Une action civile à la suite d'une cyberattaque

Yannick Caballero Cuevas, le 19 janvier 2024

À la suite d'une cyberattaque ayant touché SolarWinds Corp., la SEC a déposé une action civile contre la société qui aurait trompé les investisseurs sur ses pratiques en matière de cybersécurité. Cette action civile met en évidence, d'une part, les mauvaises pratiques adoptées par la société, et d'autre part, l'importance accrue que la SEC porte sur les informations en matière de cybersécurité que les sociétés publient à l'attention des investisseurs.

Civil Action No. 23-cv-9518 du 30 octobre 2023

Une société divulguant des informations fausses ou trompeuses sur ses pratiques en matière de cybersécurité peut-elle faire l'objet d'une action civile au regard du droit américain ? Et qu'en est-il du droit suisse ? Le présent commentaire examine, dans un premier temps, l'action civile déposée par la *U.S. Securities and Exchange Commission* (SEC) contre SolarWinds Corp., société active dans le développement de logiciels permettant la gestion centralisée de réseaux, de systèmes et d'infrastructures informatiques. Dans un deuxième temps, il présente quelques pistes de réflexion sur comment le droit suisse pourrait aborder un tel état de fait. Bien que cette affaire soit intéressante à plusieurs égards – notamment concernant les standards minimaux qu'une société devrait respecter en matière de cybersécurité et quelles seraient les conséquences en cas de non-respect de ces standards, ou encore les leçons que nous pourrions tirer sur les pratiques à adopter ou à ne pas adopter – nous allons nous limiter à une analyse générale du droit des marchés financiers.

De janvier 2019 à décembre 2020, SolarWinds a été victime d'une cyberattaque, appelée *Sunburst*, qui a utilisé plusieurs failles de sécurité. Les cyberattaquants avaient aussi infecté le logiciel Orion développé par SolarWinds et qui permet à ses utilisateurs de surveiller et gérer leurs réseaux. Ce logiciel était d'ailleurs utilisé par des dizaines de milliers d'entreprises et d'agences gouvernementales. Dès lors, aussi bien SolarWinds que ses clients étaient touchés par la cyberattaque, car les cyberattaquants pouvaient accéder librement aux réseaux des clients au moyen du virus téléchargé dans Orion, et ce pendant plusieurs mois.

Dans son action civile, la SEC reproche à SolarWinds d'avoir trompé les investisseurs sur ses

pratiques en matière de cybersécurité et d'avoir eu connaissance des risques qu'elle encourrait. À l'appui de ses allégations, la SEC dresse une liste de pratiques de SolarWinds en contradiction avec ses déclarations publiques. On y apprend que la société n'a pas maintenu un cycle de développement sécurisé pour ses logiciels, n'a pas imposé l'utilisation de mots de passe forts sur tous ses systèmes, ou encore n'a pas remédié à des problèmes de contrôle d'accès permettant à des acteurs externes d'accéder au VPN de la société. Parmi les exemples les plus effarants, on peut citer l'utilisation de mots de passe par défaut comme 'password' pour ses produits alors que sa politique interne exigeait que les mots de passe soient changés tous les 90 jours, aient au moins 8 caractères incluant au moins des majuscules et minuscules, des chiffres et des caractères non alphanumériques.

Ces vulnérabilités se sont montrées au grand jour lorsque des clients de la société ont été victimes de la cyberattaque. Le 14 décembre 2020, SolarWinds informe à l'aide du formulaire 8-K de la SEC que son logiciel Orion contenait un code malicieux installé par des cyberattaquants dans le cadre d'une attaque de type *supply chain*. Dans les jours qui suivent cette annonce, l'action de SolarWinds chute de plus de 24%.

Fin octobre 2023, la SEC dépose une action civile se fondant notamment sur la *Section 10(b)* du *Securities Exchange Act* [15 U.S.C. § 78j(b)] et la *SEC Rule 10b-5* [17 C.F.R. § 240.10b-5], interdisant à toute personne de commettre une fraude à l'investissement ou de faire des déclarations publiques fausses ou trompeuses qui influencent le cours d'une valeur mobilière. Dans le cadre d'une telle action, la SEC doit démontrer (i) la fausseté des déclarations ou qu'elles étaient incomplètes et trompeuses, (ii) que ces déclarations étaient susceptibles d'influencer un investisseur raisonnable, (iii) que l'auteur a agi avec *scienter* (notion juridique issue du *case law* américain et qui se rapproche de notre notion d'intention sans être pour autant similaire, car le *scienter* englobe également la négligence fautive), et (iv) finalement le dommage. S'agissant du lien de causalité, le *case law* reconnaît une présomption de la causalité en appliquant la *fraud-on-the-market theory*.

Au vu des faits allégués, la SEC considère que les déclarations publiques de SolarWinds étaient fausses et dépeignaient des pratiques en matière de cybersécurité autre que celles qui étaient réellement pratiquées. Selon la SEC, ces déclarations étaient d'ailleurs susceptibles d'influencer un investisseur raisonnable dans sa prise de décision d'investissement, puisqu'un tel investisseur aurait jugé important de connaître la véritable situation en matière de cybersécurité, ainsi que la durée de la cyberattaque.

Partant, nous pouvons conclure que les pratiques en matière de cybersécurité peuvent être

considérées comme des informations importantes pour les investisseurs au regard de la SEC, en particulier si la société est active dans le domaine de la cybersécurité ou du développement de logiciel. De plus, les cyberattaques devraient être annoncées au public à l'aide du formulaire SEC 8-K si elles peuvent avoir un impact négatif sur l'activité de la société, ses clients ou son image commerciale notamment. L'annonce doit d'ailleurs être la plus complète possible et présenter les risques qu'encourent la société, ses clients et investisseurs, sans quoi la déclaration pourrait être considérée comme étant trompeuse. Récemment, la SEC a précisé sa règle adoptée en juillet 2023 sur les incidents de cybersécurité.

Qu'en serait-il si un tel état de fait s'était produit en Suisse ? Plusieurs pistes de réflexion s'offrent à nous, à savoir l'art. 69 LSFin, l'art. 152 CP en lien avec l'art. 41 CO ou le régime de la publicité événementielle.

S'agissant de la responsabilité du fait du prospectus, l'art. 69 LSFin prévoit que tout dommage à la suite d'une information fausse, trompeuse ou non conforme aux exigences légales contenue dans un prospectus, une feuille d'information de base ou toute communication semblable devrait être dédommagé. L'élément important à déterminer est de savoir si les déclarations publiques d'une société sur ses pratiques en matière de cybersécurité peuvent être considérées comme étant une communication semblable. À notre avis, ces informations ne devraient normalement pas être considérées comme des communications semblables, car elles ne sont pas en lien direct avec le prospectus d'émission de l'action. Il pourrait toutefois y avoir une exception si le prospectus se réfère directement à des pratiques de cybersécurité de la société qui opèrerait dans le domaine de la cybersécurité ou du développement de solutions informatiques.

Un autre article intéressant est l'art. 152 CP qui interdit à un cercle limité d'auteurs de donner de faux renseignements au public sur des entreprises commerciales afin que des tiers disposent de leur patrimoine de manière préjudiciable à leurs intérêts. Cet article vise aussi bien à protéger la confiance du public envers les informations diffusées que les intérêts patrimoniaux des investisseurs. Dès lors, constituant une norme de protection du patrimoine, la violation de l'art. 152 CP peut entraîner une action civile au sens de l'art. 41 CO. Pour cela, il faut démontrer que l'auteur – qui doit avoir une des caractéristiques mentionnées à l'art. 152 CP – a donné des renseignements faux ou incomplets notamment au travers de communications publiques ou de rapports et que ces renseignements avaient une importance considérable, en ce sens qu'elles étaient susceptibles de déterminer un investisseur (raisonnable) à disposer de son patrimoine. La réponse à cette question dépendra dès lors du cas d'espèce. Différents éléments entreront en ligne de compte comme le type d'information, à savoir si

elle est générale ou précise, le secteur d'activité de l'entreprise, la relation entre l'information et l'activité de l'entreprise, l'influence que pourrait avoir cette information sur d'autres renseignements sur l'entreprise. L'examen se fera dès lors au cas par cas.

Outre l'annonce prévue par la loi sur la protection des données (cf. art. 24 LPD ; pour plus d'informations sur le devoir d'informer, voir Hirsch, Le devoir d'informer lors d'une violation de la sécurité des données, Schulthess 2023), il est nécessaire de se demander si la société cotée ne devrait pas faire une annonce au sens de l'art. 53 du règlement SIX de cotation. Cette disposition prévoit que l'émetteur informe le marché des faits survenus dans sa sphère d'influence et ayant une influence sur les cours. Tout fait pouvant entraîner des fluctuations de cours supérieures à la moyenne doit être divulgué. En cas de cyberattaques, la réponse – à la question de savoir si la société doit faire une annonce événementielle ou non – dépend notamment de son secteur d'activité, de l'impact direct et indirect que la cyberattaque a sur ses affaires, et des conséquences futures. Dans le cas de SolarWinds, son domaine d'activité était la cybersécurité. De plus, la faille utilisée par les cyberattaquants permettait d'avoir accès aussi bien aux données de SolarWinds qu'à celles de ses clients. En outre, la cyberattaque a duré plusieurs mois, mobilisant ainsi les ressources de SolarWinds. À notre avis, il est très vraisemblable qu'une telle cyberattaque aurait également dû faire l'objet d'une annonce événementielle en droit suisse, notamment en raison de son échelle et sa durée, des conséquences sur les clients, et du potentiel dégât d'image. À noter que SolarWinds a bel et bien fait une annonce auprès de la SEC à l'aide du formulaire 8-K.

Ce bref exposé montre qu'il existe certaines pistes de réflexion en droit suisse en cas de diffusion d'informations fausses ou trompeuses par la société sur ses pratiques internes en matière de cybersécurité ou sur les cyberattaques. Cependant, le régime suisse de la responsabilité civile ne permet pas aisément à l'investisseur lésé d'être dédommagé. En effet, de nombreux obstacles de droit de fond et de procédure se dressent, notamment l'absence d'action collective, la définition d'acte illicite, l'absence de présomption du lien de causalité entre la fausse information et son impact sur les cours, ou encore le calcul du dommage.

Bien que l'indemnisation de l'investisseur lésé semble peu plausible à l'heure actuelle au regard du droit suisse de la responsabilité civile, des exigences de transparence pour la société peuvent découler du régime de la publicité événementielle en cas de cyberattaques. La nécessité d'informer le public au travers d'une annonce événementielle devra être analysée au cas par cas et différents aspects devront être examinés, notamment la nature de la cyberattaque, sa durée, son impact sur les affaires de la société, les ressources que la société devra mobiliser, ou encore les potentielles conséquences légales et réputationnelles.

_swissprivacy.law

Proposition de citation : Yannick CABALLERO CUEVAS, Une action civile à la suite d'une cyberattaque, 19 janvier 2024 *in* www.swissprivacy.law/278