.

Contrairement aux assurances reçues et à deux *Reports on Compliance* remis avant l'acquisition de Starwood par Marriott, ce système n'était pas protégé par une authentification à facteurs multiples.

C'est uniquement en septembre 2018, lorsque les pirates ont profité de leur accès à Starwood afin de tenter d'accéder aux données des cartes de crédit des clients de Marriott, que le système d'alerte *Guardium* a détecté l'attaque. En effet, ce système surveillait uniquement les données de cartes de crédit. Le piratage d'autres données ne pouvait ainsi pas être repéré par *Guardium*.

Suite au repérage de cet incident, Marriott a activé son *Information Security and Privacy Incident Response Plan* le 9 septembre 2018 afin de procéder à une analyse forensique. Le 22 novembre 2018, elle a informé l'*Information Commissioner's Office* (ICO), l'autorité britannique de protection des données, de cette fuite de données. Quelques jours plus tard, Marriott a mis en place un site Internet dédié à l'information sur cet incident. En résumé, les pirates ont pu obtenir des données d'environ 339 millions de clients.

Dans sa décision, l'ICO reconnaît en premier lieu qu'elle ne peut pas sanctionner Marriott pour n'avoir pas mis en place une authentification à facteurs multiples. En effet, Marriott avait reçu deux *Reports on Compliance* avant l'acquisition de Starwood lui certifiant qu'un tel

procédé avait été mis en place. Elle pouvait ainsi légitimement se fonder sur l'existence d'une telle mesure de sécurité.

Cela étant, l'ICO reproche à Marriott quatre violations distinctes du principe de sécurité du traitement (art. 32 RGPD).

Premièrement, Marriott n'a pas suffisamment surveillé les comptes privilégiés. Bien qu'il ne puisse pas lui être reproché de ne pas avoir été consciente de l'absence d'une authentification à facteurs multiples, la société aurait dû mettre en place d'autres dispositifs de sécurité afin de pouvoir repérer les pirates dans le système. Elle aurait notamment pu l'effectuer avec un suivi des logs. Cela lui aurait permis de constater que les pirates utilisaient des comptes légitimes afin d'effectuer des actes non autorisés.

Deuxièmement, Marriott n'a pas suffisamment surveillé sa base de données. La limite de la surveillance du système d'alerte *Guardium*, à savoir les données de carte de crédit, démontre que Marriott ne pouvait repérer les activités délictueuses que de manière limitée. Même si une approche fondée sur le risque justifie une protection plus importante de ces données, cela ne permet pas pour autant de ne pas protéger d'une manière équivalente les autres données personnelles.

Troisièmement, Marriott n'a pas suffisamment contrôlé ses systèmes critiques. Le groupe hôtelier aurait notamment pu intégrer une liste blanche, à savoir que seulement certaines adresses IP ou certains appareils pouvaient avoir accès à certaines parties du système. Selon l'ICO, un tel système devrait être mis en place pour les appareils qui peuvent se connecter à distance au système informatique. Le *National Institute of Standards and Technology* considère d'ailleurs que les listes blanches sont plus efficaces que les logiciels antivirus.

Quatrièmement, Marriott n'aurait pas dû crypter uniquement les données de carte de crédit, mais également d'autres données, en particulier celles relatives à l'identité.

Enfin, l'ICO souligne qu'il n'est pas suffisant de mettre en place une page Internet et de publier à large échelle un communiqué de presse afin d'informer les personnes concernées. En effet, l'art. 34 al. 3 let. c RGPD prévoit qu'une « communication publique » n'est mise en œuvre que lorsque l'information directe « exigerait des efforts disproportionnés ». Or, en l'espèce, l'envoi de courriel aux personnes concernées était possible puisque Marriott disposait en principe des adresses électroniques des personnes concernées. Le communiqué de presse était ainsi suffisant uniquement pour les personnes dont le groupe hôtelier ne disposait pas d'adresse électronique.

Dans la seconde (importante) partie de sa décision, l'ICO justifie le montant de l'amende imposé à Marriott au sens de l'art. 83 RGPD, à savoir £18'400'000. Pour ce faire, elle procède en quatre étapes.

Elle enlève d'abord les éventuels gains résultant de la violation du RGPD (il n'y en a pas en l'espèce).

Dans la deuxième et troisième étape, l'ICO examine les critères expressément mentionnés à l'art. 83 par. 2 RGPD. L'autorité souligne notamment que Marriott est complètement responsable de cette fuite de données (art. 83 par. 2 let. d RGPD), qu'elle a entièrement collaboré avec l'ICO (art. 83 par. 2 let. f RGPD) et que la fuite concernait des données non cryptées de passeport ainsi que des données de carte de crédit (art. 83 par. 2 let. g RGPD).

Dans la quatrième étape, l'ICO examine d'autres facteurs pertinents, notamment le fait que l'amende doit avoir un caractère dissuasif (art. 83 par. 1 *in fine* RGPD). Dans la cinquième et dernière étape, elle examine les éventuels motifs justifiant une réduction du montant de l'amende (art. 83 par. 2 let. k RGPD), notamment la situation liée à la crise du coronavirus.

Cette décision rappelle que les exigences découlant du principe de sécurité (art. 32 RGPD ; art. 7 LPD ; art. 8 nLPD) sont particulièrement élevées. Même si une fuite de données ne permet pas nécessairement de conclure que ce principe n'a pas été respecté, il semble que les autorités européennes découvrent facilement, *a posteriori*, certaines lacunes dans la sécurité informatique du traitement.

En droit suisse, les conséquences d'une violation du principe de sécurité ne nous semblent pas aussi importantes qu'en droit européen. Non seulement le Préposé ne peut (et ne pourra) pas imposer d'amende, mais les personnes affectées par la fuite peineront probablement à prouver un éventuel dommage. Cela étant, dans la nLPD, une violation intentionnelle des « exigences minimales en matière de sécurité des données » sera punie pénalement (art. 60 let. c nLPD). Afin de prouver l'élément subjectif, le ministère public devra probablement procéder à la délicate distinction entre le dol éventuel et la négligence consciente ; seul le premier pourra permettre l'application de la disposition pénale pertinente (cf. ég. ROSENTHAL David, Das neue Datenschutzgesetz, in : Jusletter 16 novembre 2020, N 195).

Proposition de citation : Célian HIRSCH, Condamnation de Marriott pour une fuite de données, 9 avril 2021 *in* www.swissprivacy.law/68