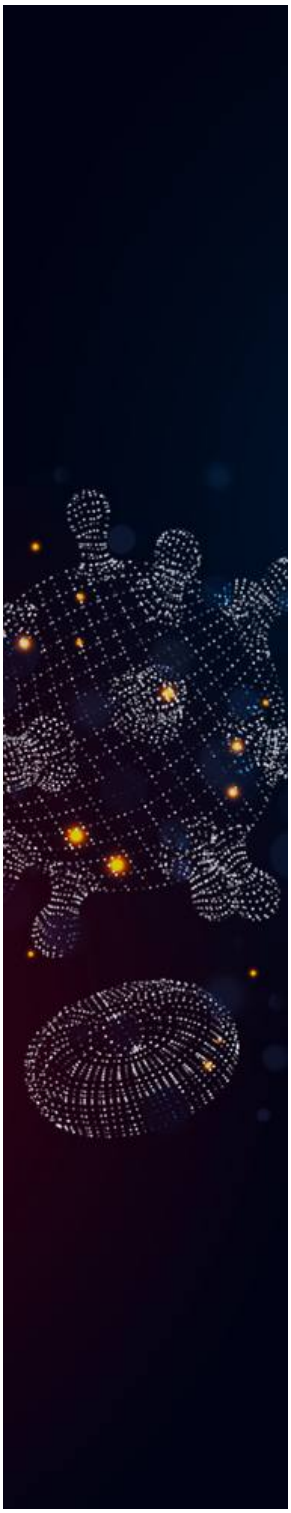


ARTICLE

CYBERSÉCURITÉ ET COVID-19 : PRÉVOIR ET AGIR DANS UN CONTEXTE INÉDIT

IT et données personnelles Droit de la propriété intellectuelle, média et art | 07/04/20 |

PROTECTION DES DONNÉES PERSONNELLES

La pandémie de Covid-19 est une période propice aux cyberattaques en raison du climat d'inquiétude générale et de l'usage accru du numérique. Dans ce contexte, les organisations, et notamment les entreprises, sont des cibles privilégiées. Ainsi, au cours des dernières semaines des cyberattaques ont été observées à travers le monde. Dimanche 22 mars, l'AP-HP a été visée par une attaque DDoS qui a restreint l'accès à ses services pendant plusieurs heures. Dans un autre registre, la société britannique Hammersmith Medicine Research a été visée par une attaque de *ransomware* entrainant le vol de plusieurs fichiers de données. Selon le Cyberpeace Institute, une ONG luttant contre l'insécurité numérique, plusieurs logiciels malveillants circulent par ailleurs actuellement par le biais d'emails de *phishing* contenant des liens ou des pièces jointes infectées qui peuvent affecter l'ordinateur du salarié et potentiellement tout le réseau de son entreprise. Dans un tel contexte la vigilance des entreprises est nécessaire.

La cybersécurité représente d'abord un enjeu important en raison des mesures prises par les autorités nationales visant à endiguer Covid-19, et en particulier les mesures de confinement, qui ont conduit les entreprises à généraliser le télétravail des salariés, parfois dans l'urgence. Or, le travail à distance peut augmenter considérablement les risques de cyberattaque (hameçonnage, piratage de l'accès distant ou de l'équipement du collaborateur, usurpation d'identité, etc.), menaçant ainsi sérieusement la sécurité informatique des entreprises : vol de données, blocage des données contre rançon, fraude et faux ordres de virement etc. Dans ce contexte, le site gouvernemental cybermalveillance.gouv.fr a publié des recommandations de sécurité informatique pour le télétravail en situation de crise où il exhorte les entreprises à renforcer leurs mesures de sécurité pour détecter ou éviter les cyberattaques. Il est ainsi indispensable d'assurer la sauvegarde des données, la mise à jour des logiciels (bureautique, logiciel email, antivirus, etc.), renforcer les accès et les mots de passe (par exemple par l'emploi d'un VPN) ou de sensibiliser ses collaborateurs aux bonnes pratiques[1]. L'ANSSI a publié, dans cette perspective, en octobre 2018 un guide de bonnes pratiques pour le travail à distance : « Recommandations sur le nomadisme numérique ».

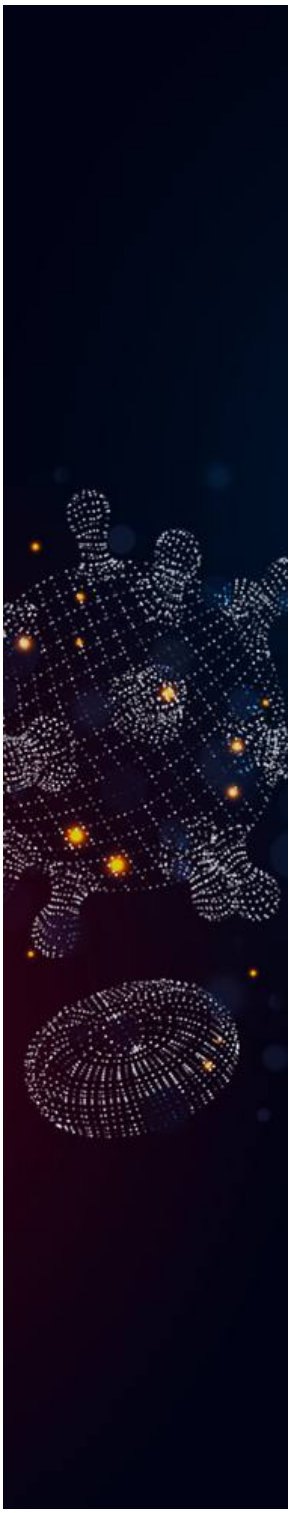
Les entreprises qui seraient victimes de cyberattaques peuvent emprunter la voie pénale pour que les auteurs de ces attaques soient condamnés. A ce titre, les articles 323-1 à 323-7 du Code pénal créés par la loi n° 88-19 du 5 janvier 1988, dite « loi Godfrain », sanctionnent les atteintes aux systèmes de traitement automatisé de données (« STAD »). Parmi les actions contre un STAD, l'article 323-1 du Code pénal sanctionne par exemple l'accès ou le maintien frauduleux dans tout ou partie d'un STAD par deux ans d'emprisonnement et 60 000 € d'amende. Les tribunaux condamnent régulièrement les auteurs de cyberattaques. Par exemple, des attaques de type déni de service, destinées à altérer le fonctionnement d'un site par une saturation de requête ont été jugées comme constituant des entraves au fonctionnement d'un système de traitement automatisé de données, punis et réprimés par l'article 323-2 du code pénal (TGI Paris, 19 mai 2006).

Dès lors qu'une cyberattaque porterait sur des données à caractère personnel et entraînerait une violation de données (ou *data breach*), les entreprises devraient en outre respecter les obligations qui leur incombent en vertu des articles 33 et 34 du RGPD. Pour rappel, une violation de données est « *une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel… ou l'accès non autorisé à de telles données* ». Une violation de sécurité, au sens du RGPD, peut donc être d'origine malveillante ou non, et avoir comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité des données personnelles. Le responsable de traitement doit notifier la CNIL de cette violation, par téléservice, dans un délai de 72h après en avoir pris connaissance, pour les violations entrainant un risque ou un risque élevé pour les droits et libertés des personnes concernées. La notification des personnes concernées ne doit se faire qu'en cas de risque élevé. En tout état de cause, il est nécessaire de documenter en interne, sous forme de registre, l'incident. En cas de non-respect de ces obligations, les sanctions peuvent aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial de l'entreprise.

Attention, le sous-traitant qui traite des données personnelles pour le compte d'un organisme responsable du traitement, a l'obligation de notifier ce dernier de toute violation de données à caractère personnel, par exemple suite à une faille de sécurité, dans les meilleurs délais. A défaut, il engagera sa responsabilité (Art. 33 RGPD).

La CNIL offre une synthèse des actions à prendre en cas de *data breach*. Par ailleurs, en cas de cyberattaque, il faut penser à déposer plainte en parallèle au commissariat de police ou à la gendarmerie la plus proche.

Enfin, au-delà du respect des obligations légales, les obligations de sécurité stipulées dans les contrats informatiques doivent faire l'objet d'une attention particulière dans un contexte propice aux cyberattaques. Ainsi, plusieurs mesures de sécurité sont souvent imposées aux prestataires, parmi lesquelles des obligations relatives au contrôle d'accès et d'authentification du personnel, la gestion des mises à jour et des correctifs de sécurité, la réalisation de tests des systèmes (ex. test d'intrusion), etc. Il est aussi généralement prévu que le client puisse diligenter, ou faire réaliser, un audit de contrôle afin de déterminer le caractère approprié et efficace des mesures organisationnelles et techniques de sécurité. En cas de non-respect de ces obligations, le prestataire engagera sa responsabilité contractuelle qui pourra cependant être limitée s'il existe une clause limitative de responsabilité encadrant la réparation du préjudice indemnisable. Il faut noter que l'intensité de la responsabilité du prestataire dépendra aussi de la qualification des



obligations dans le contrat en obligation de moyen ou de résultat.

Le respect des obligations de sécurité est d'autant plus important que la jurisprudence retient régulièrement la responsabilité du prestataire en cas de cyberattaque, dès lors que toutes les mesures de sécurité raisonnablement envisageables – c'est-à-dire conformes à l'état de l'art – n'auraient pas été mises en place. Il a ainsi été récemment jugé par la Cour d'appel de Paris, dans un arrêt du 7 février 2020 (n°18/03616), qu'un virus informatique type *ransomware* ayant rendu inutilisable des fichiers du client, après l'ouverture d'un email infecté par une employée du prestataire, ne constituait pas un cas de force majeure pour le prestataire (ici absence de sauvegarde régulière des fichiers). En outre, dans un arrêt du 25 mars 2014 (n° 12/07079), la Cour d'appel de Versailles a retenu la responsabilité d'un prestataire de fourniture d'accès, installation et maintenance au réseau téléphonique, pour manquement à des obligations contractuelles de sécurité en ne donnant pas au client les moyens d'éviter le piratage dont il a été victime : *« il appartenait à la société XX, notamment à l'occasion des visites annuelles auxquelles elle devait procéder, de vérifier l'état de sécurisation de l'installation téléphonique de sa cliente et de vérifier que celle-ci utilisait l'installation dans des conditions optimales de sécurité et d'efficacité ; qu'elle devait s'assurer qu'elle était informée de la nécessité de modifier son mot de passe régulièrement »*. La même solution a été retenue par le Tribunal de commerce de Nanterre le 5 février 2015 (n° 2013F00738). Il est donc recommandé aux prestataires informatiques de s'assurer qu'ils respectent bien, surtout en cette période de crise, leurs obligations contractuelles de sécurité. Plus généralement, il convient de rappeler qu'une obligation générale de conseil, de renseignement et de mise en garde pèse sur le prestataire informatique, notamment en matière de sécurité. Par exemple, dans l'arrêt précité rendu par la Cour d'appel de Versailles, les juges ont à ce titre considéré que le prestataire avait « *manqué à ses obligations d'information et de conseil en n'informant pas* [le client] *des risques de piratage et de la nécessité de mettre à jour ses logiciels et de changer ses codes* ». À l'avenir, les prestataires IT peuvent envisager d'adopter la certification ISO/27001 démontrant qu'ils ont mis en place un système de management de la sécurité de l'information (SMSI) efficace.

Article écrit avec l'aide de Sophie DE KERMENGUY

[1] Cybersécurité en entreprise, comment protéger votre patrimoine intellectuel et industriel ? – Renaud Échard – Dalloz IP/IT 2019. 675