Le dommage moral en raison d'une fuite de données ? EUR 2'500.- !

Célian Hirsch, le 10 février 2022

Le *Landgericht* de Munich a condamné un responsable du traitement à payer EUR 2'500.- comme dommage moral à un client en raison d'une fuite des données, en plus du dommage matériel que le client pourra éventuellement subir à l'avenir.

Landgericht München, 31. Zivilkammer O 16606/20 vom 9 Dezember 2021

Scalable Capital GmbH, une FinTech allemande, octroie à Codeship Inc., une société spécialisée en *Software as a Service*, un accès complet à son système informatique. Malgré la fin de la relation contractuelle en 2015 entre ces deux sociétés, Codeship continue à avoir accès aux archives de la FinTech.

Or, entre 2019 et 2020, une cyberattaque contre Codeship permet aux assaillants d'accéder aux archives de Scalable Capital, en particulier à 389'000 documents de 33'200 clients.

Ces documents contiennent diverses données clients : prénom et nom, titre, adresse, adresse électronique, numéro de téléphone portable, date de naissance, lieu et pays de naissance, nationalité, situation familiale, résidence fiscale et numéro d'identification fiscale, numéro IBAN, copie d'une pièce d'identité et photo portrait prise lors de la procédure d'identification.

Mécontent que ses données personnelles aient été compromises, un client intente une action contre la FinTech allemande auprès du *Landgericht* de Munich. Il exige que Scalable Capital soit condamnée à réparer son dommage futur. Il demande également l'octroi d'une indemnité pour dommage moral dont le montant est laissé à l'appréciation du juge.

Afin de justifier sa prétention, le client invoque l'art. 82 par. 1 RGPD. Cette disposition prévoit que

> « [t]oute personne ayant subi un dommage matériel ou moral du fait d'une violation du [RGPD] a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi. »

Pour sa défense, la FinTech affirme qu'elle n'a pas violé le RGPD. En effet, l'origine de la fuite se trouve auprès de la société Codeship. Scalable Capital ne serait donc qu'une victime collatérale de cette cyberattaque. Par ailleurs, non seulement la société allemande bénéficierait d'un système informatique sûr, mais en plus il serait certifié selon diverses normes internationalement reconnues.

Le *Landgericht* de Munich rétorque à la FinTech qu'elle aurait simplement dû bloquer les accès de Codeship après la fin de la relation contractuelle. L'omission de la suppression des accès de 2015 jusqu'à la cyberattaque en 2019 constitue ainsi une violation de la sécurité du traitement au sens de l'art. 32 RGPD. Preuve en est d'ailleurs que Scalable Capital a supprimé tous les accès à ses archives précisément après la cyberattaque.

Le *Landgericht* de Munich constate ensuite qu'il existe un lien de causalité entre cette violation du RGPD et le dommage (tant matériel que moral) invoqué par le client. Il souligne que la fuite concerne de nombreuses données. Or les dommages-intérêts doivent être dissuasifs (art. 83 par. 1 RGPD par analogie). Partant, il condamne la FinTech à payer à la demanderesse EUR 2'500.- à titre de dommage moral. La société allemande devra également dédommager le client de tout dommage futur.

Même si le montant octroyé est, en absolu, relativement bas, il a toutefois son importance.

Premièrement, cet arrêt est probablement le premier à octroyer un dommage moral (au sens de l'art. 82 par. 1 RGPD) à la suite d'une fuite de données. Il rejoint par ailleurs les autres arrêts qui considèrent que l'octroi d'une indemnité pour dommage moral, au sens de l'art. 82 RGPD, n'est pas dépendante de la gravité de l'infraction (cf. swissprivacy.law/35/). La Cour de justice de l'Union européenne (CJUE) a d'ailleurs été saisie de cette question par l'*Oberste Gerichtshof* d'Autriche afin d'apporter quelques clarifications (affaire C-300/21). À notre avis, il y a de fortes chances que la CJUE retienne une notion large de dommage moral au sens de l'art. 82 RGPD (cf. consid. 146 du RGPD).

Deuxièmement, l'Union européenne connaitra, dès la fin de cette année 2022, le régime des « actions représentatives » (Directive 2020/1828). Des actions « de masse » sont ainsi prévisibles après une importante fuite des données. En outre, il semblerait que le financement de procès par des tiers gagne en importance, ce qui risque d'augmenter encore le nombre de litiges en la matière. Le client de la FinTech allemande aurait d'ailleurs précisément bénéficié d'un tel financement.

Comme nous l'avions déjà souligné (cf. swissprivacy.law/35/), la nLPD n'apporte aucune modi-

fication à la notion de dommage. Une fuite des données devrait ainsi porter une atteinte grave à la personnalité afin qu'un tort moral soit reconnu et en conséquence indemnisé (art. 49 CO).

Partant, les tribunaux suisses risquent malheureusement de ne pas reconnaître un tort moral lorsqu'une personne voit ses données personnelles en libre accès sur le dark web à la suite d'une fuite des données. *De lege ferenda*, l'octroi d'une indemnité pour tort moral devrait être octroyée plus facilement, non seulement car les montants restent modestes (et loin de ceux octroyés aux États-Unis), mais en plus car la reconnaissance d'un tort moral correspond au but principal de la responsabilité civile : rétablir la situation qui aurait prévalu sans l'acte illicite.

Proposition de citation : Célian HIRSCH, Le dommage moral en raison d'une fuite de données ? EUR 2'500.- !, 10 février 2022 *in* www.swissprivacy.law/123