Bulletin Juridique Des Assurances
BJDA
Anciennement Actuassurance
www.bjda.fr
LexisNexis®
www.lexisnexis.fr

L'assurance des risques de cyberattaque est (légalement) née !

A. Touzain,

Professeur agrégé, Univ Rouen Normandie, CUREJ, UR 4703

L'assurance des risques de cyberattaque fait, avec la loi n° 2023-22 du 24 janv. 2023, son entrée dans le Code des assurances à compter du 24 avril prochain, dans le nouvel article L. 12-10-1 (joie de la numérotation moderne, qui ne supporte pas les dizaines[1]…).

Ce texte unique était très attendu, ayant pu se nourrir du rapport de la DGT[2], et prévoit que, pour les assurés personnes morales et physiques dans leur activité professionnelle, le versement de l'indemnité d'assurance pour garantir les pertes et dommages causés par une atteinte à un système de traitement automatisé de données (STAD) est subordonné au dépôt de plainte de la victime dans les soixante-douze heures suivant sa connaissance de l'atteinte[3].

Le projet de loi visait quant à lui la seule couverture du « *paiement d'une rançon* », ce qui a été abondamment discuté[4] : les rapports parlementaires privilégiaient une inassurabilité des rançons, afin d'éviter un effet incitatif de leur paiement par la victime (ce qui encouragerait les *hackers*). Cet argument de déresponsabilisation qui rappelle ceux qui étaient opposés à la consécration de l'assurance RC, à la fin du XIXe siècle, était justement critiqué : après tout, l'assurance contre le vol n'est pas soupçonnée d'encourager cette infraction, et les garanties souscrites comprendraient sans doute des exigences de prévention qui permettraient justement de lutter contre les attaques[5]. La loi finalement votée lève les ambiguïtés et confirme l'assurabilité : la France n'interdit donc pas (à l'instar des autres États) la couverture des cyber-

---

[1] Il s'agit de suivre l'art. L. 129-1 en consacrant un « 10 » par référence au numéro du nouveau chapitre consacré à l'assurance des risques de cyberattaques, dans le titre II relatif aux assurances de dommages, du Livre I consacré au contrat d'assurance.

[2] S. Porcher, « L'assurance du risque cyber : quelques recommandations de la Direction générale du Trésor », *Dalloz Actu*, 26 sept. 2022 ; A. Touzain, « *Le développement de l'assurance du risque cyber* : rapport de la Direction générale du Trésor », *bjda.fr* 2022, n° 81.

[3] V. l'analyse de P.-G. Marly, « L'assurance des risques de cyberattaques », *D.* 2023. 112.

[4] V. par ex. P. Berger de Gallardo et P.-O. Leblanc, « Risques cyber : à quelles conditions les entreprises seront-elles assurées ? », *L'argus de l'assurance*, 2 déc. 2022, p. 30.

[5] Sur ces aspects, et le rappel de l'existence, en pratique, des assurances en matière de risque de kidnapping, v. P.-G. Marly, « Vers un encadrement de l'assurance des cyber-rançons ? », *JCP E* 2022. 807. *Adde* P. Pierre, « Assurabilité des sommes extorquées par les rançongiciels : vers une prochaine approbation légale ? », *Resp. civ. et assur.* 2022, alerte 21.

rançons. En revanche, en subordonnant l'indemnisation à une plainte, il s'agit d'inciter les entreprises à les déposer, ce qui permettrait une meilleure connaissance par les autorités de la consistance des cyberattaques. De ce point de vue, le texte paraît tout à fait satisfaisant.

Mais le texte va plus loin, puisque le terme « *rançon* », initialement prévu, a été remplacé par l'expression « *pertes et dommages* », qui est beaucoup plus large et concerne toutes les conséquences d'une cyberattaque, « *telles que les pertes d'exploitation, les coûts de remédiation et le paiement d'une rançon* »[6]. La portée de la règle est considérable : désormais, ce ne serait pas seulement la rançon, mais la totalité des conséquences dommageables dont la garantie serait perdue à défaut de plainte, ce qui rend le « prix » du silence pour l'assuré extrêmement important. Alors que nombre d'entreprises préfèrent rester silencieuses pour ne pas révéler avoir fait l'objet d'une cyberattaque, une telle sanction n'est-elle pas excessive ? Peut-être permettra-t-elle une meilleure acclimatation à la culture du risque cyber. Peut-être conduira-t-elle aussi à un défaut d'assurance : pour une société envisageant de rester discrète sur les cyberattaques, pourquoi souscrire une telle garantie, si elle sait qu'elle ne sera pas couverte à défaut de plainte ? Cette logique de transparence pourrait bien être un frein au développement des assurances cyber… Espérons que cette consécration légale n'en sera pas un acte de décès en pratique.

Le texte :
Loi n° 2023-22 du 24 janv. 2023 d'orientation et de programmation du ministère de l'intérieur, art. 5

I.-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.

[6] P. Linais et O. Lyon Lynch, « LOPMI : un éclaircissement bienvenu sur la légalité de l'assurabilité des cyber-rançons », *JCP G* 2023. Act. 4.