Global Security Mag

THE LOGICAL & PHYSICAL SECURITY MAGAZINE

TECHNOLOGIES

SÉCURITÉ

POLITIQUE NATIONALE
Interview de Jérôme Notin
et Jean-Jacques Latour,
Cybermalveillance.gouv.fr

N°51 - Prix : 24 € TTC - Trimestriel : avril, mai, juin 2020

DE QUOI LE ZOOMBOMBING EST-IL LE NOM ?

Par Olivier Iteanu, Avocat à la Cour,
Chargé d'enseignement à l'Université de Paris I Sorbonne

Avec la pandémie de Covid-19 et la crise d'urgence sanitaire qui l'a suivie, la visioconférence a accompagné le confinement de millions de travailleurs. Bien que le service ne soit pas nouveau, son utilisation a littéralement explosé ces derniers mois. On peut d'ailleurs dire aujourd'hui que la visioconférence est devenue la norme pour toutes les réunions entre professionnels, et même au-delà… pour le meilleur et pour le pire !

Les grands gagnants de cet usage massif ont été les éditeurs de ces services et leurs plateformes. Le français Tixeo a tiré son épingle du jeu [1] aux côtés notamment des GAFAM, avec Microsoft et ses deux produits Skype et Teams, ou encore Google Hangouts Meet. Les autres grands éditeurs américains, tels que Cisco et son service Webex, ne sont pas restés les bras croisés… C'est le cas également de la plateforme Zoom. La société californienne éponyme, fondée en 2011, s'est retrouvée projetée sur le devant de la scène par le succès foudroyant de son service, en termes d'utilisateurs. Au même moment d'ailleurs, par les effets du hasard et en dépit de cette période si particulière, elle entrait le 30 avril 2020 au Nasdaq, la plus importante bourse d'actions au monde cotant très majoritairement des entreprises du secteur des technologies de l'information. Il faut dire que la société, fondée par l'ingénieur Eric Yuan, était valorisée à plus d'un milliard de dollars dès 2017. Mais être le premier de la classe n'est pas toujours de tout repos… Au cours de cette même période à succès pour Zoom, diverses insuffisances en termes de sécurité ont été révélées au grand public, dont notamment le très sérieux New York Times s'est fait l'écho. Parmi celles-ci, on observe un nouveau comportement déviant rendu possible par certaines insuffisances de Zoom, appelé le « zoombombing ». Cette pratique consiste à faire irruption dans une réunion en visioconférence à laquelle on n'a pas été convié, d'y injecter des images le plus souvent déplacées, voire racistes, et à enregistrer une vidéo du tout. Le terme est devenu si populaire qu'on l'utilise pour des agissements similaires réalisés sur d'autres plateformes que Zoom. Il est dès lors intéressant de réfléchir à ce phénomène pour voir, d'une part, si le zoombombing est illégal au regard de la loi française et, d'autre part, qui est responsable en cas de fuites de données consécutives à ces agissements.

LE ZOOMBOMBING, EST-CE VRAIMENT ILLÉGAL ?

La réponse est indubitablement affirmative. Le délit pénal commis à coup sûr par le seul fait de faire irruption intentionnellement dans une réunion en visioconférence à laquelle on n'a pas été invité, est le délit d'accès frauduleux de l'article 323-1 du Code pénal : *« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende. »* Ce délit issu de la Loi Godfrain de 1988 est le pendant numérique de la « violation de domicile ». Les conditions de sa commission sont ici remplies. La plateforme de visioconférence est bien le « *système de traitement automatisé de données* » visé par l'article. C'est une notion d'ailleurs entendue au sens très large par la jurisprudence, dès qu'on se trouve en présence d'un matériel qui fonctionne au moyen du numérique et/ou de l'électronique et stocke des données. Dès lors que la visioconférence est destinée à un petit nombre de personnes et qu'elle n'est pas publique, ce qui constitue sa nature profonde car elle ne peut concerner qu'un nombre fini de participants, et que l'intrus n'y est pas invité, il y a bien accès frauduleux au sens de l'article 323-1. Le caractère intentionnel de l'acte, condition du délit, découle de la saisine des identifiants et mots de passe par l'intrus. Enfin, le délit est commis qu'il y ait ou non dommage comme pour une violation de domicile, car c'est bien le seul fait d'accéder frauduleusement qui est sanctionné. Néanmoins, le même article prévoit, en son alinéa 2, un second délit plus lourdement sanctionné, soit les peines maximales de trois ans d'emprisonnement et 100 000 euros d'amende *« Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système… »*. En fonction des circonstances et des faits, d'autres délits pourraient être appelés à la rescousse. Par exemple, l'irruption dans une réunion en visioconférence peut mettre en jeu les données personnelles et le RGPD. En effet, les participants s'identifient, il y a donc là des données personnelles. Les informations échangées et les documents partagés peuvent également concerner de telles données au statut particulier, comme chacun sait. L'article 226-18 du Code pénal punit de cinq ans d'emprisonnement et 300 000 euros d'amende *« Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite … »* [2]. Ainsi, comme on le voit, le

premier nom du zoombombing est bien celui de délit. Il reste à résoudre une seconde question bien plus délicate.

QUI EST RESPONSABLE D'UN POINT DE VUE JURIDIQUE ?

La question de la responsabilité est d'une autre nature que celle de l'illégalité et de la sanction. Dans la première partie, nous avons étudié les moyens légaux pour les victimes, au premier rang desquelles l'organiseur de la visioconférence et les participants, voire l'éditeur de la plateforme, de mettre en marche le système judiciaire, pour identifier l'intrus, le poursuivre en justice, afin qu'il soit sanctionné. La question de la responsabilité induit celle de savoir « qui va payer » si un dommage a été causé. Bien sûr, l'auteur du délit est le premier concerné. Cependant, son identification n'est jamais aisée. Le plus souvent les cybercriminels savent jouer des frontières, ce qui ne facilite pas la tâche des enquêteurs, et à l'arrivée, en l'absence d'un auteur devant les juges, la question de l'indemnisation des victimes n'est pas résolue. Les différents protagonistes se tournent les uns vers les autres pour savoir qui sera responsable : l'organisateur, les participants qui peuvent appartenir à l'organisation ou lui être extérieurs, l'éditeur de la plateforme, voire des tiers extérieurs à la visioconférence piratée, si l'intrusion a révélé des informations les concernant ? Pour répondre à la question, on peut tout d'abord se tourner vers le contrat d'adhésion conclu avec la plateforme, le plus souvent appelé Conditions Générales d'Utilisation (CGU). Sans surprise, ces CGU comportent le plus souvent des clauses limitatives et même exclusives de toute responsabilité. C'est le cas des CGU de Zoom. A l'article 17 de ses CGU (avril 2020), Zoom prévoit que *« en aucun cas, Zoom ou ses sociétés affiliées, fournisseurs ou revendeurs ne seront tenus responsables de quelconques dommages spéciaux, accessoires, indirects … »*, l'éditeur californien ajoutant même, disposition là encore courante, que son client *« … accepte d'indemniser, de défendre et d'exonérer Zoom, ses sociétés affiliées, dirigeants, administrateurs, employés, consultants, agents, fournisseurs et revendeurs de toute réclamation, responsabilité, tous dommages ou frais par ou de tiers (y compris, mais sans s'y limiter, les honoraires d'avocat) découlant de Votre utilisation des Services … »*. Inutile de préciser que ces CGU sont soumises à la Loi de l'État de Californie et aux juridictions du Comté de Santa Clara, selon un système bien rodé, et trop souvent admis par les juges européens. Bien entendu, ces dispositions issues d'un contrat d'adhésion sont contestables, y compris devant les juges européens. Toutefois, la partie n'est jamais gagnée d'avance, et l'organisateur de la visioconférence attaquée risque de se retrouver bien seul face aux participants, si ceux-ci ont subi un préjudice du fait de l'intrusion. En tant qu'organisateur, sa responsabilité sera sans doute engagée, et si la cyberattaque est la conséquence d'une défaillance du système, il devra se battre contre l'éditeur et ses CGU pour obtenir la garantie prévue.

LEGAL BRIEFING

What does zoombombing mean?

By Olivier Iteanu, Avocat à la Cour, Lecturer at the University of Paris I Sorbonne

With the Covid-19 pandemic and the health emergency crisis that has followed, videoconferencing has become the norm during the lockdown of millions of workers. Although the service is not new, its use has grown enormously in recent months. It can be said that videoconferencing is now standard practice for all business meetings and more, from homeworking to interpersonal consumer communications ... for better and for worse!

En conclusion, le zoombombing est le nom d'un délit pénal et le fait générateur d'une action en responsabilité possible contre, en premier lieu compte tenu de sa position mais fonction aussi des circonstances, l'organisateur de la réunion attaquée. Voilà qui nous promet des joutes juridiques de grand intérêt. ■■■

[1] Le 30 avril 2020, à l'occasion d'une audience de plaidoiries en visioconférence, en plein confinement, le Président du Tribunal de commerce de Paris rendait une Ordonnance de référé qui a été remarquée et commentée. Tixeo était la plateforme utilisée par le Greffe du Tribunal sur laquelle les Avocats plaidaient. https://www.legalis.net/jurisprudences/tribunal-de-commerce-de-paris-ordonnance-de-refere-du-30-avril-2020/

[2] Sans compter que la CNIL et ses sanctions administratives pourraient s'en mêler au travers de l'article 32 du RGPD qui prévoit que « le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque … », l'absence de telles mesures pouvant impliquer les sanctions de la CNIL, ici à hauteur au maximum, de 2% du chiffre d'affaires mondial et 10 millions d'euros.