

**ASSEMBLÉE NATIONALE**

19 février 2026

RELATIVE À LA SÉCURISATION DES MARCHÉS PUBLICS NUMÉRIQUES - (N° 2258)

Tombé

N° CL8

**AMENDEMENT**

présenté par

M. Le Gall, 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, 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. Pilato, M. Piquemal, M. Portes, M. Prud'homme, M. Ratenon, M. Saint-Martin, M. Saintoul, Mme Soudais, Mme Stambach-Terrenoir, M. Aurélien Taché, Mme Taurinya, M. Tavel, Mme Trouvé et M. Vannier

-----

**ARTICLE UNIQUE**

Après l'alinéa 4, insérer l'alinéa suivant :

« *I bis.* – Les entités mentionnés au I du présent article doivent, dans la mesure du possible, avoir recours à des solutions locales d'hébergement des données afin d'assurer le plus haut niveau de protection et de sécurité de ces dernières. »

**EXPOSÉ SOMMAIRE**

Par cet amendement, le groupe LFI souligne à nouveau l'importance de la préservation de la sécurité de l'hébergement de nos données numériques, en ayant recours à des solutions locales d'hébergement de ces dernières.

La numérisation croissante de la société a notamment entraîné une production massive de données numériques, parfois très sensibles comme les données personnelles. Or, l'hébergement de ces données s'est souvent reposé sur des services d'hébergement en nuage - aussi appelé "cloud" - qui permettent notamment d'avoir accès aux données stockées partout dans le monde, en ayant uniquement besoin d'une connexion à Internet pour ce faire. Or, en raison de la nationalité d'origine des acteurs économiques dominants sur ce marché, principalement des acteurs américains comme Amazon Web Services (AWS), Microsoft Azure et Google Cloud, les données que nous faisons

héberger sur ces services sont soumis à des législations extra-territoriales permettant à des puissances étrangères d'y avoir accès, sans notre autorisation. Ainsi, aux États-Unis, plusieurs législations permettent au Gouvernement d'accéder à nos données comme la section 702 du Foreign Intelligence Surveillance Act (Fisa) qui permet aux autorités américaines, sans nécessité de mandat, de recueillir des données personnelles de citoyens étrangers stockées sur des serveurs gérés par des fournisseurs de services cloud domiciliés aux États-Unis, y compris lorsque les serveurs ne sont pas situés sur le territoire américain. D'autres pays comme la Chine ou l'Inde ont également des législations similaires.

Face à cette situation, il est indispensable de réfléchir à d'autres solutions techniques d'hébergement plus fiables en termes de préservation de la sécurité de nos données, les solutions locales de stockage ayant un rôle important à jouer en la matière. Très concrètement, les solutions locales désignent des solutions où les données sont stockées sur des dispositifs physiques comme des serveurs internes, des disques durs externes ou des NAS (Network Attached Storage), et ces dernières présentent plusieurs avantages non négligeables : tout d'abord, le recours à ce type de solution permet aux propriétaires des données d'avoir un contrôle total sur la configuration et les autorisations d'accès des utilisateurs, d'autant plus que l'absence de nécessité d'utiliser Internet pour y avoir accès est une garantie de sécurité supplémentaire. Par ailleurs, les coûts pour ce type d'installation sont beaucoup moins élevés que pour le "cloud" puisqu'il s'agit souvent de coûts fixes (achat de l'infrastructure) et non de coûts récurrents (abonnement à un service "cloud"). Enfin, de nombreuses études démontrent que le recours au "cloud" a des conséquences environnementales majeures, les data centers utilisés pour héberger les données étant très énergivores. Ainsi, selon une étude publiée par l'Agence de la transition écologique (Ademe) le mardi 6 janvier 2026, les data centers sont « parmi les infrastructures les plus concentrées spatialement et intensives énergétiquement », leur développement devant être maîtrisé pour être compatible avec la transition écologique. Sur l'année 2024, les data centers installés en France avaient une consommation totale d'environ 10 térawattheures (TWh) d'électricité (sur une consommation annuelle totale du pays de 450 TWh). Si les tendances actuelles se poursuivent, l'Ademe estime que cette demande pourrait être multipliée par 3,7 d'ici à 2035 (37 TWh) et par 6,4 à l'horizon 2060.