ASSEMBLÉE NATIONALE

5 septembre 2025

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

Adopté

N° CS318

AMENDEMENT

présenté par
M. Latombe

ARTICLE 14

I. – Après la deuxième phrase de l'alinéa 1, insérer la phrase :

« Le choix de ces mesures tient compte de leur capacité à être audités, de la transparence de leur fonctionnement, de leur interopérabilité, de leur résilience et de la maîtrise qu'elles permettent d'acquérir sur les systèmes d'information afin de minimiser les dépendances technologiques à l'égard de prestataires tiers en présentant pas de garanties suffisantes de conformité aux exigences de cybersécurité et de souveraineté numérique telles que fixées par la stratégie nationale dans une perspective de long terme. »

II. – En conséquence, compléter l'alinéa 8 par les mots :

« , en veillant au respect des principes énoncés au premier alinéa du présent article. »

EXPOSÉ SOMMAIRE

Proposition de modification substantielle de l'article 14.

Le présent amendement vise à renforcer les objectifs de sécurité et de résilience numérique inscrits dans ce projet de loi en s'assurant que les mesures de cybersécurité prises par les entités critiques reposent sur des fondations techniques saines, maîtrisées et souveraines. Cet amendement s'inscrit dans la continuité de l'article 16 de la loi n° 2016-1321 pour une République numérique, qui dispose déjà que les administrations doivent veiller « à préserver la maîtrise, la pérennité et l'indépendance de leurs systèmes d'information ». Il propose d'étendre cette exigence à l'ensemble des entités essentielles et importantes et de la traduire en critères techniques objectifs. En effet, une sécurité effective et une résilience durable ne peuvent être atteintes avec des solutions opaques ou qui créent une dépendance excessive. C'est pourquoi cet amendement propose d'introduire cinq critères fondamentaux pour guider le choix des technologies et services :

1. Auditabilité et transparence : Une entité ne peut sécuriser efficacement une « boîte noire ». La capacité d'auditer le fonctionnement d'un logiciel est indispensable pour s'assurer de l'absence de vulnérabilités cachées ou de portes dérobées. La directive NIS 2 elle-même, dans son considérant 52, souligne que « Les sources ouvertes peuvent conduire à un processus de vérification plus transparent ».

2. Interopérabilité et pérennité : La résilience d'une infrastructure est compromise si elle est dépendante d'une technologie propriétaire unique (« enfermement propriétaire »). Cette notion est au cœur de l'analyse des dépendances exigée pour les OIV à l'article L. 1332-4 du code de la défense, tel que modifié par le présent projet de loi.

3. Maîtrise : Ce critère est la condition de notre souveraineté numérique. Le rapport d'information de l'Assemblée Nationale « Bâtir et promouvoir une souveraineté numérique nationale et européenne » (dit « rapport Latombe », n°4299, 2021) insiste sur les trois grands principes pour l'État que sont la liberté de choix, la maîtrise technologique et la réversibilité. Le présent amendement traduit directement ces principes en obligations pour les entités critiques.

En introduisant ces critères, cet amendement dote les entités concernées et l'autorité de contrôle (ANSSI) d'une boussole claire pour le choix des solutions, sans imposer une technologie particulière. Il encourage une approche vertueuse de la sécurité, fondée sur la confiance et la vérification, et aligne la France sur les ambitions maintes fois réaffirmées par le Parlement en matière de souveraineté numérique.