Par **Valérie Lafarge Sarkozy** et
Lætitia Daage (ADVANT Altana)

La loi LOPMI et l'indemnisation des pertes et dommages liés à une attaque cyber

De gauche à droite :

VALÉRIE LAFARGE SARKOZY
partner
ADVANT Altana

LÆTITIA DAAGE
avocate
ADVANT Altana

Le nouvel article L. 12-10-1 du Code des assurances entré en vigueur le **24 avril 2023** prévoit que : *« Le versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnée aux articles 323-1 à 323-3-1 du Code pénal est subordonné au dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime. »*

Cette disposition ne concerne que les personnes physiques et morales victimes d'une atteinte à un système de traitement automatisé de données dans le cadre de leur activité professionnelle.

Le texte a évolué très sensiblement depuis l'article 5 du projet de loi initial qui conditionnait uniquement le remboursement des cyber rançons au dépôt d'une plainte dans un délai de 48 heures après le paiement de cette rançon.
Désormais, le texte ne vise plus explicitement la rançon, mais l'ensemble « des pertes et dommages » visés dans le contrat d'assurance et pouvant être indemnisés à la suite d'une cyberattaque, et a étendu le délai pour le dépôt de plainte à 72 heures après avoir eu connaissance de l'attaque.

Les conséquences de cette nouvelle disposition pour les entreprises ayant contracté une assurance cyber sont nombreuses.

En effet, pour voir couverts notamment leurs pertes d'exploitation, frais de remédiation et, a priori, le montant de la rançon qu'elles décideraient de payer, la loi les contraint à une formalité dont la méconnaissance est lourdement sanctionnée puisque la conséquence est la perte du droit à indemnisation.

Étant précisé que cette disposition ne paraît pas pouvoir être écartée par une stipulation contractuelle contraire.
Par conséquent, les entreprises doivent, dans les 72 heures de la connaissance du sinistre, déposer plainte afin d'éviter la sanction prévue par la loi. Ce délai de 72 heures est le même que celui préexistant de la déclaration à la Commission nationale de l'informatique et des libertés (Cnil) en cas de violation de données à caractère personnel, cette absence de déclaration à la Cnil étant assortie de sanctions pécuniaires pouvant aller jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires mondial.

La victime d'une attaque cyber doit donc, alors qu'elle subit les affres de la restauration de son système d'information et de la perte de ses données, impérativement respecter ce délai de 72 heures afin d'éviter de se voir déchoir de son droit à indemnisation et sanctionnée par la Cnil.

Cette plainte peut être déposée dans tous les commissariats ou gendarmeries par un représentant de la société ou une personne dûment habilitée, ou par lettre plainte adressée au procureur territorialement compétent, à savoir celui du ressort du lieu de commission de l'infraction, qui sera le plus souvent le parquet dont dépend le siège social de la société victime.
La plainte pourra également être déposée en ligne lorsque l'application « ma sécurité » sera mise en place par deux décrets du Conseil d'État qui devraient intervenir dans le courant de l'année 2023.

Afin d'éviter toute contestation relative à la découverte de l'attaque, nous conseillons de joindre à la plainte, et de les conserver, tous documents permettant d'en justifier, et de faire établir par un huissier spécialisé un constat qui sera également joint au dépôt de plainte.

On soulignera enfin que si le projet de loi se bornait à viser originellement le « paiement d'une rançon », le texte qui a finalement été adopté par le législateur fait référence aux « pertes et dommages » causés par l'attaque. On s'accorde à considérer que le choix de cette expression vise à donner à la disposition une portée plus large englobant non seulement le montant de la rançon payée, mais aussi les autres possibles conséquences de l'atteinte, telles que les pertes d'exploitation et les coûts de remédiation.