Qu’est-ce que le contrat d’assurance cyber risque ?

Actualité législative publié le **01/03/2023**, vu **1984 fois**, Auteur : La zone du droit

L’espace numérique est un terrain de conflits sans frontière, dont les profondeurs sont parfois si sombres que l’on parle de dark web.

L’espace numérique est un terrain de conflits sans frontière, dont les profondeurs sont parfois si sombres que l’on parle de *dark web. (1)*

Également, avec l’arrivée fulgurante du numérique, les cyberattaques contre les nombreuses infrastructures publiques comme privées connaissent un véritable essor dans le monde plus particulièrement en France. Il ne se passe pas un jour sans que nous n’ayons échos d’une cyber-attaque provenant d’hackers. De nombreux hôpitaux en France ont été victimes de cyberattaque en 2022. L’importance vitale de ces établissements, la sensibilité des données qu’ils hébergent et l’effet médiatique en font des cibles de choix pour les pirates informatiques.

Ces attaques provoquent une violation de données personnelles hébergées dans les différents systèmes informatiques.

La violation de données est définie comme « 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 transmises, conservées ou traitées d’une autre, manière ou l’accès non autorisé à de telles données ».

A titre d’illustration, en septembre 2022, le groupe *Lockbit,* un célèbre groupe de pirates russophones, a officialisé sur son site du Darknet, l’attaque contre le centre hospitalier Sud francilien (CHSF), situé à Corbeil-Essonnes. Avec les ransomwares, les pirates informatiques ont montré qu’ils étaient plutôt du genre à « tirer sur l’ambulance ».

Aussi, l’hôpital de Saint-Dizier et de Vitry-le-François ont été victimes d’un ransomware le 19 avril 22. Les auteurs exigeaient une rançon de 1,2 million d’euros.

Ces cyberattaques font d’énormes victimes en ce sens que les personnes concernées voient leurs données personnelles prises en otage par des individus de très mauvaise moralité.

Les données de santé en dehors de la rançon sont un business lucratif et la quantité d’informations privées que détiennent les hôpitaux, adresse, pathologie, pièce d’identité, carte vitale peut se revendre à bon prix, indique Jérôme Soyer, directeur chez Varonis, société spécialisée dans la cybersécurité.

Une violation de données à caractère personnel risque, si l’on n’intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral tels qu’une perte de contrôle sur leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d’identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données à caractère personnel ou tout

autre dommage économique ou social important.

La question de la couverture des risques cyber a commencé à se poser de plus en plus dans cette société du virtuel voire du numérique.

Ainsi, le projet de loi d'orientation et de programmation du ministère de l'intérieur (LOPMI) est venu fixer l'encadrement juridique des couvertures cyber. (2)

I. Enoncée de la loi

L'Assemblée nationale et le Sénat ont adopté la LOI no 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur.

Le titre II du livre Ier du code des assurances est complété par un chapitre X ainsi rédigé : « CHAPITRE X

« L'ASSURANCE DES RISQUES DE CYBERATTAQUES

« Art. L. 12-10-1. – 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.

« Le présent article s'applique uniquement aux personnes morales et aux personnes physiques dans le cadre de leur activité professionnelle. »

II. – Le I entre en vigueur trois mois après la promulgation de la présente loi.

Ce régime juridique entrera en vigueur à compter du 24 avril 2023.

II. Les conditions pour être indemnisé

Afin d'être indemnisée en cas de cyberattaque, toutes personnes morales et physiques dans le cadre de leur activité professionnelle doivent répondre aux conditions de l'article 5 de la LOPMI (3) :

- D'abord, la personne doit souscrire à un contrat d'assurance cyber risque ;

- L'assuré doit avoir été victime d'une atteinte à un système de traitement automatisé de données ;

- Il doit avoir été victime de pertes et dommages causés par une atteinte à un système de traitement automatisé de données ;

- La victime doit enfin avoir déposé une plainte auprès des autorités compétentes au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime.

III. Que prévoit l’article 5 la LOI no 2023-22 du 24 janvier 2023 d’orientation et de programmation du ministère de l’intérieur.

L’article 5 énumère les différentes atteintes à un système de traitement automatisé de données (STAD), mentionnés aux articles 323-1 à 323-3-1 du code pénal et donnant lieu à indemnisation (4) :

· Art. 323-1 (CP) - Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé ;

· Art. 323-2 (CP) - Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé ;

· Art. 323-3 (CP) - Le fait d'introduire frauduleusement des données dans un système de traitement automatisé (L. no 2014-1353 du 13 nov. 2014, art. 16) «, d'extraire, de détenir, de reproduire, de transmettre, » de supprimer ou de modifier frauduleusement les données qu'il contient ;

· Art. 323-3-1 (CP) - Le fait, sans motif légitime (L. no 2013-1168 du 18 déc. 2013, art. 25) «, notamment de recherche ou de sécurité informatique », d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3.

Les personnes concernées devront ainsi êtres victimes de l’une de ces infractions et remplir les conditions de l’article 5 de la LOPMI pour pouvoir bénéficier de la couverture d’assurance cyber risque. Un exemple d’infraction est celui du crasher - Il rentre dans un système informatique afin de le détruire ou de le saboter. Pour cela, il va utiliser deux moyens principaux : la technique du déni de service ou denial of service.

La technique du déni de service ou denial of service : c’est l’arrêt de toute fonctionnalité informatique. Tel a été le cas dans une affaire ayant occupé le parquet de Paris en juin 2018 et qui concernait l’Office des Postes et de Télécommunication de la Polynésie Française (OPT).

Le parquet de Paris a ouvert une enquête pour déni de service affectant depuis le début de l’année 2018 le principal fournisseur d’accès à internet, le fameux OPT. Il s’agissait d’attaque par réflexion qui est une technique servant à usurper une adresse mail pour interroger un certain nombre de serveurs repartis dans le monde et qui répondront légitiment à cette adresse IP.

Cette adresse IP usurpée sera destinataire d’un nombre important d’informations et sous le poids de cet afflux énorme d’informations venant d’autres ordinateurs arrivera à saturation.

Ce qui aura pour conséquence une défaillance des serveurs informatiques en Polynésie.

Un internaute sous pseudonyme revendiquait sur internet être l'auteur de cette attaque par déni de service et il justifiait ses attaques du fait des tarifs qu'il considérait comme étant trop élevés. Il y avait une très grande distorsion entre les motivations du délinquant et son pouvoir de nuisance. Il demandait ainsi la somme de 300 dollars de bitcoins pour cesser ces attaques.

Des investigations ont été menées par le parquet de Paris qui a lui-même désigné la DGSI sur les éléments techniques qui lui ont été remis par la société victime de cette attaque et uniquement par les constatations de source ouverte. Le cyber-délinquant a finalement été identifié et interpellé au mois de juillet reconnaissant les faits.

Lors de sa garde à vue et de l'enquête, il a indiqué que pour réaliser cette attaque il avait seulement fait une location du temps avec un hébergement d'internet à hauteur de 60 dollars.

Ce sont des attaques peu coûteuses à réaliser et qui peuvent survenir assez fréquemment, mettant ainsi les entreprises dans un état de vulnérabilité. Le constat est que de grands effets néfastes peuvent être causés par l'utilisation de matériels assez simples et accessibles à tous.

IV. Délai pour déposer plainte

La LOPMI rappelle au titre de l'article 5 que toute personne victime pourrait déposer plainte auprès des autorités compétentes au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime.

En outre, les victimes pourront être entendues par la police en visioconférence. En 2023, l'application « Ma Sécurité » lancée début 2022, devra permettre de déposer plainte en ligne et à terme de suivre son traitement.

Les éventuels assurés devront ainsi en cas de cyber attaque touchant leurs données à caractère personnel, s'activer dans le délai imparti pour déposer plainte. Cela passera bien sûr par la réunion des éléments de preuve.

Des sensibilisations devront être faites afin que tant les maisons d'assurance et les potentiels assurés en soient informés sur les modalités de dépôt de plainte et surtout le respect des conditions émises par la LOPMI via son article 5.

Sources :

1. (J.P Vergne et R.Durand, « Cyberespace et organisations « virtuelles » : l'Etat souverain a-t-il encore un avenir ? », Regards croisés sur l'économie).

2. (Loi n° 2023-22 du 24 janv. 2023, art. 5 et 29, JO 25 janv.).

3. Article 5 de la loi n° 2023-22 du 24 janv. 2023, art. 5 et 29, JO 25 janv

4. Articles 323-1 à 323-3-1 du Code pénal