

ASSEMBLÉE NATIONALE

3 octobre 2026

**RÉSILIENCE DES INFRASTRUCTURES CRITIQUES ET RENFORCEMENT DE LA
CYBERSÉCURITÉ - (N° 1779)**

Commission	
Gouvernement	

N° 369

AMENDEMENT

présenté par

Mme Thillaye, Mme Darrieussecq, M. Balanant, Mme Bannier, Mme Bergantz, M. Blanchet,
Mme Brocard, M. Cosson, M. Croizier, M. Daubié, M. Fesneau, M. Fuchs, Mme Gervais,
Mme Perrine Goulet, M. Grelier, Mme Guillerm, M. Gumbs, M. Isaac-Sibille, Mme Josso,
M. Lecamp, Mme Lingemann, M. Mandon, M. Martineau, M. Mattei, Mme Maussion, Mme Mette,
Mme Morel, M. Ott, M. Padey, M. Pahun, M. Frédéric Petit, Mme Maud Petit, Mme Poueyto,
M. Ramos, M. Turquois et M. Philippe Vigier

ARTICLE 16

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

Compléter l'alinéa 4 par la phrase :

« L'autorité nationale de la sécurité des systèmes d'information veille à ce que les processus de certification, de qualification et d'agrément soient fondés sur des critères techniques objectifs, transparents et non-discriminatoires, afin de garantir leur accessibilité aux logiciels libres et aux solutions proposées par les petites et moyennes entreprises innovantes. ».

EXPOSÉ SOMMAIRE

Cet amendement a pour objectif de garantir que la promotion de solutions de cybersécurité certifiées, prévue par l'article 16, ne crée pas d'effets pervers en défavorisant l'écosystème français et européen de l'innovation, notamment les acteurs du logiciel libre et les PME.

L'article 16 permet au Premier ministre de prescrire le recours à des produits ou services certifiés ou qualifiés par l'ANSSI pour les systèmes les plus sensibles de la Nation. Cette démarche est un gage de sécurité. Toutefois, il existe un risque avéré que les processus de certification, par leur complexité ou leur coût, favorisent de facto les grands éditeurs, souvent extra-européens, au détriment d'alternatives innovantes et souveraines. Le rapport d'information de l'Assemblée nationale « Bâtir et promouvoir une souveraineté numérique nationale et européenne » (n°4299,

2021) souligne la nécessité de « faire confiance à nos entreprises technologiques » et de « privilégier, en matière de commande publique, le recours aux solutions d'acteurs technologiques français ou européens » (Proposition n°26).

Cet amendement vise à prévenir ce risque en prévoyant une obligation pour l'ANSSI de concevoir des processus de qualification équitables et ouverts. Il s'agit de s'assurer que :

1. L'évaluation est fondée sur le mérite technique : Les critères doivent être objectifs et basés uniquement sur la robustesse et la sécurité de la solution, indépendamment du modèle économique (libre, propriétaire) ou de la taille du fournisseur.
2. Les barrières à l'entrée sont réduites : Les modalités ne doivent pas constituer un obstacle insurmontable pour les PME et les structures (associations, fondations) qui portent de nombreux projets de logiciels libres, en cohérence avec l'esprit de l'article 16 de la loi pour une République numérique qui en encourage l'utilisation.
3. La souveraineté numérique est renforcée : En garantissant une compétition équitable, nous permettons aux solutions françaises et européennes les plus performantes, y compris celles issues du logiciel libre, d'obtenir les qualifications nécessaires pour être déployées sur nos infrastructures critiques, renforçant ainsi notre filière technologique.

Cet amendement est une mesure de sauvegarde pragmatique qui garantit que le renforcement de notre cybersécurité se fera en s'appuyant sur l'ensemble de nos forces vives, favorisant ainsi l'émergence d'une filière de confiance diversifiée et véritablement souveraine.