ASSEMBLÉE NATIONALE

19 février 2026

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

Tombé

N° CL5

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 Élisa 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 3, insérer l’alinéa suivant :

« I *bis*. – Les titulaires de marchés retenus par les entités mentionnées au I du présent article ne peuvent être que des structures publiques qui 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. Les titulaires de ces marchés doivent également s’assurer de prendre toutes les mesures indispensables pour se prémunir de tout effet extraterritorial d’une législation étrangère qui aboutirait à les contraindre à communiquer ou à transférer d’une manière ou d’une autre ces données à des autorités étrangères. »

EXPOSÉ SOMMAIRE

Par cet amendement, le groupe LFI souhaite réaffirmer la nécessité de protéger les données numériques des citoyennes et citoyens récoltées par les différents acteurs publics, en ayant systématiquement recours à des solutions développées par des structures publiques nationales, et qui prévoient un hébergement des données sur des serveurs régis par le droit national et/ou européen 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 désormais 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.

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 transmise à des autorités étrangères – ce qui pose la question de l'extraterritorialité.

Dans ce contexte, et s'afin de s'assurer que la France continue d'avoir un accès souverain aux données numériques qu'elle a collectées, il nous semble indispensable d'avoir recours à des solutions développées par des structures publiques - d'autant plus qu'elles existent. A titre d'illustration, l'État a développé deux offres de services d'hébergement et de traitement des données entièrement maîtrisés par des ressources internes, incluant l'hébergement, l'ingénierie, l'exploitation et la surveillance des données sensibles, exploitées et surveillées par le ministère de l'Intérieur (cloud Pi), initialement associé à un niveau de sécurité « Diffusion restreinte » ou encore le ministère des finances (cloud Nubo) associé au standard SecNumCloud - qui garantit un haut niveau d'exigences tant du point de vue technique, qu'opérationnel ou juridique car protégée des législations extra-territoriales et donc un niveau de sécurité de la solution dans son ensemble.