Les sanctions américaines et l'assurance cyberattaque

Célian Hirsch, le 25 octobre 2023

L'assureur qui veut s'opposer au paiement de la prestation d'assurance suite à une cyberattaque, en invoquant les sanctions américaines, doit prouver que la cyberattaque a servi les intérêts d'une entité visée par ces sanctions et qu'il risque ainsi concrètement d'être réprimandé par l'autorité américaine compétente. Le simple fait que le type de logiciel utilisé pour la cyberattaque en question soit habituellement déployé par un groupe de cyberpirates sous sanction *(in casu Evil* Corp) ne suffit pas pour refuser le paiement de la prestation d'assurance.

Arrêt du Tribunal fédéral 4A_206/2023 du 17 août 2023

Comment un assureur peut-il s'opposer à devoir dédommager une société cotée d'un dommage estimé à près d'un million suite à une cyberattaque réussie ? En invoquant que le paiement contreviendrait aux sanctions américaines, car la cyberattaque serait l'œuvre de pirates russes sous sanctions. Le *Handelsgericht* de Zurich, puis le Tribunal fédéral n'ont néanmoins pas été convaincus par cette argumentation .

En juillet 2020, une société cotée au NYSE est victime d'une attaque par le rançongiciel *Wasted-Locker*, lequel chiffre notamment ses données clients. Les cyberattaquants exigent une rançon de 1'500 bitcoins (environ CHF 13,5 millions à l'époque) contre la remise de la clé de déchiffrage. La société paie finalement un montant de probablement 10 millions aux cyberattaquants afin d'obtenir cette clé.

La société se retourne contre l'un de ses assureurs au Royaume-Uni, lequel refuse de payer. L'assureur soutient que l'attaque provient d'Evil Corp, des pirates russes inscrits sur la *Specially Designated Nationals and Blocked Persons-List* (liste SDN) du *U.S. Treasury Department's Office of Foreign Assets Controls* (OFAC). Le paiement de la prestation d'assurance contreviendrait ainsi aux sanctions américaines. L'assureur se fonde en particulier sur la clause contractuelle suivante :

> *SANCTION LIMITATION AND EXCLUSION CLAUSE*
>
> *No (re) insurer shall be deemed to provide cover and no (re) insurer shall be liable to pay*

> *any claim or provide any benefit hereunder to the extent that the provision of such cover, payment of such claim or provision of such benefit would expose that (re) insurer to any sanction, prohibition or restriction under United Nations resolutions or the trade or economic sanctions, laws or regulations of the European Union, United Kingdom or United States of America*.

Saisi par la société, le *Handelsgericht* de Zurich admet la demande en paiement de près d'un million de dollars. Le tribunal considère que l'assureur n'a pas réussi à prouver que l'attaque provenait d'Evil Corp, respectivement qu'Evil Corp aurait profité financièrement de l'attaque. Il serait ainsi hautement improbable que l'assureur soit sanctionné par l'OFAC en cas de paiement de la somme assurée.

L'assureur saisit le Tribunal fédéral, qui est amené à examiner la clause invoquée par l'assureur.

En premier lieu, le simple fait que le logiciel utilisé provienne d'Evil Corp, à savoir une entité inscrite sur la liste SDN, ne suffit pas pour refuser le paiement de l'indemnité. En effet, comme la clause contractuelle l'indique, il est nécessaire pour l'assureur d'établir un risque d'être réprimandé pour violation des sanctions américaines.

En second lieu, le Tribunal fédéral revoit si, comme l'a retenu le *Handelsgericht*, il était hautement improbable que l'assureur soit sanctionné par l'OFAC en cas de paiement de la somme assurée. Le Tribunal fédéral procède à cet examen uniquement sous l'angle de l'arbitraire, puisqu'il s'agit de l'application du droit étranger dans une affaire pécuniaire.

Dans l'arrêt cantonal, le *Handelsgericht* a tout d'abord retenu qu'il n'était pas prouvé que l'attaque provenait d'Evil Corp. En second lieu, il a considéré que chaque déploiement du logiciel *Wasted-Locker* ne constitue pas forcément un « intérêt » d'Evil Corp au sens du droit américain des sanctions (*property or interests in property*). En effet, même si Evil Corp devait être l'auteur de ce logiciel, il n'est pas exclu qu'il soit désormais utilisé par d'autres cyberattaquants, sans qu'Evil Corp en tire un intérêt financier. Enfin, l'OFAC n'a pour l'instant ouvert de procédure ni à l'encontre de la société cotée, ni à l'encontre de la société américaine qui a négocié et payé la rançon, ni à l'encontre des autres assureurs qui ont payé leur prestation en lien avec cette cyberattaque.

Le Tribunal fédéral considère que ce raisonnement résiste à l'arbitraire. Il rejette en particulier l'argument de l'assureur selon lequel toute utilisation de *Wasted-Locker* (même par des

tiers) conduit à une transaction interdite, car Evil Corp participerait à cette transaction soit directement, soit indirectement par le biais de *Wasted-Locker*. Partant, le Tribunal fédéral rejette le recours de l'assureur.

Cet arrêt est intéressant à plusieurs titres et appelle quelques brèves remarques.

Premièrement, il s'agit du premier arrêt du Tribunal fédéral relatif au paiement d'une rançon suite à une cyberattaque. Cette problématique a fait l'objet de récentes publications doctrinales, lesquelles examinent en particulier si le paiement de la rançon, par la victime ou par l'assureur, constitue un acte pénalement répréhensible (cf. Benhamou Yaniv/Wang Louise, Cyberattaque et ransomware : risques juridiques à payer et assurabilité des rançons, RSDA 2023 p. 80 ss ; Sarrasin Delphine/Pangrazzi Sara/Meyer Pauline, The Legal Risks of Ransomware Payments, PJA 2023 p. 1077 ss).

Deuxièmement, cet arrêt rappelle la portée très large des sanctions américaines (cf. ég. Emmenegger Susan/Zuber Florence, To Infinity and Beyond : U.S. Dollar-Based Juristiction in the U.S. Sanctions Context, RSDA 2022 p. 114 ss). Cela étant, le *Handelsgericht* souligne dans son arrêt que l'OFAC n'a publié encore aucune décision en matière de cybersanctions, ce qui ne permet pas de comprendre sa pratique en la matière.

Enfin, l'assureur a échoué *in casu* à apporter la preuve de l'imputabilité de l'attaque à Evil Corp. Le degré de la preuve était pourtant moins élevé qu'en droit suisse, puisque c'est le droit des États-Unis qui s'appliquait comme *lex causae*. Or, celui-ci prévoit un critère de « *more likely than not* » (degré de preuve de la *preponderance*). Malheureusement pour l'assureur, plusieurs cyberexpertises qu'il avait produites ont été jugée comme déposées tardivement par le *Handelsgericht* et donc irrecevables (cf. art. 229 al. 1 let. b CPC).

Ce commentaire est repris de celui du même auteur publié sous cdbf.ch/1303/.

Proposition de citation : Célian Hirsch, Les sanctions américaines et l'assurance cyberattaque, 25 octobre 2023 *in* www.swissprivacy.law/260