

**ASSEMBLÉE NATIONALE**

16 mars 2026

RELATIVE À LA SÉCURISATION DES MARCHÉS PUBLICS NUMÉRIQUES - (N° 2522)

Commission	
Gouvernement	

N° 3

**AMENDEMENT**

présenté par

M. Coulomme, 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. 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. 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 10, insérer l'alinéa suivant :

« *I ter.* – Les entités mentionnées au I du présent article doivent prévoir des conditions d'exécution de marchés comportant des prestations d'hébergement et de traitement de données par les services de l'informatique en nuage les protégeant de tout effet extraterritorial d'une législation étrangère aboutissant à contraindre le titulaire d'un marché à communiquer ou à transférer ces données à des autorités étrangères. Par ailleurs, les titulaires de marchés retenus par les entités mentionnées au I doivent garantir que les données récoltées dans le cadre de l'exécution du marché soient hébergées sur des serveurs situés sur le territoire national ou de l'Union européenne. »

**EXPOSÉ SOMMAIRE**

Par cet amendement, le groupe LFI souhaite réaffirmer l'importance d'utiliser des solutions numériques souveraines, en garantissant l'hébergement des données récoltées par les pouvoirs publics sur des serveurs situés sur le territoire national (ou européen) et sur lesquels s'applique le droit national et protégé de tout effet d'une législation étrangère qui aboutirait d'une manière ou d'une autre à un transfert de données à des autorités étrangères.

Face à la numérisation de la société, l'usage de "cloud" est devenu indispensable au bon fonctionnement de l'administration publique. Selon les données de la Cour des Comptes sur le sujet, les dépenses publiques en la matière sont passées d'1 M€ en 2020 à 52 M€ en 2024 (les services de l'État représentent les 2/3 de la somme, soit 32 M€). Au total, entre 2020 et 2024, 120 M€ ont été dépensés. Si des données sont disponibles sur l'identité des fournisseurs d'accès choisis par l'État, il n'existe aucune donnée agrégée sur l'identité des fournisseurs choisis par les collectivités territoriales, alors même qu'elles sont des acteurs incontournables de l'action publique. Par conséquent, il est impossible d'évaluer le niveau d'exposition aux risques de ces dernières, ainsi que le coût engendré. Or, ces interrogations sont particulièrement légitimes, au vu de la structure du marché actuel. En effet, 3 grandes entreprises américaines en situation de quasi-monopole sur le numérique, Amazon Web Services (AWS), Microsoft Azure et Google Cloud, représentent à elles seules 70% des parts de marché en Europe, tandis que la part des fournisseurs de cloud européens a connu une diminution au cours des dernières années, représentant 27 % des parts en 2017 puis seulement 16 % en 2021. Par ailleurs, malgré une volonté affichée des pouvoirs publics de promouvoir des solutions alternatives, ces dernières restent largement dépendantes de solutions étrangères : à titre d'illustration, la conclusion par le ministère de l'éducation nationale et de la jeunesse d'un accord cadre pour le renouvellement de ses licences Microsoft en mars 2025, proposant des outils bureautiques et des prestations d'hébergement en nuage est très critiquée : interrogé dans le cadre de la commission d'enquête sénatoriale sur "les coûts et les modalités effectifs de la commande publique et la mesure de leur effet d'entraînement sur l'économie française" adopté le 8 juillet 2025, M. Anton Carniaux, directeur des affaires publiques et juridiques de Microsoft France, a avoué que son entreprise ne pouvait pas garantir que les données hébergées ne soit jamais transmises à des autorités étrangères – ce qui pose la question de l'extraterritorialité.

En effet, de nombreuses législations étrangères permettent aux États les ayant mises en place de récupérer les données collectées par les entreprises, même lorsque cette récolte a été effectuée à l'étranger. A titre d'illustration, aux Etats-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. Face à cela, il est donc indispensable de développer l'usage de nouveaux outils permettant de garantir un accès souverain aux données, parfois très sensibles, hébergées par les administrations publiques afin de préserver notre souveraineté numérique. En l'absence de telles mesures, notre pays risque de devenir une véritable "colonie numérique" de puissances étrangères, annihilant ainsi notre capacité même à agir. Cette situation n'est pas tolérable.