NOTE D'INFORMATION SUR L'ASSURANCE DU RISQUE CYBER

Adoptée en décembre 2022, la loi LOPMI (Loi d'Orientation et de Programmation du ministère de l'Intérieur)[1] a donné la faculté aux entreprises de souscrire une assurance cyber, dont le remboursement en cas d'attaque serait conditionné au dépôt de plainte par la victime dans un délai de 72h.

1. Eléments de contexte

Face à la numérisation croissante de l'économie, **le risque cyber s'est considérablement accru dans les grandes entreprises comme dans les TPE/PME**[2], ces dernières étant particulièrement exposées car insuffisamment sensibilisées ou protégées. Or, avec l'interconnexion grandissante des entreprises, le risque cyber peut générer un effet rebond pouvant impacter l'ensemble des partenaires d'une entreprise attaquée.

Toutefois la question de l'assurabilité du risque cyber est débattue depuis quelques temps.

D'un côté, l'ANSSI et les autorités judiciaires ont longtemps critiqué l'assurance cyber en ce qu'elle pourrait **favoriser les rançongiciels** lorsque les victimes paient, alors même qu'elles n'ont **aucune garantie de récupérer intégralement ou en partie leurs données**. Dans son rapport parlementaire sur la cyber-assurance publié en octobre 2021, la députée Valéria Faure-Muntian allait jusqu'à **préconiser l'interdiction légale pour les assureurs de garantir, couvrir ou indemniser le paiement des rançons**.

D'un autre côté, il est clair que le niveau de cybersécurité global des entreprises doit être renforcé, sachant qu'une cyberattaque peut paralyser plusieurs jours l'activité d'une entreprise avec des conséquences dramatiques en termes financiers ou humains.

2. Enjeux pour les entreprises et conditions de garantie

L'enjeu pour les entreprises était donc de **mettre à disposition du chef d'entreprise un outil pour gérer ce risque** à travers cette assurance cyber.

L'article 5 de la LOPMI vient modifier le code des assurances en intégrant un chapitre X sur l'assurance des risques de cyberattaques. Cet article **rend désormais possible la couverture assurantielle de l'ensemble des risques de cyberattaques sous certaines conditions :**

1. **Un contrat d'assurance doit le prévoir :**
   - Une clause d'un contrat d'assurance, **peu importe qu'il s'agisse d'un contrat d'assurance générale ou d'un contrat spécifique d'assurance cyber**, doit prévoir la couverture d'un risque cyber (pertes et dommages causés par une atteinte à un système de traitement automatisé de données prévue par les articles 323-1 et suivants du Code pénal).
   - L'attaque cyber s'entend largement au sens des articles 323-1 et suivants du Code pénal (accès ou maintien frauduleux sur un système de traitement automatisé de données, entrave ou dysfonctionnement d'un tel système ou atteinte à l'intégrité du système).
   - **La couverture du paiement des rançongiciels**[3] **est rendu possible par la LOPMI**, si le contrat d'assurance le prévoit.

[1] Article 5 de la loi n°2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur

[2] La France est le 3e pays le plus touché au monde par les cyberattaques (avec une hausse de 225% des signalements d'attaques par rançongiciel en 2020 selon l'ANSSI), derrière les Etats-Unis (350 millions de dollars payés en 2020 aux US selon le FBI) et les Royaume-Uni.

[3] Ou *ransomware* : technique de cyberattaque consistant en l'envoi à la victime d'un logiciel malveillant rendant illisibles ses données, le cyberpirate demandant le paiement d'une rançon (généralement sous forme de cryptomonnaie) en échange du mot de passe permettant de déchiffrer / décrypter les données de la victime.

- A noter que la réforme s'appliquera aux futurs contrats d'assurance conclus, mais également aux contrats d'assurance en cours.

2. **Le dépôt d'une plainte dans les 72h de la découverte de l'attaque**
   - A noter que **ce délai de 72h est un délai légal et non une déchéance de garantie du contrat**. Cela signifie que le délai n'est d'une part pas négociable dans les contrats d'assurance et d'autre part peu importe que rien ne soit indiqué dans le contrat quant à ce délai.
   - Le délai commence à courir **à partir du moment où l'assuré a connaissance de la cyberattaque**, c'est-à-dire une fois qu'il est alerté par son prestataire informatique le cas échéant (même si l'attaque s'est déroulée plusieurs jours, voire plusieurs mois auparavant).
   - Attention, **l'entreprise ne doit pas attendre de connaître l'ampleur des conséquences**, pertes ou dommages. Elle doit porter plainte dès qu'elle a connaissance du fait.

3. **La victime doit être une entreprise ou une personne physique agissant dans le cadre de son activité professionnelle**

Par conséquent, il est important de noter que le remboursement par l'assurance ne sera pas automatique et qu'il dépendra du contrat souscrit prévoyant les modalités de couverture.

3. Prochaines étapes

L'article 5 de la LOPMI est **entré en vigueur le 24 avril 2023** (soit trois mois après la promulgation de la loi).

La Direction générale du Trésor (DGTrésor) organise des groupes de travail pour la mise en place de cette assurance cyber.

Le Medef participe à un groupe de travail qui doit définir un **référentiel « d'audit » de sécurité dans les entreprises pour identifier les niveaux de maturité face au risque cyber**. Cela permettra à la fois aux assureurs de mieux évaluer le risque pour déterminer les conditions d'assurance et aux entreprises d'accroître leur niveau de protection pour accéder plus facilement à l'assurance du risque cyber.

Ce référentiel devrait être présenté en septembre 2023.