ASSEMBLÉE NATIONALE

5 septembre 2025

RÉSILIENCE DES INFRASTRUCTURES CRITIQUES ET RENFORCEMENT DE LA CYBERSÉCURITÉ - (N° 1112)

Non soutenu

N° CS116

AMENDEMENT

présenté par
M. Allegret-Pilot

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 5, insérer l'article suivant:

La section 3 du chapitre Ier du titre III du livre VII du code de la sécurité intérieure est ainsi modifiée :

I. – Le I de l'article L. 731-3 est ainsi modifié :

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 services à la population, » ;

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

« 8° Assurant des activités de service public dont la continuité est susceptible d'être perturbée par des incidents informatiques, et dont la liste est déterminée par décret en Conseil d'État. »

II. – À l'article L. 731-5, après le mot : « sauvegarde », sont insérés les mots : « , notamment pour prendre en compte le risque d'incident informatique, ».

III. – Les dispositions du présent article entrent en vigueur à l'occasion de l'actualisation du plan communal ou, au plus tard, à la date de sa révision.

EXPOSÉ SOMMAIRE

Le présent amendement vise à améliorer sensiblement le degré de préparation des collectivités

territoriales face à la menace cyber en intégrant explicitement le risque de cyberattaque au sein du

Plan Communal de Sauvegarde (PCS).

Alors que les collectivités jouent un rôle essentiel dans la continuité des services publics et la gestion des crises locales, elles sont devenues ces dernières années des cibles privilégiées des cybercriminels et d'acteurs étatiques hostiles. Selon l'ANSSI), plus de 350 collectivités ont été victimes d'une cyberattaque en 2023, dont une majorité de communes de taille moyenne, souvent démunies en matière de protection informatique.

Les exemples concrets abondent. En septembre 2024, la mairie de Caen a été victime d'une attaque par rançongiciel paralysant plusieurs de ses services administratifs pendant plusieurs jours. À la même période, la ville de Chaville (Hauts-de-Seine) a vu son système d'information compromis, entraînant la perte d'accès à des documents sensibles et des données personnelles. En 2022, la ville de La Rochelle avait également subi une cyberattaque majeure, impactant la gestion de ses services numériques.

Ces incidents démontrent la vulnérabilité des collectivités et l'impact potentiel de ces attaques : paralysie administrative, interruption des services aux usagers, atteinte à la confidentialité des données des citoyens, voire mise en danger de la sécurité des populations en cas d'atteinte aux systèmes d'alerte ou de gestion de crise.

Or, le Plan Communal de Sauvegarde, prévu par l'article L.731-3 du Code de la sécurité intérieure, constitue l'outil de référence permettant d'organiser la réponse opérationnelle de la commune en cas d'événement grave : catastrophes naturelles, risques technologiques, sanitaires… Il apparaît aujourd'hui indispensable que les risques cyber soient explicitement intégrés à ce dispositif, au même titre que les autres menaces susceptibles de désorganiser la vie locale. Le présent amendement vise donc à améliorer sensiblement le degré de préparation des collectivités en ajoutant le risque cyber au sein du plan communal de sauvegarde. Cet amendement a été travaillé avec Hexatrust