

Ransomware : le Gouvernement n'est pas pour interdire le paiement des rançons

Faut-il interdire aux assureurs d'indemniser les rançons que versent leurs clients victimes de cyberattaques ? En octobre dernier, le législateur – plus précisément un groupe d'études de l'Assemblée nationale – s'était [prononcé](#). Il avait répondu par l'affirmative, en écho à des appels dans ce sens [jusqu'aux sommets](#) de l'appareil d'État.

Le Gouvernement n'a pas la même approche. En tout cas à en juger un projet de loi pour lequel il vient d'engager une procédure accélérée : la LOPMI (loi d'orientation et de programmation du ministère de l'Intérieur pour 2022-2027).

En l'état, le texte **n'interdit pas l'indemnisation des rançons** par les assureurs. Mais la **subordonne au dépôt d'une plainte au plus tard 48 heures après le paiement**. Par « rançon », il faut entendre les sommes versées dans le cadre d'extorsions ([article 312-1](#) du Code pénal) au moyen d'atteintes à des systèmes de traitement automatisé des données ([323-1 à 323-3-1](#)).

Journée de la résilience et saisie d'actifs numériques

Toujours en matière de cybercriminalité, la LOPMI modifie l'article [706-154](#) du Code de procédure pénale, relatif à la saisie de biens par l'officier de police judiciaire. Pour le moment, ledit article fait référence aux sommes d'argent versées sur des comptes de dépôt. Il s'agit ici d'y ajouter les « actifs numériques ». Plus précisément, ceux mentionnés au [L. 54-10-1](#) du Code monétaire et financier. Lequel renvoie lui-même à d'autres articles tout en listant les actifs numériques suivants :

Le projet de loi LOPMI apporte aussi des modifications [au Code des postes et communications électroniques](#). Dans les grandes lignes, le Gouvernement veut se réserver le droit d'établir, par ordonnance, un cadre pour le déploiement de réseaux en cas de crises et de catastrophes : statut et missions des opérateurs exploitants, modalités d'accès, obligations de résilience, etc.

Il est aussi question d'instaurer une journée nationale de la résilience, pour préparer la population face aux risques naturels ou technologiques. Les employeurs auraient par ailleurs à organiser, au moins une fois par an, une information sur les conduites à tenir face à de tels risques. Et, plus globalement, à désigner un référent chargé de l'information des travailleurs.

Illustration principale ©