…la proposition de loi relative à

LA SÉCURISATION DES MARCHÉS PUBLICS NUMÉRIQUES

La proposition de loi n° 8 (2025-2026) *relative à la sécurisation des marchés publics numériques*, inscrite à l'ordre du jour réservé du groupe Les Indépendants – République et Territoire (LIRT) entend **renforcer le niveau de protection des données hébergées en nuage par les acheteurs publics**. La commission d'enquête[1] issue du droit de tirage de ce même groupe a en effet mis en lumière **les risques d'interception par des autorités étrangères** de ces données du fait des législations non-européennes à portée extraterritoriale.

Dans un contexte géopolitique incertain, la volonté de préserver les données françaises fait consensus et rejoint d'ailleurs un ensemble de dispositions réglementaires et législatives adoptées ces dernières années afin de protéger les données dites « sensibles ». Pour autant, la rapporteure a souligné que le périmètre retenu par l'article unique présentait des limites tant d'un point de vue juridique qu'opérationnel.

En conséquence**, la commission a restreint le périmètre du dispositif** afin de le rendre cohérent avec la nature du risque encouru et elle a tenu compte des difficultés, notamment financières et techniques, qu'il pourrait présenter pour certaines collectivités, afin de garantir sa bonne application.

1. LE RECOURS À DES PRESTATAIRES ÉTRANGERS CONSTITUE UN RISQUE POUR LA SOUVERAINETÉ DES DONNÉES HÉBERGÉES EN NUAGE

A. LES GRANDS PRESTATAIRES DE *CLOUD* ÉTRANGERS SONT SOUMIS À DES LÉGISLATIONS À PORTÉE EXTRATERRITORIALE

La commission d'enquête sur les coûts et les modalités effectifs de la commande publique et la mesure de leur effet d'entraînement sur l'économie française a mis en lumière la dépendance des administrations françaises aux solutions informatiques proposées par des acteurs extra-européens. Cette situation est source de vulnérabilités pour les données publiques hébergées chez ces acteurs, en raison de leur soumission à un cadre juridique de nature extraterritorial. De fait, certaines législations étrangères peuvent compromettre **la souveraineté et la confidentialité des données hébergées en nuage** :

- **Aux États-Unis,** le *Foreign Intelligence Surveillance Act* (FISA), l'*Executive Order 12.333* et le *Clarifying Lawful Overseas Use of Data (Cloud) Act* permettent aux autorités américaines de contraindre un fournisseur de services informatiques à distance à lui dévoiler toute communication ou information concernant un client se trouvant en sa possession, que cette donnée se trouve ou non aux États-Unis.

[1] L'urgence d'agir pour éviter la sortie de route : piloter la commande publique au service de la souveraineté économique, rapport n° 830 (2024-2025) fait par Simon Uzenat (Président) et Dany Wattebled (rapporteur) au nom de la commission d'enquête sur les coûts et les modalités effectifs de la commande publique et la mesure de leur entraînement sur l'économie française, déposé le 8 juillet 2025.

- **En Chine**, la loi sur le renseignement national impose aux citoyens et aux entreprises de « *soutenir, assister et coopérer aux efforts des services de renseignement nationaux […] tant à l'intérieur qu'à l'extérieur du pays* ».
- **En Inde**, le *Digital Personnal Data Protection Act* prévoit également que toute personne responsable du traitement de données est tenue de communiquer à l'État les données qu'il détient, lorsque cette donnée est nécessaire à l'exercice d'une fonction légale, contribue à la sécurité, la souveraineté et l'intégrité du pays, ou au maintien de l'ordre public.

B. LA FRANCE DISPOSE D'UN CADRE JURIDIQUE PRÉCURSEUR EN MATIÈRE DE PROTECTION DES DONNÉES DES ENTITÉS PUBLIQUES

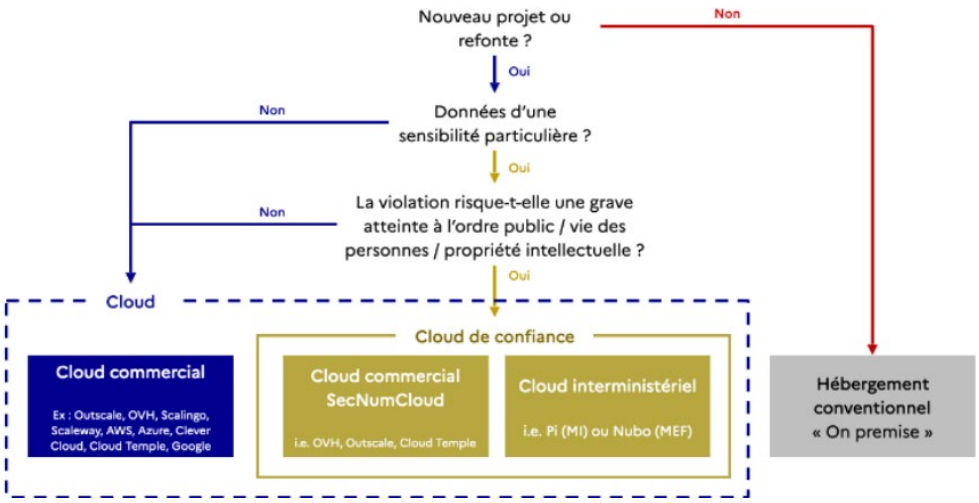
Afin de se prémunir contre les risques d'interception de données européennes à la demande d'autorités étrangères, l'Union européenne et la France ont renforcé leur cadre juridique au cours des dernières années.

Au niveau communautaire, les exigences en matière de protection des données relèvent essentiellement du **règlement général sur la protection des données**[1] (RGPD) qui interdit le transfert de données vers tout État tiers pour lequel la Commission n'aurait pas reconnu une équivalence de protection des données.

En France, depuis 2023, **la doctrine « *cloud* au centre »** prévoit le recours à **des prestataires souverains** et immuns aux législations étrangères pour l'hébergement des données sensibles des services et des organisations publiques. L'immunité des solutions d'hébergement contre toute règlementation extraterritoriale est notamment garantie par le recours à des offres disposant de **la qualification SecNumCloud**. Délivrée par l'agence nationale de sécurisation des systèmes d'information (ANSSI), cette certification atteste d'un haut niveau d'exigences d'un point de vue technique, opérationnel ou juridique et donc d'un niveau de sécurité globale, notamment en matière de protection face à l'application de lois extraterritoriales.

Par son article 31, **la loi visant à sécuriser et réguler l'espace numérique** (SREN)[2] a transcrit ces obligations réglementaires au niveau législatif, **faisant de la France le premier État de l'Union européenne s'étant doté d'un tel niveau de protection des données publiques**.

Schéma de prise de décision concernant l'offre d'hébergement adapté selon la doctrine *cloud au centre* et l'article 31 de la loi SREN



Source : Direction interministérielle du numérique.

[1] Règlement (UE) 2016/6709 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD).

[2] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et réguler l'espace numérique.

2. LA PROPOSITION DE LOI VISE À PROTÉGER L'ENSEMBLE DES DONNÉES PUBLIQUES DU RISQUE DE CAPTATION

La commission d'enquête sénatoriale sur le coût et les modalités effectifs de la commande publique a néanmoins constaté, d'une part, que les récentes avancées règlementaires et législatives visant à renforcer la souveraineté des données peinent à être pleinement appliquées par les entités publiques qui y sont assujetties et, d'autre part, que ce cadre normatif demeure insuffisant face à l'étendue des risques de captation des données par des États tiers. Le rapporteur de la commission d'enquête et auteur de la présente proposition de loi, Dany Wattebled, a ainsi souhaité transcrire dans la loi les conclusions des travaux conduits.

En conséquence, l'article unique de la proposition de loi vise à rendre obligatoire, pour les marchés publics comportant des prestations d'hébergement et de traitement des données publiques en nuage, l'introduction, par l'acheteur public, de conditions d'exécution du marché garantissant :

- d'une part, **la non-application d'une législation étrangère à portée extraterritoriale** de nature à contraindre le titulaire à communiquer ou à transférer ces données à des autorités étrangères ;
- d'autre part, **l'hébergement de ces données sur le territoire de l'Union européenne** dans des conditions assurant leur protection contre toute ingérence par des États tiers.

Le dispositif proposé représente donc une **évolution substantielle du cadre juridique français** : alors qu'en l'état du droit, seules les données d'une sensibilité particulière des administrations et des opérateurs de l'État doivent faire l'objet d'un hébergement souverain et immun aux législations extraterritoriales, **l'article unique entend imposer de telles obligations pour toute donnée publique détenue par les acheteurs publics, y compris les collectivités locales**.

3. L'AVIS DE LA COMMISSION : UN OBJECTIF LÉGITIME MAIS QUI DOIT ÊTRE CONCILIÉ AVEC LES EXIGENCES EUROPÉENNES ET LES CONTRAINTES OPÉRATIONNELLES DES ACHETEURS PUBLICS

Selon Olivia Richard, rapporteure, le dispositif proposé, s'il témoigne d'une volonté politique légitime au vu des conclusions alarmantes de la commission d'enquête, soulève néanmoins un certain nombre **de difficultés juridiques et opérationnelles**.

Les travaux conduits préalablement à l'examen du texte ont permis de démontrer que si la prépondérance d'acteurs étrangers sur le marché de l'hébergement en nuage est avérée à l'échelle de l'Union européenne, **ce constat est à nuancer s'agissant des administrations publiques françaises**, qui s'adaptent progressivement aux nouvelles obligations d'hébergement souverain.

des parts du marché de *cloud* en Europe sont captées par trois entreprises américaines

des nouveaux marchés publics de l'État retiennent des solutions souveraines

A. UN RISQUE DE NON-CONFORMITÉ DES MARCHÉS PUBLICS AUX EXIGENCES DE NON-DISCRIMINATION ET D'ÉGALITÉ DE TRAITEMENT

En premier lieu, les obligations nouvelles que l'article unique entend imposer dans tous les marchés publics présentent **un risque d'inconventionnalité et d'inconstitutionnalité**. En effet, le dispositif proposé, conduisant indirectement à écarter les acteurs non-européens de la commande publique de *cloud,* pourrait s'apparenter à une discrimination en raison de la nationalité du fournisseur. Or, les textes français et européens, ainsi que les engagements internationaux de la France, notamment l'accord sur les marchés publics de l'OMC, n'admettent de telles restrictions d'accès que lorsque celles-ci sont prévues en raison d'un motif impérieux d'intérêt général.

Cependant, selon l'ANSSI, toutes les données détenues par des entités publiques ne présentent par le même intérêt pour des puissances étrangères, et ne connaissent donc pas le même besoin de protection. Dès lors, **les restrictions d'accès à certains marchés publics d'hébergement de données peu sensibles apparaissent disproportionnées**.

B. DES OBLIGATIONS NOUVELLES POUR LES ACHETEURS PUBLICS QUI POURRAIENT ÊTRE SOURCES DE DIFFICULTÉS

En second lieu, **les obligations créées par l'article unique semblent trop importantes et complexes** pour être mises en œuvre par l'ensemble des acheteurs publics.

Alors que la commission d'enquête sur les coûts et les modalités effectifs de la commande publique a mis en avant les difficultés rencontrées par les petits acheteurs publics pour se conformer aux exigences du code de la commande publique, l'introduction de conditions d'exécution relatives au domaine d'application de lois étrangères extraterritoriales en matière numérique sera inévitablement complexe pour les petites collectivités, qui ne comptent, le plus souvent, pas d'acheteur professionnel au sein de leur équipe.

La rédaction de l'article unique présente en outre certaines imprécisions – car elle ne définit notamment pas clairement le terme de donnée publique – et engendre ainsi **un risque de confusion** pour les acheteurs quant au périmètre de données à protéger.

Enfin, l'obligation de recourir à un prestataire souverain présentant de fortes garanties de sécurité risque d'engendrer **un surcoût** pour ces acheteurs. Les tarifs des offres qualifiées SecNumCloud présentent en effet des coûts supérieurs par rapport aux offres non qualifiées d'un même prestataire, **de l'ordre de 25 % à 40 %**[1]**.** Au regard de l'état des finances locales, l'application indifférenciée du dispositif à l'ensemble des collectivités serait problématique.

C. DES EFFETS INCERTAINS SUR LES ENTREPRISES FRANÇAISES

Selon l'Autorité de la concurrence, le recours obligatoire de l'ensemble des acheteurs publics à des prestataires souverains hautement sécurisés, disposant par exemple de la qualification SecNumCloud, pourrait de surcroît avoir des **effets contre-productifs pour l'émergence d'acteurs français et européens**. Les coûts d'investissement nécessaires à l'obtention d'une telle qualification sont en effet susceptibles d'exclure du marché les entreprises européennes émergentes.

D. EN CONSÉQUENCE, LA RAPPORTEURE A PROPOSÉ UNE ÉVOLUTION DU PÉRIMÈTRE ET DE LA PORTÉE DU DISPOSITIF

Devant les limites juridiques et opérationnelles soulevées par la proposition de loi**, la commission a adopté un amendement de la rapporteure visant à recentrer le dispositif** et ainsi permettre **une mise en œuvre progressive et réaliste**.

Afin de se conformer au cadre juridique français et européen en matière de commande publique, la commission a premièrement **limité le dispositif aux seules données sensibles**, selon la définition retenue par l'article 31 de la loi SREN. Pour rappel, cet article est aujourd'hui uniquement applicable aux administrations de l'État et aux opérateurs publics.

[1] Observations définitives de la Cour des comptes sur les enjeux de souveraineté des systèmes d'informations civils de l'État, publié le 31 octobre 2025.

La commission a également restreint le nombre d'entités soumises à ces obligations de protection, en excluant les communes de moins de 30 000 habitants et les communautés de communes qui risqueraient de ne pas disposer de ressources humaines et techniques suffisantes afin d'adapter leurs marchés publics, et pour lesquelles le risque d'interception des données par une autorité publique étrangère est, selon l'ANSSI, plus faible. Ces entités ont d'ailleurs également été exemptées des obligations nouvelles en matière de cybersécurité prévues par le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, en cours d'examen à l'Assemblée nationale.

Afin de tenir compte des enjeux de développement des marchés français et européen de *cloud*, **la commission a fixé la date d'entrée en vigueur du dispositif au 1er janvier 2030**. Durant cette période, les prestataires souverains devraient être en mesure de développer une offre à moindre coût et de se préparer à une hausse des sollicitations dans le cadre des achats publics.

Enfin, au regard des difficultés techniques ou financières que pourraient rencontrer les collectivités pour se conformer aux exigences de protection souveraine de leurs marchés, **la commission a créé un mécanisme de dérogation au présent dispositif**, avec la volonté de garantir ainsi une trajectoire de sécurisation des données publiques progressive et réaliste.

La commission **a adopté la proposition de loi ainsi modifiée.**
Ce texte sera examiné par le Sénat en séance publique **le 17 décembre 2025.**

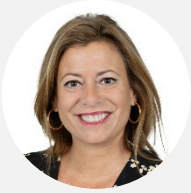
POUR EN SAVOIR +

- **Rapport de la commission d'enquête sur les coûts et les modalités effectifs de la commande publique et la mesure de leur effet d'entraînement sur l'économie française, juillet 2025.**
- **Rapport de la Cour des comptes sur les enjeux de souveraineté des systèmes d'information civils de l'État, octobre 2025.**
- **Rapport de l'ANSSI sur l'état de la menace informatique en matière de *cloud computing,* février 2025.**
- **Avis de l'autorité de la concurrence sur le fonctionnement concurrentiel du secteur du *cloud*, juin 2023.**

Muriel Jourda

Présidente de la commission

Sénateur (Les Républicains) du Morbihan



Olivia Richard

Rapporteure

Sénatrice (Union centriste) représentant les Français établis hors de France

Commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale

Téléphone : 01.42.34.23.37

Consulter le dossier législatif : https://www.senat.fr/dossier-legislatif/ppl25-008.html