ASSEMBLÉE NATIONALE

5 septembre 2025

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

Rejeté

N° CS193

AMENDEMENT

présenté par
M. Mazaury, Mme Thillaye et Mme Sebaihi

ARTICLE 9

À l'alinéa 5, après les mots :

« communautés de communes »,

insérer les mots :

« de 20 000 habitants et plus ».

EXPOSÉ SOMMAIRE

Le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité transpose trois directives européennes dont la directive NIS2 du 14 décembre 2022, qui concerne plus spécifiquement les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union.
Le choix qui a été fait par le Gouvernement est celui d'une transposition très étendue de cette directive, comme l'a indiqué le Conseil d'Etat.

Ainsi, dans son avis N° 408329 rendu le 6 juin 2024, il relève que « le projet de loi mobilise dans un sens extensif les possibilités d'options offertes par la directive, notamment en incluant dans le champ du dispositif des collectivités territoriales autres que les régions, à savoir tous les départements ainsi que les communes et groupements de communes de plus de trente mille habitants (…) ». « Ces choix, qui vont au-delà de ce qu'appelle strictement la transposition de la directive NIS2, trouvent leur justification dans la volonté du Gouvernement d'assurer en France un haut niveau de cybersécurité. »

Les nouvelles obligations imposées par ce projet de loi entraîneront des charges supplémentaires

importantes pour les communes et les intercommunalités – que l'étude d'impact n'a d'ailleurs pas chiffrées -, alors que dans le même temps, les déclarations récentes du Gouvernement appellent à un effort très important des collectivités locales au déficit public (chiffrés à 5,3 milliards hors CNRACL), tout comme les rapports de la Cour des Comptes qui invitent à contraindre davantage l'augmentation des dépenses de fonctionnement du bloc communal.

Imposer de nouvelles normes couteuses dans ce contexte relève d'une injonction contradictoire, quel qu'en soit le caractère légitime de l'intention.

Si l'ensemble des élus est soucieux des questions de cybersécurité et souhaite que l'application de la directive soit un succès, force est de constater que le texte ne tient pas compte de la réalité des moyens des communautés de communes et de leurs communes membres et du contexte financier actuel afin que la mise en œuvre des mesures requises soit supportable financièrement, faisable techniquement et progressive dans la durée.
L'absence de progressivité dans l'application du texte risque de compliquer sa mise en œuvre, d'autant plus que le secteur de la cybersécurité est déjà sous forte pression et que la filière Cyber peine à répondre à la demande. Imposer ces nouvelles obligations à un grand nombre d'acteurs dès la publication de la loi sans anticipation adéquate ne fera qu'aggraver cette tension.

Ces préoccupations touchent particulièrement les communautés de communes, situées en zone rurale, où l'accès à un certain niveau d'ingénierie est souvent difficile. Elles couvrent de vastes territoires peu denses et leur centralité repose généralement sur de petits bourgs dont les capacités techniques et les ressources financières sont limitées. Les structures de mutualisation numérique de plus grande envergure (GIP, syndicats mixtes, etc.) ne sont pas encore présents partout et leurs moyens sont variables.

C'est pourquoi et afin de tenir compte de ces situations et des ressources disponibles sur le territoire des communautés de communes tant en ingénierie que financière, le présent amendement propose :

1/ de retenir dans le périmètre des « Entités importantes » les communautés de communes dont la population totale regroupée est égale ou supérieure à 20 000 habitants. Cela concernerait 475 communautés de communes qui seraient alors soumises aux règles applicables aux « Entités importantes ».

2/ d'exclure les communautés de communes de moins de 20 000 habitants du périmètre des « entités importantes », considérant que leurs moyens sont trop insuffisants pour appliquer les exigences du texte et du projet de référentiel. Il s'agit ainsi de leur laisser le temps nécessaire pour mettre en place une nouvelle organisation de la cybersécurité, laquelle doit être adaptée à leur réalité. Cela concernerait 515 communautés de communes.

Cette mesure a également pour objectif de ne pas créer une pression supplémentaire dans la mise en œuvre des règles de cybersécurité alors que le marché est déjà sous tension (les communautés de communes entreront dans ce marché en même temps que de très nombreuses entreprises).

Pour autant, il est primordial d'assurer l'information et la formation des élus comme des agents, ainsi que de promouvoir la diffusion des bonnes pratiques dans ces collectivités comme dans les communes ; des enjeux que le projet de loi gagnerait à mieux intégrer (soutien et programme d'actions de l'Etat et de ses opérateurs).
Si les objectifs de cybersécurité sont largement partagés, les moyens pour les atteindre doivent être repensés et adaptés aux réalités de ces collectivités.