L'ASSURABILITÉ DES CYBER-RANÇONS

Le 7 septembre dernier, le Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique a publié un rapport sur « le développement de l'assurance du risque cyber. »

Force est de constater que les demandes de cyber-rançons se multiplient, de sorte que la question de l'assurabilité de leur paiement s'est posée au Gouvernement.

Si certains assureurs en garantissent le remboursement, d'autres restent silencieux. En effet, le rapport constate que les polices d'assurance traditionnelles de choses ou de responsabilité comportent une « couverture silencieuse » du risque cyber puisqu'elles couvrent les dommages consécutifs à la réalisation d'un risque cyber alors même que cette couverture n'est pas expressément mentionnée dans le contrat et n'est pas prise en compte dans sa tarification.

Or, les « couvertures silencieuses » sont source de difficultés tant pour l'assureur que pour l'assuré :

- L'assureur ne comptabilise pas le risque cyber dans son tarif et ses provisions ;
- L'assuré fait face à une incertitude quant à l'étendue des dommages couverts.

C'est pour cela que le rapport a entendu clarifier le cadre juridique de l'assurance du risque cyber et permettre la sensibilisation des entreprises au risque cyber.

Le même jour que la publication du rapport, le projet de loi d'orientation et de programmation du Ministère de l'Intérieur (LOPMI) a été, pour la seconde fois, présenté en Conseil des Ministres.

S'appuyant sur ce rapport, le Ministère de l'Intérieur a maintenu l'introduction dans le Code des assurances d'un nouvel article ainsi rédigé : « le versement d'une somme en application d'une clause assurantielle visant à couvrir le paiement d'une rançon par l'assuré dans le cadre d'une extorsion prévue à l'article 312-1 du code pénal, lorsqu'elle est commise au moyen d'une atteinte à un système de traitement automatisé de données prévue aux articles 323-1 à 323-3-1 du même code, est subordonné à la justification du dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard 48 heures après le paiement de cette rançon ».

Cependant, les 2 et 15 novembre dernier, les députés ont réécrit cet article. Désormais, l'indemnisation n'est plus conditionnée à une pré-plainte mais à une plainte dans les « 72 heures après la connaissance de l'atteinte par la victime ».

De plus, il n'est plus mentionné explicitement l'assurabilité du paiement des cyber-rançons. En effet, le périmètre de l'article a été élargi à tous les dommages causés par une cyberattaque.

Si le terme « rançon » a été supprimé, le remboursement du paiement d'une rançon semble toujours couvert.

L'ASSURABILITÉ DES CYBER-RANÇONS

Cette proposition reste donc très discutée.

Si l'ACPR a publié le 23 septembre un communiqué en faveur de l'assurabilité des rançons, deux rapports parlementaires ont, quant à eux, proposé d'interdire celle-ci.1

Par ailleurs, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) recommande de ne pas payer la rançon, de même que le Parquet de Paris.

Ainsi, deux parties s'affrontent, celle en faveur de l'assurabilité des rançons et celle en sa défaveur.

Le principal argument en défaveur de l'assurabilité des rançons est celui de l'alimentation d'un circuit criminel. En effet, le paiement de la rançon favoriserait la commission de l'infraction et inciterait les entreprises à moins se protéger contre le risque cyber.

En réponse à cet argument, certains prennent pour exemple l'assurance contre le vol qui n'aurait jamais encouragé le vol, ni incité les assurés à ne pas se protéger.

En autorisant l'assurabilité des rançons, l'Etat entendrait satisfaire l'intérêt des victimes pour lesquelles la récupération des données en échange de la rançon est primordiale.

À cet argument, il est rétorqué que le paiement ne garantirait pas la restitution des données, ni que celles-ci ne seraient pas corrompues. De même, cela pourrait inciter le bourreau à réitérer son acte auprès de la victime.

De plus, en autorisant cette assurance, l'Etat entendrait satisfaire l'intérêt des assureurs pour lesquels la couverture des cyber-rançons remédierait à la situation de désavantage dans laquelle ils se trouvent par rapport au marché européen.

Enfin, cette assurance permettrait, selon certains, une certaine prévention puisque cela pourrait obliger les assurés à prendre des mesures de protection.

En tout état de cause, le projet de loi sera encore étudié par la commission mixte paritaire parlementaire et pourra encore faire l'objet de modifications.

Sarah AUFORT & Léa THUILLIER

[1] Rapp. Sénat, n° 678, 10 juin 2021, relatif à la cybersécurité des entreprises ; Rapp. La cyber-assurance, 13 oct. 2021