

ASSEMBLÉE NATIONALE

4 septembre 2025

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

Rejeté

N° CS56

AMENDEMENT

présenté par

M. Pilato, Mme Abomangoli, M. Alexandre, M. Amard, Mme Amiot, Mme Amrani, M. Arenas,
M. Arnault, Mme Belouassa-Cherifi, M. Bernalicis, M. Bex, M. Bilongo, M. Bompard,
M. Boumertit, M. Boyard, M. Cadalen, M. Caron, M. Carrière, Mme Cathala, M. Cernon,
Mme Chikirou, M. Clouet, M. Coquerel, M. Coulomme, M. Delogu, M. Diouara, Mme Dufour,
Mme Erodi, Mme Feld, M. Fernandes, Mme Ferrer, M. Gaillard, Mme Guetté, M. Guiraud,
Mme Hamdane, Mme Hignet, M. Kerbrat, M. Lachaud, M. Lahmar, M. Laisney, M. Le Coq,
M. Le Gall, Mme Leboucher, M. Legavre, Mme Legrain, Mme Lejeune, Mme Lepvraud,
M. Léaument, Mme Élisabeth Martin, M. Maudet, Mme Maximi, Mme Mesmeur,
Mme Manon Meunier, M. Nilor, Mme Nosbé, Mme Obono, Mme Oziol, Mme Panot, M. Piquemal,
M. Portes, M. Prud'homme, M. Ratenon, M. Saint-Martin, M. Saintoul, Mme Soudais,
Mme Stambach-Terreiro, M. Taché, Mme Taurinya, M. Tavel, Mme Trouvé et M. Vannier

ARTICLE 20

Compléter cet article par l'alinéa suivant :

« Les données mentionnées à l'alinéa précédent sont conservées dans un système de sauvegarde sécurisé pour une durée de dix ans aux seules fins de répondre à une demande émanant de l'autorité judiciaire dans le cadre d'une procédure pénale ou de permettre à l'autorité nationale de sécurité des systèmes d'information d'identifier l'origine d'un incident de cybersécurité ou d'assurer la résilience des réseaux. Ce dispositif de conservation prolongée est soumis à des conditions strictes d'accès, de traçabilité et de protection des données, dans le respect des droits fondamentaux. »

EXPOSÉ SOMMAIRE

Par cet amendement, le groupe parlementaire LFI prévoit un système de sauvegarde sécurisé pour les données mentionnées à l'article 20, exclusivement pour répondre aux besoins spécifiques des procédures pénales et des enquêtes en cybersécurité.

Cette mesure répond à des enjeux majeurs liés à la nature même des incidents de cybersécurité, qui sont souvent complexes, dissimulés, et détectés avec un retard important, parfois plusieurs années après leur survenue. La capacité des autorités judiciaires et des organismes de sécurité à reconstituer

les chaînes d'attaque, identifier les auteurs, et comprendre les mécanismes d'intrusion repose donc sur la disponibilité prolongée de données fiables et complètes.

Par ailleurs, dans le cadre des procédures pénales, la continuité probatoire est essentielle pour garantir l'efficacité des enquêtes et la sécurité juridique des actes réalisés. La conservation étendue des données permet d'éviter que des preuves essentielles soient détruites prématurément, ce qui pourrait compromettre la poursuite des infractions graves liées au cybercrime ou à d'autres formes de délinquance numérique.

Toutefois, conscient des enjeux de protection des données personnelles et des libertés fondamentales, cet amendement insiste sur la mise en place de conditions strictes encadrant l'accès, la traçabilité et la sécurisation de ces données prolongées. Cette organisation garantit que la conservation ne constitue pas un stockage généralisé injustifié, mais un outil ciblé, contrôlé et proportionné, respectant les exigences du droit à la vie privée et des règles applicables en matière de données personnelles.

En somme, cette disposition équilibre la nécessité impérieuse de disposer d'éléments probatoires suffisants dans le temps, tout en assurant un cadre transparent et rigoureux de gestion des données sensibles, contribuant ainsi à renforcer la confiance dans les dispositifs de cybersécurité et dans le système judiciaire.