

**ASSEMBLÉE NATIONALE**

27 janvier 2024

---

**ENCADRER L'INTERVENTION DES CABINETS DE CONSEIL PRIVÉS DANS LES  
POLITIQUES PUBLIQUES - (N° 2112)**

Commission	
Gouvernement	

Rejeté

**AMENDEMENT**

N° 138

présenté par

Mme Le Hénanff, M. Patrier-Leitus, M. Christophe, M. Valletoux, M. Plassard, M. Lamirault,  
Mme Kochert, M. Thiébaud, M. Lemaire, Mme Rauch, Mme Carel, M. Jolivet, M. Marcangeli,  
Mme Bellamy, M. Pradal, Mme Félicie Gérard, M. Gernigon et Mme Violland

-----

**ARTICLE ADDITIONNEL****APRÈS L'ARTICLE 18, insérer l'article suivant:**

I. – Lorsque l'objet ou les caractéristiques du marché nécessitent le traitement de données d'une sensibilité particulière, définies au III, qu'elles soient à caractère personnel ou non, et si leur violation est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé ou à la vie des personnes ou à la protection de la propriété intellectuelle, l'administration bénéficiaire veille à ce que le prestataire et les consultants mettent en œuvre des critères de sécurité et de protection des données garantissant notamment la protection des données traitées ou stockées contre tout accès non autorisé par des autorités publiques d'États en dehors de l'Union européenne.

II. – On entend par administration bénéficiaire les administrations de l'État ou ses opérateurs, dont la liste est annexée au projet de loi de finances et qui ont recours aux prestations de conseil définies au II de l'article 1<sup>er</sup> de la présente loi.

III. – Sont qualifiées de données d'une sensibilité particulière au sens du I :

1° Les données qui relèvent de secrets protégés par la loi, notamment au titre des articles L. 311-5 et L. 311-6 du code des relations entre le public et l'administration ;

2° Les données nécessaires à l'accomplissement des missions essentielles de l'État, notamment la sauvegarde de la sécurité nationale, le maintien de l'ordre public et la protection de la santé et de la vie des personnes.

IV. – Un décret en Conseil d'État précise les modalités d'application du présent article, notamment les critères de sécurité et de protection, y compris en termes de détention capitalistique, des données

mentionnés au III et les conditions dans lesquelles une dérogation peut être accordée par le Premier ministre.

### EXPOSÉ SOMMAIRE

La circulaire du 5 juillet 2021 relative à l'application de la doctrine d'utilisation de l'informatique en nuage par l'État actualisée par la circulaire du 31 mai 2023 fait du cloud le mode d'hébergement et de production par défaut des services numériques de l'État et impose des critères stricts de sécurité pour les cloud proposés par les industriels à l'État. Pour chaque produit numérique manipulant des données, à caractère personnel ou non, d'une sensibilité particulière et dont la violation est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé et la vie des personnes ou à la protection de la propriété intellectuelle, l'offre de cloud commerciale retenue doit impérativement respecter la qualification SecNumCloud établie par l'ANSSI et être immunisée contre tout accès non autorisé par des autorités publiques d'État tiers.

Par ailleurs, l'article 10 bis A du projet de loi sécuriser et réguler l'espace numérique, voté à une large majorité en séance publique en octobre dernier, a souhaité établir des règles sur le recours à des prestataires d'informatique en nuage pour l'administration de l'État ou ses opérateurs lorsque les données concernées sont d'une sensibilité particulière.

De même, la commission d'enquête du Sénat sur l'influence croissante des cabinets de conseil privés sur les politiques publiques a établi que les cabinets de conseil sont destinataires de données pouvant présenter un caractère sensible, comme en témoigne par exemple la mission de réorganisation du service de santé des armées (2018-2021) menée par des consultants au cours du quinquennat précédent.

La problématique de la maîtrise des données des administrations et la perte de souveraineté numérique française a été relevée de nombreuses fois, notamment dans le rapport de la mission d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne » (2021).

Ainsi, en cohérence avec les efforts de protection des données sensibles de l'État, les administrations concernées par des prestations de conseils devraient être tenues d'avoir recours à des cabinets de conseils garants des mêmes critères de sécurité.

L'absence de règles spécifiques de sécurité pour les prestations de conseil qui traitent des données particulièrement sensibles constituerait une brèche majeure pour la protection des données de l'administration.