N° 894
SÉNAT

2024-2025

Enregistré à la Présidence du Sénat le 16 septembre 2025

PROPOSITION DE LOI

visant à **intégrer** *les* **risques** *en* **matière** *de* **cybersécurité**

au **plan communal** *de* **sauvegarde**,

PRÉSENTÉE

Par M. Mickaël VALLET,

Sénateur

(Envoyée à la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale, sous réserve de la constitution éventuelle d'une commission spéciale dans les conditions prévues par le Règlement.)

EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

La cybersécurité constitue un enjeu majeur pour les collectivités locales, dans un contexte de transformation numérique profonde et de recrudescence des menaces cyber. D'après l'étude sur la maturité des collectivités en matière de cybersécurité réalisée par le groupement d'intérêt public - action contre la cybermalveillance (GIP ACYMA) en 2024[1], une collectivité sur dix déclare avoir été victime d'une ou de plusieurs cyberattaques[2] au cours des 12 derniers mois.

Ces attaques, en constante augmentation, sont loin d'être anodines : elles ont provoqué une interruption d'activité et de service pour plus d'un tiers des communes touchées et une destruction ou un vol de données pour un quart d'entre elles[3]. À La Rochelle par exemple, une cyberattaque subie entre Noël et le jour de l'an 2021 a directement causé l'interruption de plusieurs services publics locaux et notamment le service d'état civil, le service des cimetières ou encore le service de gestion des parkings.

Même si les collectivités prennent de plus en plus conscience du risque cyber, elles ne se sentent pas suffisamment armées en cas d'incident cyber. Seules 14 % d'entre elles se disent préparées en cas de cyberattaque et à peine une collectivité sur cinq dispose d'une procédure de réaction adaptée.[4]

La présente proposition de loi a ainsi pour objectif d'améliorer sensiblement le degré de préparation des collectivités en cas d'incident cyber en intégrant explicitement le risque cyber au sein du plan communal de sauvegarde.

Cette proposition s'inspire de l'une des recommandations de l'autorité des marchés financiers (AMF) au sein de son guide sur la cybersécurité à destination des communes, publié en novembre 2020, dans lequel

---

[1] 3ème étude du baromètre de la maturité Cyber des Collectivités françaises, Opinionway pour le GIP ACYMA, 25 octobre 2024, p.30

[2] L'Agence nationale de la sécurité des systèmes d'information (ANSSI) définit, dans son Cyberdico, la cyberattaque comme une attaque consistant à porter atteinte à un ou plusieurs systèmes informatiques dans le but de satisfaire des intérêts malveillants.

[3] 3ème étude du baromètre de la maturité Cyber des Collectivités françaises, Opinionway pour le GIP ACYMA, 25 octobre 2024, p.31

[4] *Ibid*., p.28

l'association affirmait que « *les plans de crise des communes et des intercommunalités doivent être complétés par un volet numérique.* »[5] Cette proposition vise également à répondre aux demandes formulées par les élus au numérique lors du 5ème Congrès national organisé par Villes Internet en 2023 à savoir « *rendre obligatoire une périodicité d'exercices de cyberattaques* » et « *établir un plan de gestion de crise et de continuité de l'activité en cas de cyberattaque, mobilisable jusqu'aux plus petites communes* ».

Même si certaines communes comme Châteauroux ou Colmar ont intégré le risque cyber au sein de leur plan communal de sauvegarde, ce n'est pas le cas de la grande majorité des 21 057 communes tenues de rédiger un tel plan.

Créé par la loi du 13 août 2004 de modernisation de la sécurité civile, le plan communal de sauvegarde (PCS), est un document élaboré sous l'autorité du maire, visant à organiser les moyens communaux existants pour faire face aux situations d'urgence. La loi de 2004 a rendu obligatoire son élaboration dans toutes les communes concernées par la prescription d'un plan de prévention des risques naturels ou par un plan particulier d'intervention. La loi dite « Matras » du 25 novembre 2021 a élargi l'obligation d'élaborer un PCS aux communes exposées à d'autres risques naturels dont l'intensité ou la soudaineté le rendent nécessaire (risques forestiers, volcaniques, cycloniques ...). Cette loi rend également obligatoire la réalisation d'un plan intercommunal de sauvegarde (PICS) pour tous les établissements publics de coopération intercommunale (EPCI) à fiscalité propre dès lors qu'au moins une des communes membres est soumise à l'obligation d'élaborer un PCS. Le PCS et le PICS sont désormais régis par les articles L. 731-3 à L. 731-5 et les articles R. 731-1 à D. 731-14 du code de la sécurité intérieure.

L'article 1er modifie le premier alinéa de l'article L. 731-3 du code de la sécurité intérieure afin de préciser que le risque cyber fait nécessairement partie des risques connus devant être traités au sein du PCS.

Le risque cyber est décrit dans cet article comme « *le risque d'incident informatique ayant un impact important sur la fourniture des services à la population* ». Le choix de la notion d'incident informatique permet d'englober à la fois les cyberattaques mais également les pannes informatiques ayant une autre cause (mauvaise utilisation, catastrophe naturelle, problème de matériel ou de logiciel). Pour déterminer si l'incident a un impact important ou non, la commune pourra se référer au paragraphe 3

[5] Guide sur la cybersécurité à destination des communes, AMF, septembre 2020, p.22

de l'article 23 de la directive (UE) 2022/2555 du Parlement européen et du Conseil (directive NIS 2).

Le volet cyber du PCS permettra d'agir sur les piliers de la gestion d'une crise numérique : la résolution technique ; la continuité d'activité pour assurer les services essentiels de la collectivité ainsi que la mise en place d'une communication appropriée vers les usagers, les agents, les médias et les acteurs publics.

Ainsi, en rédigeant ce volet, les collectivités soumises à la directive NIS 2 satisferont à l'obligation contenue à l'article 21 de ladite directive imposant la mise en place de mesures de gestion des crises (obligation qui sera transposée dans un futur décret). Pour les collectivités non concernées par la directive NIS 2 (qui seront probablement les communes de moins de 30 000 habitants), le volet cyber du PCS permettra d'assurer une protection minimale de leurs systèmes d'information et de limiter les dégâts en cas d'incident cyber.

L'intégration d'un volet cyber au sein du PCS sera accessible pour toutes les communes. Dans les communes ayant rédigé leur PCS, la gestion d'une crise cyber ne différant pas fondamentalement d'une crise ayant une autre origine, la gestion de crise est déjà formalisée et constituera un socle sur lequel s'intègrera naturellement un volet cyber. Pour les autres communes, des ressources sont mises à leur disposition pour les aider à rédiger ce volet cyber comme celles de cybermalveillance.gouv.fr ou encore le guide du Pôle d'excellence cyber publié en novembre 2024[6].

L'article 2 vise à renforcer la prise en compte du risque cyber dans la gestion communale des crises, en modifiant explicitement le code de la sécurité intérieure pour que le plan communal de sauvegarde (PCS) intègre ce risque à tous les niveaux de son élaboration.

L'article 3 est le gage de la proposition de loi.

[6] Guide « Intégration du risque cyber au plan communal de sauvegarde des petites communes », Pôle d'excellence cyber, novembre 2024

Proposition de loi visant à intégrer les risques en matière de cybersécurité au plan communal de sauvegarde

Article 1er

① Le I de l'article L. 731-3 du code de la sécurité intérieure est ainsi modifié :

② 1° À la seconde phrase du premier alinéa, après le mot : « connus, », sont insérés les mots : « y compris le risque d'incident informatique ayant un impact important sur la fourniture des activités de service public à la population, » ;

③ 2° Après le 7°, il est inséré un 8° ainsi rédigé :

④ « 8°Assurant des activités de service public dont la continuité est susceptible d'être perturbée par des incidents informatiques. La liste de ces activités de service public est fixée par le décret en Conseil d'État mentionné à l'article L. 731-5. »

Article 2

À l'article L. 731-5 du code de la sécurité intérieure, après le mot : « sauvegarde », sont insérés les mots : « , notamment pour prendre en compte le risque d'incident informatique, ».

Article 3

① I. – Les éventuelles conséquences financières résultant pour les collectivités territoriales de la présente loi sont compensées, à due concurrence, par une majoration de la dotation globale de fonctionnement.

② II. – L'éventuelle perte de recettes résultant pour l'État du I est compensée, à due concurrence, par la création d'une taxe additionnelle à l'accise sur les tabacs prévue au chapitre IV du titre Ier du livre III du code des impositions sur les biens et services.