ASSEMBLÉE NATIONALE

6 novembre 2024

PLF POUR 2025 - (N° 324)

Commission	
Gouvernement	

AMENDEMENT

N º II-2148

présenté par
M. Bothorel, Mme Morel et M. Latombe

ARTICLE 42

ÉTAT B

Mission « Relations avec les collectivités territoriales »

Sous réserve de son traitement par les services de l'Assemblée nationale et de sa recevabilité

Modifier ainsi les autorisations d'engagement et les crédits de paiement :

(en euros)

Programmes	+	-
Concours financiers aux collectivités territoriales et à leurs groupements	10 000 000	0
Concours spécifiques et administration	0	10 000 000
TOTAUX	10 000 000	10 000 000
SOLDE	0	

EXPOSÉ SOMMAIRE

Le présent amendement vise à allouer 10M d'euros supplémentaires aux départements et régions prochainement concernés par la transposition de la directive NIS2, à travers une hausse des crédits alloués à l'action 3 « Soutien aux projets des départements et des régions » du programme 119 « concours financiers aux collectivités territoriales et à leurs groupements ».

Il y a quelques semaines, le Gouvernement a présenté son projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, qui vise notamment à transposer dans le droit national la directive européenne NIS2. Cette dernière vise à rehausser le niveau de cybersécurité au sein des entités considérées comme importantes ou essentielles pour le fonctionnement de la Nation, avec des obligations proportionnées.

Si la directive laisse au Législateur national le soin de déterminer si les collectivités territoriales entrent dans le champ de la législation, la version initiale du projet de loi considère notamment les régions, les départements, les communes d'une population supérieure à 30 000 habitants, les communautés urbaines, les communautés d'agglomération et les métropoles comme des entités essentielles. Ce choix s'explique par le fait que les collectivités territoriales sont régulièrement victimes de cyberattaques : entre janvier 2022 et juillet 2023, l'Anssi a traité 187 incidents de cybersécurité touchant les collectivités territoriales, soit 17% de l'ensemble des incidents. 37% de ces collectivités ont déjà été touchées par une cyberattaque.

Si le Parlement fait le choix de confirmer l'équilibre dessiné par le Gouvernement, cela signifie que 661 collectivités territoriales ou groupements de collectivités territoriales devraient être concernés au titre des entités essentielles, parmi lesquelles les régions de métropole ainsi que les régions et pays et territoires d'outre-mer (22 entités) ainsi que les départements de métropole et d'outre-mer (97 entités).

Face à cet important passage à l'échelle dans le domaine cyber, le présent amendement alerte sur la nécessité d'établir un accompagnement financier pour les collectivités concernées. Ces dernières ne disposent en effet ni des compétences ni des moyens de mettre en œuvre les nouvelles obligations qui se profilent. Une note interne du Gouvernement publiée dans le média L'Informé souligne que les « parcours de cybersécurité » proposés dans le cadre du plan de relance pour un coût unitaire de 100 000 € peuvent constituer une première étape vers la mise en conformité, ce qui apparaît souhaitable. Cette même note établit également que, « si l'on estime à 400 000 € le coût moyen de mise en conformité pour une entité, quelle qu'elle soit, une subvention moyenne de 25 % pour les collectivités territoriales supposerait un budget global triennal de 60 millions €/an. »

Aussi cet amendement propose, tant en autorisations d'engagement qu'en crédits de paiement, de :

- majorer de 10 000 000 euros les crédits de l'action 3 du programme 119 ;

- minorer de 10 000 000 euros les crédits de l'action 4 du programme 122.

Il ne s'agit pas de pénaliser le programme 122 mais uniquement de respecter les conditions de recevabilité financière. Il conviendra que le Gouvernement lève le gage en cas d'adoption de l'amendement.