ASSEMBLÉE NATIONALE

5 septembre 2025

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

Rejeté

N° CS323

AMENDEMENT

présenté par
M. Latombe

ARTICLE 14

Compléter l'alinéa 2 par la phrase :

« Le choix d'une solution logicielle dont le code source n'est pas accessible ou vérifiable, et lorsqu'elle concerne un système d'information critique, fait l'objet d'une analyse de risques spécifique, documentée et présentée aux organes de direction évaluant la dépendance vis-à-vis du fournisseur, les limitations en matière d'audit de sécurité et les stratégies de réversibilité à brève échéance. »

EXPOSÉ SOMMAIRE

Le présent amendement vise à instaurer une saine gestion des risques technologiques pour les systèmes d'information les plus critiques de la Nation, en application du principe « appliquer ou expliquer ». Le projet de loi renforce à juste titre les obligations de cybersécurité. Cependant, une part majeure du risque provient des briques logicielles elles-mêmes, notamment lorsqu'elles sont des « boîtes noires » dont le fonctionnement interne est inaccessible à l'entité qui les utilise et aux autorités de contrôle. Cet amendement ne vise pas à interdire le recours aux logiciels propriétaires, mais à s'assurer que leur choix pour un usage critique soit une décision éclairée et documentée. En exigeant une analyse de risques spécifique pour les solutions à code source fermé, cet amendement contraint les entités essentielles et importantes à évaluer objectivement :

1. La dépendance technologique (vendor lock-in) : Le risque de se retrouver prisonnier d'un fournisseur unique, souvent soumis à des législations étrangères, est une vulnérabilité stratégique majeure. L'analyse devra porter sur les stratégies de réversibilité et de sortie.

2. Les limitations en matière d'audit de sécurité : L'impossibilité de réaliser ou de faire réaliser un audit complet du code source constitue un risque de sécurité intrinsèque. L'entité devra formaliser la manière dont elle entend pallier cette opacité.

3. La souveraineté des données et des systèmes : Cet amendement s'inscrit dans la continuité de l'article 16 de la loi pour une République numérique, qui demande aux administrations de préserver la « maîtrise, la pérennité et l'indépendance de leurs systèmes d'information ». Il précise cette exigence de maîtrise dans le cas des infrastructures critiques du pays.