Les dispositions assurantielles de la LOPMI sont entrées en vigueur le 24 avril 2023

Les dispositions portant sur les assurances des risques de cyberattaques de la Loi n° 2023-22 d'Orientation et de Programmation du Ministère de l'Intérieur (LOPMI) qui a été promulguée le 24 janvier 2023 sont entrées en vigueur le 24 avril 2023.

> *« 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.*
>
> *L'article entre en vigueur trois mois après la promulgation de la présente loi. »*

Le législateur avait choisi de différer (rapport de la commission mixte paritaire du 1er décembre 2022[1]) de trois mois l'entrée en vigueur de ces nouvelles dispositions afin de laisser le temps aux assurés de prendre connaissance de leurs obligations.

1. Qui est concerné par cette obligation ?

Cette obligation s'applique **uniquement** aux personnes morales et aux personnes physiques dans le cadre de leur activité professionnelle, et donc pas aux consommateurs.

2 Une obligation qui concerne toutes les garanties des risques des cyberattaques

L'obligation d'effectuer un dépôt de plainte concerne toutes les garanties des risques des cyberattaques y compris l'assurance du paiement des rançongiciels.

Le législateur a volontairement supprimé la référence spécifique « au paiement des rançons » du premier projet de loi pour lui substituer la formulation « des pertes et dommages causés par une atteinte à un système de traitement automatisé de données… » (rapport 436 de l'Assemblée nationale du 4 novembre 2022 [2]).

[1] https://www.assemblee-nationale.fr/dyn/16/rapports/343/l16b0590_rapport-fond#

[2] https://www.assemblee-nationale.fr/dyn/16/rapports/cion_lois/l16b0436_rapport-fond#

La lecture du rapport de la commission des lois de l'Assemblée nationale n°436-4 de novembre 2022 confirme que rien dans le droit positif (Droit Européen, législation des pays l'OCDE, Code Civil, Code des Assurances, Code Pénal et dans la Jurisprudence) ne s'oppose à l'assurabilité de la prise en charge du paiement des rançons. Cette position a été affirmée par le Haut comité juridique de la place financière de Paris[3] (rapport du 28 janvier 2022). Seul le cas du paiement d'une rançon faite en connaissance que les fonds fournis seraient destinés à la commission d'un acte terroriste (article 421-2-2 du Code pénal[4]) peut s'opposer à l'assurabilité de ce risque.

La référence aux articles 323-1 à 323-3-1 du Code Pénal écarte de cette obligation les conséquences des incidents de sécurité informatique ayant une cause accidentelle ou résultant d'une erreur. **Il s'agit bien des conséquences d'une cyberattaque.**

3. Une consécration de l'assurabilité du paiement des rançons qui encadre l'indemnisation des victimes de cyberattaques

La commission des lois de l'Assemblée nationale (rapport 436 - page 48) confirme qu'il s'agit d'une consécration de l'assurabilité des rançons et non d'une légalisation. En effet, la prise en charge des rançons a toujours été assurable dès lors que la victime et son assureur respectaient la législation sur les infractions de lutte contre le financement du terrorisme prévue à l'article 421-2-2 du Code Pénal.

4. Un délai de 72h00 pour respecter cette nouvelle obligation

Le choix de la durée de ce délai résulte d'un équilibre entre les intérêts de la victime (à qui il faut laisser le temps de réagir) et les nécessités de l'enquête.

Ce choix, initialement porté à 24h00, a été allongé à 48h00 puis à 72h00.

Ce nouveau dispositif subordonne le paiement d'une indemnité d'assurance « 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 ». Il favorise l'information des forces de sécurité et de l'autorité judiciaire, et les investigations. Il contribuerait ainsi à une meilleure réaction face à une cyberattaque, grâce au recoupement des plaintes et des indices, puisqu'une cyberattaque frappe rarement une seule victime. Il permettrait également de mieux connaître les techniques et les méthodes suivies par les cybercriminels (Rapport Sénat N°19 page 32 - 5 octobre 2022 / rapport Assemblée nationale n°436 page 48 – 4 novembre 2022).

Le point de départ :

Quant au point de départ de ce délai pour faire le dépôt de plainte, le législateur a opté pour **le moment de « la constatation de l'infraction par la victime »** au lieu « du moment du paiement de la rançon » ou celui « du moment de l'attaque ». Il s'agit ainsi de tenir compte des difficultés pour les victimes de connaître le moment exact de début d'une attaque cyber. Cette formulation vise à apporter de la sécurité juridique au dispositif légal. Elle s'inspire de la disposition de la directive NIS 2 qui prévoit une notification d'incident dans les soixante-douze heures qui suivent « la découverte de l'incident de sécurité ».

Selon la taille et les effectifs de l'assuré, le délai pour le dépôt de plainte commencera à courir au moment où les représentants légaux ou leurs délégataires (risque manager, RSSI, Secrétaires généraux, etc.) seront informés ou auront conscience que leur société est victime d'une infraction pénale (cyberattaque).

[3] https://www.banque-france.fr/sites/default/files/rapport_45_f.pdf

[4] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418433

5. Quels sont les contrats d'assurance concernés ?

La restriction au paiement des rançons a été volontairement supprimée par la commission des lois de l'Assemblée nationale (rapport 436 Assemblée nationale page 51[5]) pour étendre cette obligation à l'ensemble des remboursements assurantiels.

Cet article concerne les assurés qui bénéficient de garanties des risques cyber (pertes financières ou gestion de crise cyber) dans le cadre des assurances des risques cyber ou qui pourraient être annexées à d'autres contrats d'assurance (ex. volet gestion de crises cyber dans un contrat d'assurance RCP).

6. Modalités du dépôt de plainte

En cas de cyberattaque, nous vous recommandons d'associer le dépôt de plainte à votre plan de gestion de crise, et notamment penser à :

- Préserver toutes les traces visibles de l'attaque (photos, captures d'écran, etc.),
- Lister par ordre chronologique toutes les actions entreprises à la suite de l'attaque,
- Apporter ou tenir à disposition un maximum de preuves (fichiers, photos, images, vidéos, clés USB, CD/DVD, disque dur, etc.).

La victime doit porter plainte dans une brigade de gendarmerie ou un commissariat dans un délai de 72h maximum à compter de la prise de connaissance de l'incident.

Les informations sur les modalités du dépôt de plainte sont disponibles sur le lien ci-dessous : https://www.masecurite.interieur.gouv.fr/fr.

Si l'entreprise, immatriculée en France et assurée par un contrat d'assurance français, est victime d'une cyberattaque à l'étranger, nous recommandons de déposer plainte à la fois :

- En France sous 72 h maximum,
- Dans le pays d'implantation sous 72 h maximum.

L'obligation de dépôt de plainte sera ainsi respectée.

[5] https://www.assemblee-nationale.fr/dyn/16/rapports/cion_lois/l16b0436_rapport-fond#

DIOT - Groupe DIOT-SIACI - Société de Courtage d'Assurance et de Réassurance.

Siège social : Siège social : Siège social : Season - 39, rue Mstislav Rostropovitch - 75815 PARIS - FRANCE - Tél. : +33 (0)1 44 79 62 00. SAS - Capital : 1 831 008 € - RCS Paris 582 013 736 - N° TVA : FR 92 582 013 736. N° ORIAS : 07 009 129 (www.orias.fr) - Sous le contrôle de l'ACPR - 4 place de Budapest - CS 92459 - 75436 PARIS CEDEX 09 - FRANCE. Réclamations : reclamations@diot.com - www.mediation-assurance.org

SIACI SAINT HONORE - Groupe DIOT-SIACI - Société de Courtage d'Assurance et de Réassurance.

Siège social : Season - 39, rue Mstislav Rostropovitch - 75815 PARIS CEDEX 17 - FRANCE - Tél. : +33 (0)1 4420 9999 - Fax : +33 (0)1 4420 9500. SAS - Capital : 120 555 961,60 € - RCS Paris 572 059 939 - APE 6622 Z - N° TVA : FR 54 572 059 939. N° ORIAS : 07 000 771 (www.orias.fr) - Sous le contrôle de /Regulated by ACPR - 4 place de Budapest - CS 92459 - 75436 PARIS CEDEX 09 - FRANCE. Réclamations / Complaint : SIACI SAINT HONORE - Service réclamations - 23, allées de l'Europe - 92587 CLICHY CEDEX - FRANCE.