N° 199

SÉNAT

SESSION ORDINAIRE DE 2025-2026

Enregistré à la Présidence du Sénat le 10 décembre 2025

RAPPORT

FAIT

au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur la proposition de loi relative à la **sécurisation** *des* **marchés publics numériques***,*

Par Mme Olivia RICHARD,

Sénatrice

(1) Cette commission est composée de : Mme Muriel Jourda*, présidente ;* M. Christophe-André Frassa, Mme Marie-Pierre de La Gontrie, M. Marc-Philippe Daubresse, Mmes Laurence Harribey, Isabelle Florennes, Patricia Schillinger, Cécile Cukierman, MM. Dany Wattebled, Guy Benarroche, Michel Masset*, vice-présidents ;* Mmes Marie Mercier, Jacqueline Eustache-Brinio, Lauriane Josende, M. Olivier Bitz*, secrétaires ;* M. Jean-Michel Arnaud, Mme Nadine Bellurot, MM. Jean-Baptiste Blanc, François Bonhomme, Hussein Bourgi, Mme Sophie Briante Guillemont, M. Ian Brossat, Mme Agnès Canayer, MM. Christophe Chaillou, Mathieu Darnaud, Mmes Catherine Di Folco, Françoise Dumont, MM. Patrick Kanner, Éric Kerrouche, Henri Leroy, Stéphane Le Rudulier, Mme Audrey Linkenheld, MM. Alain Marc, David Margueritte, Hervé Marseille, Thani Mohamed Soilihi, Mme Corinne Narassiguin, M. Paul Toussaint Parigi, Mme Anne-Sophie Patru, M. Hervé Reynaud, Mme Olivia Richard, MM. Teva Rohfritsch, Pierre-Alain Roiron, Mme Elsa Schalck, M. Francis Szpiner, Mmes Lana Tetuanui, Dominique Vérien, M. Louis Vogel, Mme Mélanie Vogel.

Voir les numéros :

Sénat : **8** et **200** (2025-2026)

SOMMAIRE

Pages

L'ESSENTIEL

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.

I. 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

[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.*

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.

- **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.

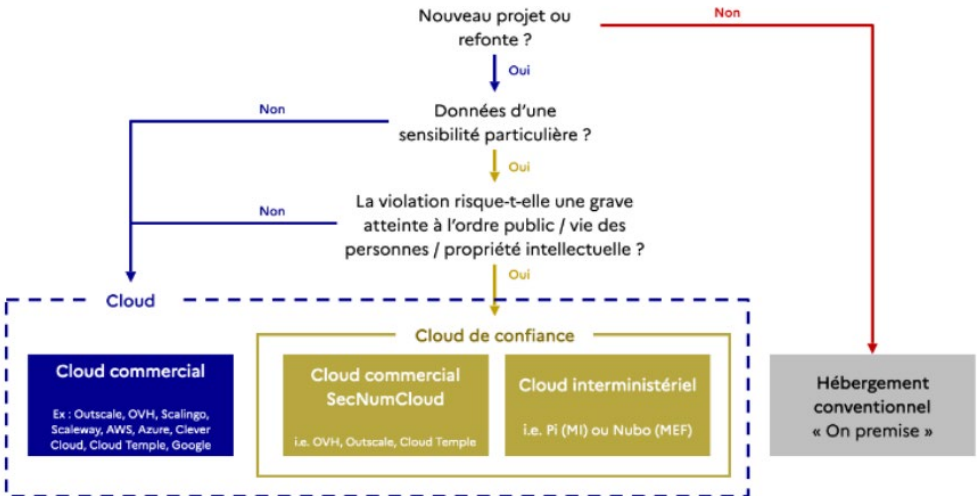
Au niveau communautaire, les exigences en matière de protection des données relèvent essentiellement du **règlement général sur la protection des données**[1] (RGPD) qui interdit le transfert de données vers tout État tiers pour lequel la Commission n'aurait pas reconnu une équivalence de protection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

[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).*

Par son article 31, **la loi visant à sécuriser et réguler l'espace numérique** (SREN)[1] 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.

II. 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.

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

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**.

III. 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.

---

[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.*

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.

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.

EXAMEN DE L'ARTICLE UNIQUE

Article unique

Préserver les données publiques hébergées en nuage du risque de captation par des autorités publiques extra-européennes

L'article unique de la proposition de loi entend rendre obligatoire, au sein des marchés publics comportant des prestations d'hébergement et de traitement de données publiques en nuage, des conditions d'exécution excluant l'application d'une législation étrangère à portée extraterritoriale de nature à contraindre le titulaire du marché à communiquer ces données à des autorités étrangères et garantissant l'hébergement de ces données sur le territoire de l'Union européenne.

Ce dispositif est la transcription législative de la recommandation n° 24 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, dont le rapporteur était Dany Wattebled, auteur de la proposition de loi.

Dans un contexte géopolitique incertain, la volonté de protéger 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, au regard du périmètre retenu par l'article unique, la rapporteure a estimé que ce dernier serait de nature à compromettre, d'une part, le respect du droit de la commande publique, qui proscrit toute forme de discrimination en raison de l'origine du produit et du fournisseur, ainsi que, d'autre part, les engagements internationaux de la France et de l'Union européenne dans le cadre de leur participation à l'OMC. La rapporteure a en outre rappelé que la commission d'enquête à l'origine de la présente proposition de loi recommandait également de ne plus adopter de normes freinant l'action des acheteurs publics. Dès lors, suivant cette analyse, 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. L'état du droit : si le droit de la commande publique proscrit la discrimination de candidats en raison de leur origine, la législation sectorielle européenne et française en matière de protection des données va dans le sens d'une vigilance accrue quant au choix du fournisseur d'hébergement en nuage

a) Des législations étrangères de portée extraterritoriale peuvent constituer une menace pour la souveraineté des données françaises

L'hébergement en nuage, ou *cloud*, est défini par l'agence nationale de la sécurité des systèmes d'information (ANSSI) comme **une pratique consistant à héberger certaines ressources informatiques dans un centre de données accessibles à distance à travers Internet**, plutôt que dans un système d'information local (« *on-premise* »). Dans son rapport sur l'état de la menace

informatique[1], l'agence observe que le *cloud*, de plus en plus sollicité dans le cadre de la transformation numérique, fait l'objet d'un nombre croissant d'actes malveillants, à des fins d'espionnage, de déstabilisation, de sabotage ou encore à des fins lucratives.

À cet égard, alors que 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[2] a mis en évidence **une dépendance généralisée des acheteurs publics à des prestataires extra-européens pour les prestations de *cloud***, l'ANSSI souligne que le recours à ces acteurs étrangers présente plusieurs risques spécifiques, liés à **la soumission de ces derniers à des lois à portée extraterritoriale,** notamment en matière de confidentialité des données hébergées.

L'extraterritorialité peut être définie comme « ***la situation dans laquelle les compétences d'un État (législatives, exécutives ou juridictionnelles) régissent des rapports de droit situés en dehors du territoire dudit État*** »[3] ou « *le fait pour l'État d'appréhender à travers son ordre juridique des situations extérieures à son territoire* »[4].

Aux États-Unis, le cadre législatif extraterritorial soumet ainsi les entreprises à certaines obligations de communication, y compris lorsqu'elles opèrent en dehors du territoire national :

- la section 702 du ***Foreign Intelligence Surveillance Act (Fisa)*** 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.

- la section 103 ***Clarifying Lawful Overseas Use of Data (Cloud) Act*** habilite le gouvernement américain à contraindre un fournisseur de services de communications électroniques ou de services informatiques à distance à « *préserver, sauvegarder ou lui dévoiler le contenu d'une communication électronique et tout enregistrement ou toute autre information concernant un client ou un abonné et se trouvant en sa possession, sous sa garde ou sous son contrôle, que cette communication, cet enregistrement ou cette information se trouve ou non aux États-Unis* ». L'émission d'un mandat de perquisition par un juge américain est toutefois nécessaire, ce qui implique l'existence d'un motif raisonnable de penser que les informations à collecter peuvent constituer des preuves utiles dans le cadre d'une enquête en cours sur un crime relevant de la juridiction des États-Unis. Le champ des données dont la communication

---

[1] Cloud computing, État de la menace, agence nationale de la sécurité des systèmes d'information, 19 février 2025.

[2] 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) déposé le 8 juillet 2025.

[3] *J. Salmon (dir.),* Dictionnaire de droit international public*, 2001, article « Extraterritorialité ».*

[4] *B. Stern, « Quelques observations sur les règles internationales relatives à l'application extraterritoriale du droit »,* Annuaire français de droit international*, vol. 32, 1986.*

est susceptible d'être exigée en application du *Cloud Act* est particulièrement large et inclut, par exemple, les données hébergées par les filiales d'entreprises américaines domiciliées en dehors des États-Unis ou par des entreprises non américaines ayant des clients américains.

- **L'*Executive Order 12.333*** autorise également la collecte de renseignements à l'étranger, y compris par des moyens techniques tels que la surveillance électronique et la collecte de données en masse.

La Chine renforce également depuis quelques années l'extraterritorialité de son droit. La commission d'enquête sénatoriale sur l'utilisation du réseau social TikTok, son exploitation des données et sa stratégie d'influence[1] mentionne à cet égard **la loi sur le renseignement national**, adoptée en 2017, comme un cadre juridique extraterritorial permettant la collecte de données étrangères. Son article 7 énonce notamment le devoir, pour les citoyens et les entreprises, de « *soutenir, assister et coopérer aux efforts des services de renseignement nationaux conformément à la loi, et protéger les secrets des services de renseignement nationaux dont ils ont connaissance* ». L'article 10 donne une portée extraterritoriale à cette disposition en précisant que « *dans la mesure où cela est nécessaire à leur travail, les services nationaux de renseignement doivent utiliser les moyens, les tactiques et les canaux nécessaires pour mener à bien leurs activités de renseignement, tant à l'intérieur qu'à l'extérieur du pays* ». Selon le rapport de la commission d'enquête[2], la combinaison des articles 7 et 10 peut laisser craindre que des données personnelles appartenant à des citoyens étrangers et détenues par des entreprises chinoises soient transmises aux services de renseignement chinois.

De la même manière, l'Inde a adopté, en août 2023, **le *Digital Personal Data Protection Act (DPDPA)***, s'appliquant hors des frontières indiennes. Le DPDPA prévoit que toute personne responsable du traitement des données, y compris en dehors du territoire national, est tenu de communiquer à l'État les données personnelles qu'il détient sans que le consentement ou l'information des personnes ne soit requis, notamment lorsque le traitement de cette donnée par l'État est nécessaire à l'exercice d'une fonction légale, contribue à la sécurité, la souveraineté et l'intégrité du pays ou est destiné à maintenir l'ordre public.

Comme l'a démontré la commission d'enquête sur les coûts et les modalités effectifs de la commande publique, ces législations **sont ainsi de nature à compromettre la souveraineté numérique de la France**, notamment en ce qu'elles peuvent conduire à l'interception de données françaises par des autorités étrangères.

---

[1] La tactique TikTok : opacité, addiction et ombres chinoises, rapport n° 831 (2022-2023) fait au nom de la commission d'enquête sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence, rapport déposé le 3 juillet 2023.

[2] *Voir la section I.B.2 « Une coopération inévitable avec les services de renseignement », page 25 et suivantes.*

Si la souveraineté est classiquement définie comme l'aptitude d'un État à exercer son autorité sur son territoire, à protéger ses citoyens et à garantir le respect de ses lois, la souveraineté numérique désigne ici **la capacité pour l'État à conserver un accès autonome à son espace numérique et aux services numériques liés à l'exercice de sa souveraineté,** en sécurisant son autonomie et l'accès aux contenus qu'il a définis comme stratégiques ou sensibles. Elle repose sur trois critères :

- **la souveraineté de la donnée**, c'est-à-dire la capacité de l'État à en disposer tout en assurant sa sécurisation vis-à-vis d'autrui ;
- **la souveraineté opérationnelle**, qui repose sur la fiabilité des structures traitant et hébergeant les données ;
- **la souveraineté technologique**, qui désigne l'absence de possibilité, pour un État tiers, de contraindre des prestataires de services numériques à refuser ou couper l'accès de certains utilisateurs nationaux clients.

Afin de se prémunir contre les effets des législations non-européennes de portée extraterritoriale, certaines entités choisissent de recourir à des méthodes de protection telles que le chiffrement, l'anonymisation ou la partition des données. Selon l'ANSSI, ces méthodes ne suffisent pas à garantir une protection adéquate contre les risques évoqués, notamment puisque les clés de chiffrement sont le plus souvent également hébergées en nuage.

Dès lors, **le seul recours à un prestataire souverain, non soumis aux législations étrangères, est une garantie sérieuse en matière de souveraineté**. Toutefois, les entités publiques, en leur qualité d'acheteur public, doivent, pour la sélection de leurs prestataires d'hébergement en nuage, concilier les exigences en matière de protection des données hébergées en nuage et celles de non-discrimination et de libre accès aux marchés publics propres à la commande publique.

b) L'union européenne a imposé un cadre juridique uniforme pour la protection des données personnelles et leur transfert vers des États tiers

(1) Le règlement général sur la protection des données (RGPD)

Au niveau communautaire, dès 1995, la directive 95/46 relative à la protection des données personnelles prévoit que « ***le transfert vers un pays tiers de données à caractère personnel [...] ne peut avoir lieu que si [...] le pays tiers en question assure un niveau de protection adéquat*** »[1]. Par la suite, le 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) a harmonisé les règles de traitement des données à caractère

[1] *Article 25 de la directive 95/46/CE du Parlement et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données.*

personnel au sein de l'Union européenne, et complété **les modalités de transfert ou de communication de celles-ci à des États extra-européens**.

Le RGPD affirme premièrement qu'il revient au responsable du traitement des données à caractère personnel de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constante des systèmes et des services de traitement[1]. Il impose également à ce dernier de notifier à l'autorité de contrôle compétente au niveau national, ainsi qu'à la personne concernée, tout incident ayant entraîné la violation de données à caractère personnel[2].

En outre, selon ce règlement, il revient à la Commission de constater qu'un pays tiers assure, en raison de sa législation interne ou de ses engagements internationaux, **un niveau de protection adéquat**[3], autorisant alors le transfert de données vers cet État.

En l'absence d'une telle décision d'adéquation, un transfert de données ne peut être réalisé que si l'exportateur des données à caractère personnel, établi dans l'Union, prévoit **des garanties appropriées**, pouvant notamment résulter de clauses types de protection des données adoptées par la Commission européenne, et **si les personnes concernées disposent de droits opposables et de voies de droit effectives**[4].

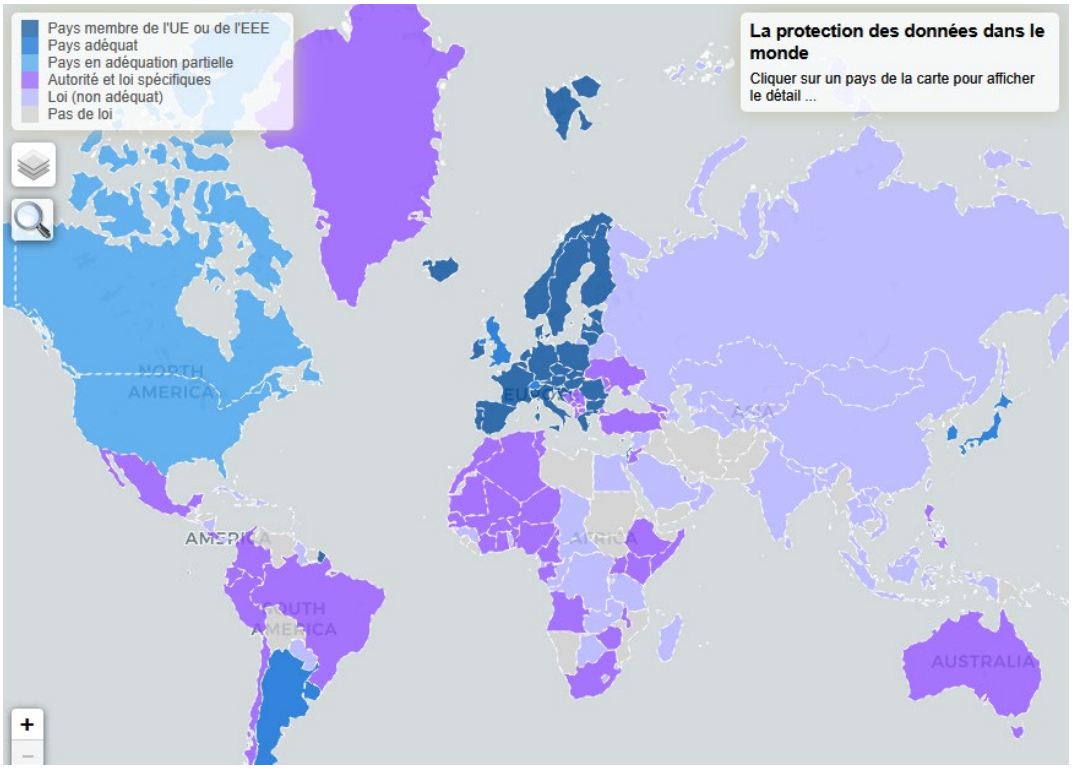
L'article 48 du règlement dispose en outre que **toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international,** tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre.

La Commission européenne a reconnu le caractère adéquat du niveau de protection de **15 États** hors de l'Union européenne.

---

[1] *Article 32.*
[2] *Article 33 et 34.*
[3] *Article 45 du RGPD.*
[4] *Article 46 du RGPD.*

États dont le niveau de protection des données est reconnu comme adéquat par la Commission européenne



Source : CNIL.

En raison de l'extraterritorialité des législations mentionnées ci-dessus, le niveau de protection des données assuré par les États-Unis fait l'objet de débats institutionnels depuis dix ans.

En effet, à deux reprises, la Commission a considéré que **les États-Unis assurent un niveau adéquat de protection aux données à caractère personnel transférées**, validant ainsi le principe de transferts de données de la part d'entreprises ou d'entités publiques européennes[1]. Toutefois, en 2015[2] puis en 2020[3], **la Cour de justice de l'Union européenne a invalidé ces décisions d'adéquation**.

[1] *Décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » publiés par le ministère du commerce des États-Unis d'Amérique (JO 2000,L 215) et décision de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis (JO 2016, L. 207).*

[2] *Arrêt de la Cour du 6 octobre 2015, Affaire C-362/14,* Maximillian Schrems contre Data Protection Commissioner.

[3] *Arrêt de la Cour du 16 juillet 2020, Affaire C-311/18,* Data Protection Commissioner/ Facebook Ireland Limited, Maximillian Schrems.

Dans son arrêt Schrems II[1] notamment, la CJUE a analysé la législation américaine en matière d'accès aux données des fournisseurs de services Internet et d'entreprises de télécommunication par les services de renseignement américains et a conclu que **les atteintes portées à la vie privée des personnes dont les données sont traitées par les entreprises et les opérateurs états-uniens sont disproportionnées au regard des exigences de la Charte des droits fondamentaux**. En particulier, la Cour a jugé que **la collecte de données par les services de renseignement n'est pas proportionnée** et que les voies de recours, y compris juridictionnelles, dont disposent les personnes à l'égard du traitement de leurs données sont insuffisantes.

Depuis, un nouveau cadre d'adéquation, le *Data Privacy Framework*, a été adopté en juillet 2021. Il consiste en un mécanisme d'auto-certification pour les entreprises états-uniennes[2]. La Commission européenne considère ainsi que les transferts de données à caractère personnel vers des entreprises américaines ayant reçu cette certification – dont par exemple Microsoft, Google, Amazon et Meta Platforms – présentent un niveau de protection adéquat. Aussi, en vertu de cet accord, **le transfert de données européennes à caractère personnel, notamment dans le cadre de prestations d'hébergement, demeure autorisé vers certaines entreprises des États-Unis**. Un premier recours contre le *Data Privacy Framework* a d'ailleurs été rejeté en septembre 2025 par la CJUE[3].

La Commission n'a en revanche pas reconnu l'adéquation de protection des données en Chine et en Inde. Les transferts de données personnelles vers des pays nécessitent en conséquence d'être encadrés par des outils de transfert spécifiques.

(2) Le règlement sur les marchés numériques (DMA) et le règlement sur la protection des données

Le règlement sur les marchés numériques du 14 septembre 2022 (DMA)[4] a également entendu réguler le pouvoir des entreprises informatiques internationales, tout particulièrement des grandes entreprises américaines, sur le marché européen, à des fins de souveraineté. S'il ne comprend pas d'obligations spécifiques aux services *cloud*, le DMA encadre indirectement la gestion des données par ces derniers, en prévoyant les obligations suivantes :

- l'interdiction de combiner les données à caractère personnel provenant d'un service de plateforme essentiel avec les données provenant de tout autre services[5] ;

---

[1] Ibid.

[2] *La liste des entreprises présentant des garanties suffisantes est présentée par le ministère américain du commerce. Voir* https://www.dataprivacyframework.gov/list .

[3] *Affaire T553-23* Philippe Latombe contre Commission européenne.

[4] *Règlement (UE) 2022/1925 relatif aux marchés contestables et équitables dans le secteur numérique modifiant les directives (UE) 2019/1937 et (UE) 2020/1828.*

[5] *Article 5(2) du règlement.*

- l'interdiction d'utiliser les données produites par les entreprises utilisatrices[1] ;
- l'obligation d'assurer la portabilité effective et gratuite des données fournies ou produites par l'utilisateur final[2].

Le règlement sur les données[3] adopté en 2023 contient en outre des mesures visant à garantir la possibilité de migrer entre différents fournisseurs de services en nuage de manière rapide, gratuite et technologiquement fluide. Elle prévoit également des garanties en matière de transferts internationaux de données, **en imposant aux fournisseurs de service de prendre toutes les mesures techniques, organisationnelles et juridiques afin d'empêcher l'accès des autorités publiques des pays tiers aux données à caractère non personnel** détenues dans l'Union (les données à caractère personnel étant déjà couvertes par le RGPD[4]).

(3) Les travaux de la Commission européenne en matière de sécurisation des données hébergées en nuage

Afin d'accompagner le transfert progressif du stockage de données sur des serveurs internes vers des hébergements en nuage de manière sécurisée et souveraine, la Commission européenne a par ailleurs engagé plusieurs travaux.

La proposition de règlement sur le développement de l'informatique en nuage, dont la présentation est annoncée pour fin 2025, doit, selon la Commission « *renforcer la souveraineté numérique de l'Europe dans le secteur de l'informatique en nuage* », par « *une proposition de politique unique en matière d'informatique en nuage à l'échelle de l'Union européenne pour les administrations publiques et les marchés publics* ». La Commission européenne indique ainsi vouloir constituer **un cadre européen unique contenant des règles contraignantes et non contraignantes pour les utilisateurs et les fournisseurs de service en nuage**, sous la forme d'un recueil de règles de l'Union européenne sur l'informatique en nuage et **d'orientations sur les marchés publics de service de traitement de données**.

Cette approche viserait ainsi à favoriser la croissance des fournisseurs européens d'informatique en nuage et **donner la priorité à l'utilisation de capacités d'informatique en nuage hautement sécurisées pour des cas d'utilisation hautement critiques**.

Dans le cadre du règlement sur la cybersécurité, l'agence européenne pour la cybersécurité (ENISA) travaille en outre à **un système européen de certification de cybersécurité pour les services en nuage dit EUCS.** Dans le cadre des négociations entre États membres pour l'adoption de la certification, **la France**

---

[1] *Article 6(2) du règlement.*
[2] *Article 6(9) du règlement.*
[3] *Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité d'accès aux données et de l'utilisation des données.*
[4] *Article 32 du règlement.*

s'est exprimée en faveur de l'inclusion de critères relatifs à la non-soumission de l'hébergeur à une législation extra-européenne susceptible de conduire à une captation de données par des pays tiers. Soutenue dans cette demande par l'association Gaia-X, initiative franco-allemande pour le développement d'un *cloud* européen, et par les ministres de l'économie allemand et italien, la France a obtenu, en 2023, l'ajout dans une version de travail d'un niveau « *high* + » reprenant les exigences du référentiel SecNumCloud présentées *infra.* Néanmoins, l'Allemagne s'est depuis éloignée de cette position, après l'annonce de la société AWS d'un investissement de 7,8 milliards d'euros dans un *cloud* « souverain » sur le territoire allemand, et plusieurs associations professionnelles américaines ont exprimé leur inquiétude auprès du gouvernement américain face à ce qu'ils décrivent comme « *une menace pour les intérêts économiques et la sécurité nationale des États-Unis* »[1]. Aussi, depuis avril 2024, le niveau « *high* + » ne figure plus dans les documents de travail des négociations conduites par l'agence.

Comme en témoigne sa mobilisation au sujet de la certification EUCS, **la France apparaît à l'échelle de l'Union européenne comme l'un des États membres les plus avancés en matière de souveraineté des données**. Le niveau de protection des données prévu en droit interne a ainsi été décrit par la direction interministérielle du numérique (Dinum) comme inégalé à l'échelle de l'Union européenne.

c) La France dispose d'un cadre normatif précurseur en Europe afin de protéger les données hébergées en nuage

En droit interne, devant les risques de violation de la confidentialité des données françaises hébergées en nuage par l'effet des législations étrangères, le législateur a affirmé, dès 2016, le principe selon lequel l'État, les collectivités territoriales, les autres personnels de droit public et les personnes de droit privé chargées d'une mission de service public devaient veiller à « ***préserver la maîtrise, la pérennité et l'indépendance de leurs systèmes d'information*** », et encourager l'utilisation de logiciels libres et de formats ouverts lors du développement, de l'achat ou de l'utilisation de tout ou partie de ces systèmes d'information[2].

En 2021, le Gouvernement a établi une **stratégie nationale pour le *cloud*** visant à faire émerger une alternative technologique française et européenne dans un contexte de croissance dynamique du secteur *cloud* à l'échelle mondiale et de prise de conscience des enjeux de souveraineté liés au recours à des prestataires étrangers dans ce domaine. La stratégie s'est déclinée en deux volets :

- **le soutien direct à des projets industriels** dans le cadre des programmes d'investissements d'avenir et de France Relance, à hauteur de 1,8 milliard d'euros, dont 667 millions d'euros de financement public ;

[1] *Cour des comptes p.25.*
[2] *Article 16 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.*

- **la définition d'une doctrine nationale** sur le recours à des « *cloud* de confiance », à destination des administrations publiques.

Pour ce second point, la circulaire du Premier ministre n° 628-SG du 5 juillet 2021 définit **la doctrine d'utilisation de l'informatique en nuage par l'État via la circulaire dite « *cloud* au centre »[1].** Rappelant que « *l'État doit veiller scrupuleusement à la protection de ses données et de celles des citoyens, et notamment à leur hébergement sur le territoire de l'Union européenne* », la circulaire incite les services et les organisations publiques à recourir à des solutions d'hébergement en nuage qui intègrent des exigences de réversibilité, de portabilité et d'interopérabilité[2] et qui « *n'entravent pas l'autonomie de l'État dans ses choix numériques à venir* ». La circulaire prévoit en outre **l'utilisation des offres de *cloud* de l'État pour l'hébergement des données sensibles** dont la compromission nuirait au bon fonctionnement de l'État.

Les offres *cloud* de l'État

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 »

- le ministère des finances (**cloud Nubo**) associé au standard SecNumCloud présenté ci-après.

Portées par le réseau interministériel de l'État, dont la raison d'être est d'assurer la continuité de l'État même en cas de défaillance majeure d'Internet, ces offres ont vocation à couvrir les besoins de *cloud* interne de l'ensemble des ministères et à héberger une instance de tout système d'information indispensable pour la continuité de l'État, à l'exception du ministère des Armées qui dispose de son propre *cloud* interne.

En outre, le ministère de l'Europe et des affaires étrangères, qui opère pour partie en dehors des frontières nationales du fait des services proposés aux français de l'étranger, a dû développer une stratégie numérique spécifique afin de sécuriser certaines opérations telles que le vote en ligne et la tenue du registre dématérialisé de l'état civil des français de l'étranger.

[1] *Circulaire du Premier ministre n° 6282/SG du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État (*« cloud au centre »).

[2] *Dans les contrats informatiques, la réversibilité désigne la faculté pour un client utilisateur d'un logiciel ou d'un système de récupérer ses données lors de la cessation du contrat. La portabilité correspond à la capacité de déplacer des données entre différents logiciels ou systèmes opérés par des fournisseurs distincts. Enfin, l'interopérabilité est la capacité des logiciels et des systèmes à échanger des données de manière sécurisée indépendamment des frontières géographiques ou organisationnelles, notamment entre différentes organisations.*

Pour ces contraintes particulières, le ministère dispose de deux centres de données (« *data centers* ») internes, situés à Paris et à Nantes. Cet hébergement interne permet notamment d'avoir un contrôle entier sur les données collectées et ainsi garantir la sécurité et la continuité des services, tout en se conformant aux cadres juridiques européens et français. Dans le cadre d'un contrat avec la structure parapublique *Voxaly* opérée par Docaposte qui assure la sécurisation des flux, le ministère et l'ANSSI garantissent le secret du vote par des dispositifs cryptographiques et de scellement numérique des données, sous le contrôle d'un auditeur externe.

Source : circulaire n° 628-SG du 5 juillet 2021 et audition de la direction du numérique du ministère de l'Europe et des affaires étrangères.

Cette doctrine a par la suite été actualisée en mai 2023[1] afin de renforcer les exigences relatives au *cloud* retenu par les administrations de l'État. Elle impose désormais, en cas de recours à une offre commerciale d'informatique en nuage, l'hébergement des données d'une sensibilité particulière par des solutions disposant de **la qualification SecNumCloud** et **immunisées contre toute règlementation extracommunautaire**.

La qualification SecNumCloud

SenNumCloud est une qualification de sécurité proposée par l'ANSSI à destination des opérateurs *cloud*, l'agence ayant constaté une intensification des attaques informatiques à destination des solutions d'hébergement en nuage depuis plusieurs années.

La qualification repose sur un ensemble de 360 règles de sécurité indissociables, garantissant un haut niveau d'exigences tant du point de vue technique, qu'opérationnel ou juridique et donc un niveau de sécurité de la solution dans son ensemble.

La qualification SecNumCloud vise notamment à assurer la protection face à l'application de lois extraterritoriales, afin de garantir la sécurité des données les plus sensibles hébergées dans le *cloud*. Le processus de qualification évalue notamment les facteurs qui permettront au prestataire qualifié de résister à une injonction de ce type. L'évaluation est basée sur la combinaison de trois types de mesures qui sont des critères de confiances envers la résilience des solutions : techniques (chiffrement, cloisonnement des systèmes d'information) organisationnelles (seul le prestataire qualifié peut intervenir sur les ressources supportant le service, et il assure un contrôle strict des accès de ses employés), juridiques (protection vis-à-vis du droit extra-européen). L'ensemble de ces exigences sont complémentaires pour assurer la sécurité des hébergements *cloud*. Dans sa version 3.2, la qualification a par ailleurs renforcé les exigences relatives à l'immunité aux lois non-européennes : le siège social du prestataire doit être situé dans le territoire de l'Union européenne, une entité non-européenne ne doit pas détenir à elle seule plus de 24 % du capital et des droits de vote du prestataire et,

[1] *Circulaire de la Première ministre n° 6404/SG du 31 mai 2023 relative à l'actualisation de la doctrine d'utilisation de l'informatique en nuage par l'État (*cloud au centre).

collectivement, plus de 39 %, enfin, la majorité des activités d'administration et de maintenance doivent être basées en Europe.

Plus d'une dizaine d'offres dispose de la qualification, et une quinzaine est en cours de qualification par l'ANSSI.

Source : données transmises par l'ANSSI.

La même année, à l'occasion de l'examen par le Sénat du projet de loi visant à sécuriser et à réguler l'espace numérique (SREN)[1], l'adoption d'un amendement de Catherine Morin-Desailly et Patrick Chaize a inscrit dans la loi les dispositions prévues par la doctrine *cloud* au centre.

L'article 31 de la loi SREN[2] impose ainsi aux administrations de l'État, à leurs opérateurs ainsi qu'à certains groupements d'intérêt publics qui ont recours à un service d'informatique en nuage pour le stockage ou l'hébergement de données d'une sensibilité particulière **de veiller à ce que le service informatique retenu dispose de critères de sécurité et de protection des données garantissant notamment la protection des données traitées ou stockées contre tout accès par des autorités publiques d'États tiers** non autorisé par le droit de l'Union européenne ou d'un État membre.

La qualification des données « d'une sensibilité particulière » entrant dans le périmètre de l'article relève **d'un double critère** :

- d'une part, sont qualifiées de données d'une sensibilité particulière **les données qui relèvent de secrets protégés par la loi et 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 ;

- d'autre part, ces données entrent dans le périmètre de l'article 31, qu'elles soient à caractère personnel ou non, 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**.

Les données qui relèvent de secrets protégés par la loi

Les secrets protégés par la loi sont notamment ceux mentionnés aux articles L. 311-5 et L. 311-6 du code des relations entre le public et l'administration (CRPA).

En vertu de l'article L. 311-5 du CRPA, ne sont pas communicables :

- les avis du Conseil d'État et des juridictions administratives, les documents de la Cour des comptes mentionnés à l'article L. 141-3 du code des juridictions financières et les documents des chambres régionales des comptes mentionnés aux articles L. 241-1 et L. 241-4 du même code, les documents élaborés ou détenus par l'Autorité de la concurrence dans le cadre de l'exercice de ses pouvoirs d'enquête,

[1] *Texte n° 593 (2022-2023) de M. Bruno Le Maire, ministre de l'économie, des finances et de la souveraineté industrielle et numérique, déposée au Sénat le 10 mai 2023.*
[2] *Loi n° 2024-449 du 21 mai 2024.*

d'instruction et de décision, les documents élaborés ou détenus par la Haute Autorité pour la transparence de la vie publique dans le cadre des missions prévues à l'article 20 de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique, les documents préalables à l'élaboration du rapport d'accréditation des établissements de santé prévu à l'article L. 6113-6 du code de la santé publique, les documents préalables à l'accréditation des personnels de santé prévue à l'article L. 1414-3-3 du code de la santé publique, les rapports d'audit des établissements de santé mentionnés à l'article 40 de la loi n° 2000-1257 du 23 décembre 2000 de financement de la sécurité sociale pour 2001 et les documents réalisés en exécution d'un contrat de prestation de services exécuté pour le compte d'une ou de plusieurs personnes déterminées ;

- les autres documents administratifs dont la consultation ou la communication porterait atteinte :

a) au secret des délibérations du Gouvernement et des autorités responsables relevant du pouvoir exécutif ;

b) au secret de la défense nationale ;

c) à la conduite de la politique extérieure de la France ;

d) à la sûreté de l'État, à la sécurité publique, à la sécurité des personnes ou à la sécurité des systèmes d'information des administrations ;

e) à la monnaie et au crédit public ;

f) au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, sauf autorisation donnée par l'autorité compétente ;

g) à la recherche et à la prévention, par les services compétents, d'infractions de toute nature ;

h) ou sous réserve de l'article L. 124-4 du code de l'environnement, aux autres secrets protégés par la loi.

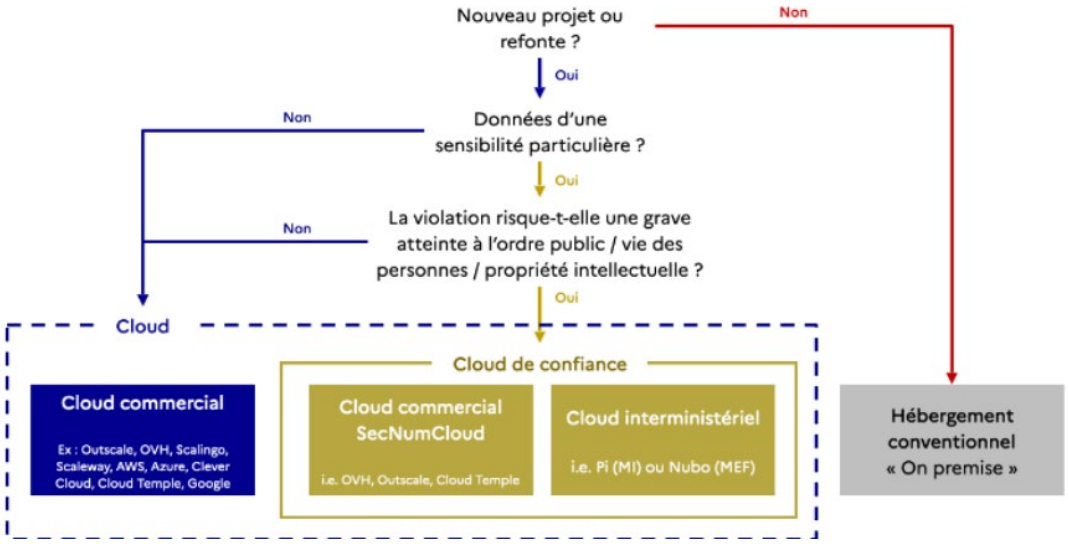
De plus, aux termes de l'article L. 311-6 du même code, ne sont communicables qu'à l'intéressé les documents administratifs :

- dont la communication porterait atteinte à la protection de la vie privée, au secret médical et au secret des affaires, lequel comprend le secret des procédés, des informations économiques et financières et des stratégies commerciales ou industrielles et est apprécié en tenant compte, le cas échéant, du fait que la mission de service public de l'administration mentionnée au premier alinéa de l'article L. 300-2 est soumise à la concurrence ;

- portant une appréciation ou un jugement de valeur sur une personne physique, nommément désignée ou facilement identifiable ;

- faisant apparaître le comportement d'une personne, dès lors que la divulgation de ce comportement pourrait lui porter préjudice.

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.

Il était prévu par la loi qu'un décret précise, dans un délai de six mois à compter de sa promulgation, les modalités d'application de l'article 31, notamment les critères de sécurité et de protection, y compris en termes de détention du capital, que doivent présenter les offres retenues pour l'hébergement des données sensibles, ainsi que les conditions dans lesquelles une dérogation peut être accordée.

Plus d'un an après la promulgation de la loi SREN, ce décret n'a toujours pas été publié. Selon les informations transmises à la rapporteure, le projet de décret serait, en décembre 2025, en cours d'examen par le Conseil d'État, et devrait être publié début 2026.

Comme le souligne la Cour des comptes dans ses observations sur les enjeux de souveraineté des systèmes d'information de l'État[1], alors que le projet de décret a été transmis par la France à la Commission européenne dans le cadre de la procédure d'information qui vise à empêcher la création d'obstacles au sein du marché intérieur, « *la période dite de statu quo permettant à la Commission et aux autres États membres d'examiner le texte notifié et de répondre de façon appropriée durait jusqu'au 28 avril 2025 et* ***aucune opposition n'a été émise dans ce délai*** ». Il apparaît ainsi que tout en imposant un périmètre de données protégées plus large que celui du RGPD – qui ne concerne que les seules données personnelles – le double critère permettant de déterminer la sensibilité des données restreint suffisamment le dispositif afin de ne pas constituer une entrave au principe de libre circulation des services de la société de l'information entre les États membres, exigence prévue par la

[1] *Avis rendu public au sein du rapport de la Cour des comptes sur les enjeux de souveraineté des systèmes d'informations civils de l'État, publié le 31 octobre 2025.*

directive 2000/31 sur le commerce électronique[1] et rappelée par la CJUE en 2023[2].

Dans l'attente de la parution de ce décret, les entités assujetties à l'article 31 de la loi SREN demeurent tenues d'en appliquer les principes. La Dinum a néanmoins indiqué avoir déjà prévu certaines dérogations, notamment concernant l'utilisation des suites bureautiques dans certains ministères ou organismes sous tutelles de l'État[3].

En complément des obligations imposées par la loi**, la commission nationale de l'informatique et des libertés (CNIL) émet régulièrement des recommandations relatives à la protection des bases de données personnelles les plus sensibles traitées par des organismes publics**. Elle a ainsi prononcé un avis défavorable concernant le choix du ministère de l'Éducation national d'avoir retenu un service américain pour la modernisation de son système informatique de ressources humaines dans le cadre du projet Virtuo en 2022[4], et a exposé, dans sa délibération n° 2020-044 du 20 avril 2020[5], ses réserves quant au recours par la plateforme des données de santé aux solutions d'hébergement fournies par Microsoft. La CNIL a également publié, en 2024, deux fiches pratiques relatives au chiffrement et à la sécurité des données dans l'informatique en nuage afin de sensibiliser les responsables de traitement aux problématiques d'hébergement par un prestataire soumis à des lois extracommunautaires.

La direction interministérielle du numérique (Dinum) contribue également à la sécurisation des données de l'État, en application de l'article 3 du décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique : **tout projet informatique dont le coût prévisionnel est supérieur à 9 millions d'euros lui est soumis pour avis conforme**, notamment afin d'assurer le respect de la doctrine « *cloud* au centre ».

Dès lors, sur le fondement des avancées législatives récentes, les entités publiques peuvent, pour l'hébergement de données dites sensibles, écarter les offres d'hébergement proposées par des acteurs non-européens qui, par définition, ne peuvent répondre aux exigences SecNumCloud. Néanmoins, elles sont tenues, pour le reste des prestations d'hébergement en nuage, de se conformer aux exigences prévues par le droit de la commande publique, qui interdit formellement la discrimination des opérateurs économiques en raison de leur nationalité ou de tout autre motif.

---

[1] *Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.*

[2] *CJUE, Affaire C-376/22 du 9 novembre 2023,* Google Ireland Limited contre le gouvernement autrichien.

[3] *Page 251 du rapport de la commission d'enquête sur les coûts et les modalités effectifs de la commande publique et leur effet d'entraînement sur l'économie française.*

[4] *Avis rendu public au sein du rapport de la Cour des comptes sur les enjeux de souveraineté des systèmes d'informations civils de l'État, publié le 31 octobre 2025.*

[5] *Délibération n° 2020-044 du 20 avril 2020 sur le fonctionnement du système de santé pour faire face à l'épidémie de covid-19.*

d) Le droit de la commande publique n'admet que dans des conditions très strictes les restrictions d'accès aux marchés publics

(1) Les marchés publics sont soumis aux impératifs de non-discrimination et d'égalité de traitement des candidats, indifféremment de leur origine ou de la localisation de leur production

Le cadre juridique de l'Union européenne proscrit de manière stricte toute forme de discrimination d'un prestataire dans le cadre de l'attribution d'un marché public, **le principe de non-discrimination étant consacré comme principe général du droit de l'Union par la Charte des droits fondamentaux**[1].

Le premier considérant de la directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics dispose ainsi que la passation de ces derniers « *doit être conforme aux principes du traité sur le fonctionnement de l'Union européenne […] ainsi qu'aux principes qui en découlent comme* ***l'égalité de traitement***, ***la non-discrimination***, ***la reconnaissance mutuelle***, ***la proportionnalité*** *et* ***la transparence*** ».

Le principe d'égalité de traitement interdit toute pratique discriminatoire de nature à favoriser certains opérateurs, dans la définition des prestations attendues, dans la façon dont l'acheteur fait connaître son besoin par ses modalités de publicité, dans l'ensemble des modalités selon lesquelles les candidats sont mis en concurrence, et dans la façon dont leurs offres sont appréciées. La non-discrimination implique quant à elle que tous les opérateurs puissent proposer leurs services pour répondre au besoin de l'acheteur, exception faite des cas d'interdiction de soumissionner.

Ces exigences sont également transposées en droit interne : le code de la commande publique précise ainsi que « ***les acheteurs respectent le principe d'égalité de traitement entre des candidats à l'attribution d'un contrat de la commande publique. Ils mettent en œuvre les principes de liberté d'accès et de transparence des procédures*** »[2]. Ces principes se sont en outre vus reconnaître une valeur constitutionnelle, le Conseil constitutionnel considérant qu'ils découlent des articles 6 et 14 de la Déclaration des droits de l'Homme et du citoyen[3].

(2) Des traités internationaux prévoient la réciprocité d'accès aux marchés publics

Le respect des principes de libre accès aux marchés publics et la non-discrimination se trouvent en outre confortés par un ensemble de règles internationales ainsi, qu'à l'échelle de l'Union, par plusieurs traités internationaux ratifiés par l'Union européenne qui prévoient la réciprocité d'accès des opérateurs économiques aux marchés publics des États signataires.

---

[1] *Article 21 de la Charte des droits fondamentaux de l'Union européenne.*
[2] *Article L. 3 du code de la commande publique.*
[3] *Conseil constitutionnel, 26 juin 2003, n° 2003-473 DC relative à la loi habilitant le Gouvernement à simplifier le droit.*

L'accord sur les marchés publics (AMP) conclu en 1994 sous l'égide de l'OMC, visant à contribuer à la libéralisation et à l'expansion du commerce mondial établit ainsi **un cadre multilatéral de droits et d'obligations équilibrés en matière de marchés publics** afin que les opérateurs économiques puissent avoir accès, **dans les mêmes conditions que les opérateurs économiques nationaux**, aux marchés publics passés par les pouvoirs adjudicateurs des États membres. S'appliquant aux marchés de fournitures, à certains marchés de services et aux marchés de travaux dont le montant atteint les seuils européens de mise en concurrence et publicité des marchés, **l'accord compte aujourd'hui 22 parties, représentants 49 membres de l'OMC**.

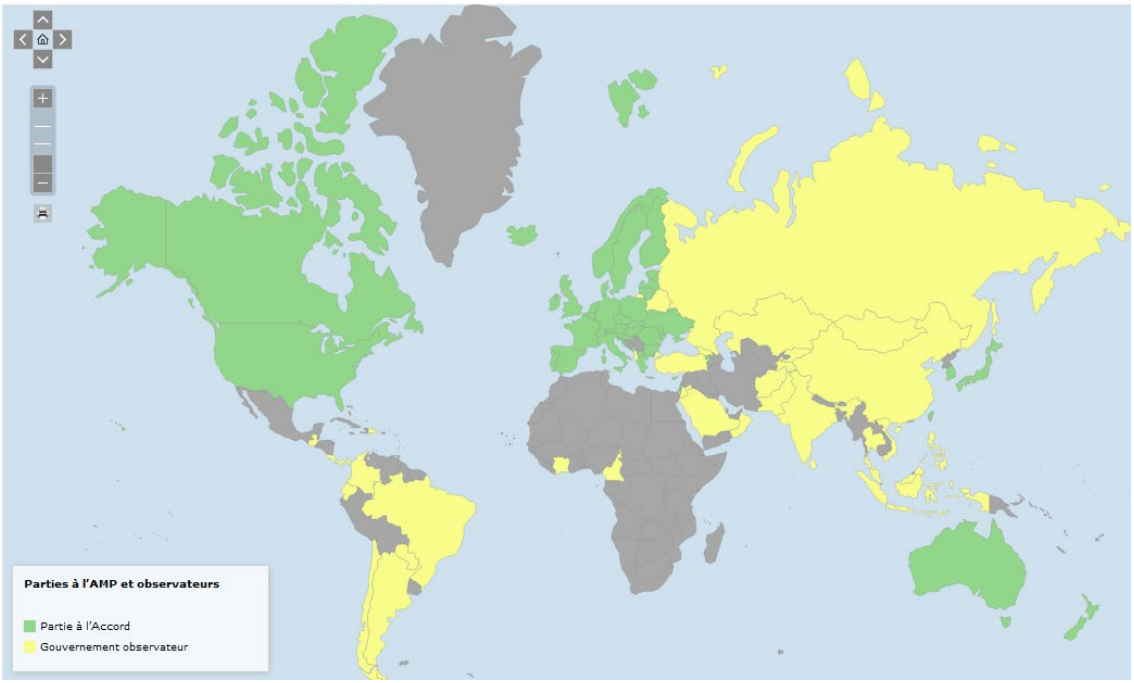
Les parties à l'accord sur les marchés publics de l'OMC

Parties à l'AMP	**Date d'entrée en vigueur / d'accession**	
	AMP de 1994 *(remplacé par l'AMP de 2012 le 1er janvier 2021)*	**AMP de 2012**
Arménie	15 septembre 2011	6 juin 2015
Australie	N/A	5 mai 2019
Canada	1er janvier 1996	6 avril 2014
Corée, République de	1er janvier 1997	14 janvier 2016
États-Unis d'Amérique	1er janvier 1996	6 avril 2014
Hong Kong	19 juin 1997	6 avril 2014
Islande	28 avril 2001	6 avril 2014
Israël	1er janvier 1996	6 avril 2014
Japon	1er janvier 1996	16 avril 2014
Liechtenstein	18 septembre 1997	6 avril 2014
Macédoine du Nord	N/A	30 octobre 2023
Moldavie	N/A	14 juillet 2016
Monténégro	N/A	15 juillet 2015
Norvège	1er janvier 1996	6 avril 2014
Nouvelle-Zélande	N/A	12 août 2015

Parties à l'AMP	**Date d'entrée en vigueur / d'accession**	
	AMP de 1994 *(remplacé par l'AMP de 2012 le 1er janvier 2021)*	**AMP de 2012**
Pays-Bas, pour le compte d'Aruba	25 octobre 1996	21 août 2014
Royaume-Uni	1er janvier 1996 (en tant qu'État membre de l'Union européenne à cette date)	1er janvier 2021
Singapour	20 octobre 1997	6 avril 2014
Suisse	1er janvier 1996	1er janvier 2021
Taipei chinois	15 juillet 2009	6 avril 2014
Ukraine	N/A	18 mai 2016
Union européenne et ses 27 États membres	1er janvier 1996	6 avril 2014
Allemagne, Autriche, Belgique, Danemark, Espagne, Finlande, France, Grèce, Irlande, Italie, Luxembourg, Pays-Bas, Portugal et Suède	1er janvier 1996	
Chypre, Estonie, Hongrie, Lettonie, Lituanie, Malte, Pologne, République slovaque, République tchèque et Slovénie	1er mai 2004	
Bulgarie et Roumanie	1er janvier 2007	
Croatie	1er juillet 2013	

38 membres de l'OMC disposent également du statut d'observateur, dont certains sont en attente de négociations pour l'accession à l'AMP.

Carte des États parties à l'AMP et des observateurs



Source : OMC

L'AMP a été intégré dans l'ordre communautaire par une décision du Conseil du 22 décembre 1994. En conséquence, l'article 25 de la directive 2014/24/UE dispose que « *les pouvoirs adjudicateurs accordent aux travaux, aux fournitures, aux services et aux opérateurs économiques des signataires de ces conventions internationales* ***un traitement non moins favorable*** *que celui accordé aux opérateurs économiques de l'Union* ».

(3) Certaines atteintes au principe de libre accès à la commande publique sont néanmoins tolérées par les directives européennes et le code de la commande publique

Malgré la prééminence de ces principes, il est prévu, pour certains marchés et sous certaines conditions, **la possibilité de déroger aux exigences de non-discrimination et de libre accès à la commande publique afin de répondre à des objectifs d'intérêt général**.

Le code de la commande publique contient des dispositifs permettant d'écarter des offres de pays tiers dans le cadre de la passation de marchés publics. Premièrement, l**es pays tiers n'ayant pas conclu d'accord multilatéral ou bilatéral qui assurent un accès comparable et effectif des entreprises de l'Union européenne aux marchés de ces pays peuvent voir leurs offres écartées dans le cadre de certains types de marchés** :

- Dans le cadre de la passation d'un marché de fournitures par une entité adjudicatrice, **cette dernière peut rejeter une offre qui contient des produits originaires d'un pays tiers s'ils représentent la part majoritaire de**

la valeur totale des produits composant l'offre[1]. Lorsque deux offres sont équivalentes au regard des critères d'attribution, une préférence peut en outre être accordée à celle n'étant pas composée d'une majorité de produits originaires d'un pays tiers[2].

- Dans le cadre de la passation d'un marché public, les acheteurs – qu'ils agissent en tant qu'entité adjudicatrice ou de pouvoir adjudicateur – peuvent introduire dans les documents de la consultation **des critères ou des restrictions fondés sur l'origine de tout ou partie des travaux, fournitures ou services** composant les offres proposées ou la nationalité des opérateurs autorisés à soumettre une offre[3].

- Dans le cadre des contrats de la commande publique de défense ou de sécurité, **qui sont systématiquement exclus du champ d'application des accords internationaux**. Pour ces marchés, il revient à l'acheteur de décider, au cas par cas, s'il autorise les opérateurs économiques de pays autres que les États membres à participer à la procédure de passation du marché public[4].

Toutefois, aucune de ces dispositions ne peut être employée par un acheteur public qui souhaiterait écarter un prestataire d'hébergement états-unien afin de se prémunir des risques de captation de données, les États-Unis étant parties à l'accord multilatéral de l'OMC présenté *supra*.

Deuxièmement, le code de la commande publique autorise, par son article L. 2112-4, de réduire de manière indirecte l'accès à des marchés publics de tout État non membre de l'Union européenne, y compris si ce dernier est signataire d'un accord de réciprocité d'accès à la commande publique, afin de poursuivre des objectifs environnementaux, sociaux, ou en matière de sécurité. Ainsi qu'en dispose l'article L. 2112-4, « *l'acheteur peut imposer que les moyens utilisés pour exécuter tout ou partie d'un marché, pour maintenir ou pour moderniser les produits acquis* ***soient localisés sur le territoire des États membres de l'Union européenne*** *afin, notamment,* ***de prendre en compte des considérations environnementales ou sociales ou d'assurer la sécurité des informations et des approvisionnements*** ». Ce dispositif peut trouver à s'appliquer en matière de marché public d'hébergement en nuage à la condition de démontrer l'existence d'un risque en matière de sécurité des informations, **ce qui, comme l'affirme l'ANSSI, n'est pas le cas pour l'ensemble des données détenues par des acheteurs publics**. Aussi le périmètre retenu par l'article 31 ne concerne-t-il uniquement les données sensibles, pour lesquelles une sécurité des informations doit être prévue.

---

[1] *Article L. 2153-2 du code de la commande publique.*
[2] *Article R. 2153-4 du code de la commande publique.*
[3] *Article L. 2153-1 du code de la commande publique.*
[4] *Article L. 2353-1 du code de la commande publique.*

(4) Les acheteurs publics peuvent mobiliser certains leviers pour favoriser indirectement la sélection d'un prestataire européen ou non soumis aux effets d'une législation de portée extraterritoriale

Les acheteurs publics peuvent toutefois recourir à d'autres outils afin de favoriser la sélection d'une offre immune aux effets des législations extraterritoriales, notamment **les critères d'attribution du marché**[1] qui peuvent conduire à valoriser les offres en fonction de leurs spécificités techniques, par exemple en matière de cybersécurité ;

Le recours aux critères d'attribution ne peut néanmoins conduire à constituer une inégalité de traitement entre candidats ou une restriction à l'accès aux marchés.

2. Le dispositif proposé : étendre les exigences de protection et de souveraineté des données à l'ensemble des données détenues par les acheteurs publics

a) La commission d'enquête a constaté les défaillances dans l'application du cadre normatif de protection des données

La commission d'enquête sur le coût et les modalités effectifs de la commande publique a consacré pour partie ses travaux aux enjeux de sécurisation des données détenues par des entités publiques à des fins de souveraineté numérique. Elle a ainsi 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**.

En effet, si l'article 31 de la loi SREN et la doctrine *cloud* de l'État prévoient désormais le recours à des solutions immunes aux législations extraterritoriales d'États tiers pour l'hébergement de leurs données sensibles, la commission d'enquête a observé que **la mise en conformité des administrations et des opérateurs de l'État à ces normes reste partielle, voire lacunaire**.

À titre d'exemple, la plateforme des données de santé, destinée à regrouper des données de santé à des fins de recherche et d'appui au système de santé, s'appuie depuis 2019 sur une solution d'hébergement proposée par Microsoft Azure, entreprise américaine. Selon la commission d'enquête, des contraintes de délais de mise en œuvre et de maîtrise des coûts ont initialement conduit le ministère de la Santé à recourir à cette offre présentant des risques pour la souveraineté des données hébergées, « *alors qu'il aurait effectivement été envisageable de recourir exclusivement à des acteurs français* »[2]. Le rapport souligne ainsi que « *l'ensemble des acteurs concernés ont semblé faire état*

[1] *Article L. 2152-7 du code de la commande publique.*
[2] *Page 166 du rapport de la commission d'enquête.*

d'une grande naïveté *au sujet des enjeux de l'hébergement de données sensibles chez des acteurs extra-européens, en dépit des premières alertes venues de la Cour de justice de l'Union européenne* » et conclut à « ***un véritable manque de volonté politique pour assurer la souveraineté des données publiques*** »[1]. Surtout, le rapport de la commission d'enquête déplore que, plus de six ans après sa création, et alors que la loi SREN impose désormais le recours à une offre souveraine pour les données sensibles, le transfert de la plateforme vers un autre prestataire ne soit toujours pas concrétisé en 2025. Si les responsables de la Plateforme de données de santé ont ainsi indiqué leur souhait de migrer les données vers une offre d'hébergement souveraine « *dès que les entreprises auront atteint le niveau de maturité requis* », ils n'avaient engagé, en juillet 2025, que la passation d'un marché pour une solution « intercalaire » à compter de 2026, et non d'un projet d'hébergement souverain pérenne.

La commission d'enquête a également déploré 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. Le rapport souligne le non-respect des procédures pour l'attribution de ce marché qui, du fait de son montant supérieur à 9 millions d'euros aurait dû, en vertu de l'article 3 du décret n° 2019-1088, faire l'objet d'un avis conforme de la direction interministérielle du numérique afin d'assurer la sécurisation du projet informatique.

La commission d'enquête a ainsi conclu à « ***l'incapacité de l'État à garantir la protection et la souveraineté des données publiques, en dépit du renforcement de la doctrine française en matière de protection des données*** ».

En conséquence, la commission d'enquête a appelé la France à se prémunir contre tout type de pression qui pourrait être exercée à son égard, soit par l'utilisation malintentionnée de données obtenues par un gouvernement étranger, soit par la restriction de l'accès à des solutions numériques dont l'Union européenne est aujourd'hui dépendante. En ce sens, **sa recommandation n° 24 préconise de rendre obligatoire, dans les plus brefs délais, l'insertion d'une clause de non-soumission aux lois extraterritoriales étrangères dans tous les marchés publics comportant des prestations d'hébergement et de traitement de données publiques en *cloud***.

L'article unique de la présente proposition de loi vise en conséquence à inscrire cette obligation dans le code de la commande publique.

b) Le dispositif proposé par l'article unique

L'article unique prévoit l'introduction d'un nouvel article au sein de la section 1 du chapitre II du titre I^er^ du livre I^er^ de la deuxième partie du code de la commande publique, traitant des règles générales pour la préparation de la passation des marchés publics.

[1] *Page 172 du rapport de la commission d'enquête.*

L'article L. 2112-4-1 que l'article unique crée vise à rendre obligatoire, pour les marchés comportant des prestations d'hébergement et de traitement de 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 ;
- de l'autre, **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.

L'article ne prévoyant pas d'entrée en vigueur différée, **ces obligations s'imposeraient dès la promulgation de la loi**, à l'occasion de la passation ou du renouvellement des marchés.

Le dispositif proposé représente donc **une évolution substantielle du cadre juridique français en matière de sécurisation des données publiques**.

Premièrement, le périmètre des données faisant l'objet d'une protection spécifique se trouve fortement élargi par l'article unique : alors que l'article 31 de la loi SREN ne prévoit des mesures de sécurisation qu'à l'égard des données dites sensibles – qualification répondant d'un double critère exposé *supra* – **l'article L. 2112-4-1 aurait vocation à s'appliquer à toute « donnée publique »**.

Le terme de donnée publique n'est défini, en l'état du droit, ni par les textes européens, ni par les textes internes. Il pourrait en conséquence faire l'objet de diverses interprétations, renvoyant :

- à la notion d'information publique, qui est encadrée par l'article L. 321-2 du code des relations entre le public et l'administration. Celui-ci indique en effet que « *ne sont pas considérées comme des informations publiques, les informations contenues dans des documents dont la communication ne constitue pas un droit pour toute personne en application du titre Ier ou d'autres dispositions législatives ou sur lesquels des tiers détiennent des droits de propriété intellectuelle* ».
- à toutes les données accessibles en droit ouvert et publiées par des acheteurs publics ;
- plus largement, au regard du rapport de la commission d'enquête dont l'article unique est issu, à l'ensemble des données détenues par des entités publiques.

Dans les trois acceptions, le volume de données protégées serait fortement élargi par le dispositif proposé.

De même, l'article unique propose **un élargissement substantiel des acheteurs soumis à des obligations de protection de la souveraineté des données**. L'article 31 de la loi SREN n'est aujourd'hui applicable qu'aux administrations de l'État, à leurs opérateurs ainsi qu'aux groupements d'intérêt public comprenant les administrations ou les opérateurs dont la liste doit être fixée par un décret en Conseil d'État. L'article 31 est également applicable, du fait de son IV, au groupement d'intérêt public de la Plateforme des données de santé. L'article unique de la proposition de loi vise pour sa part **l'ensemble des acheteurs publics**, qu'ils agissent en tant qu'entité adjudicatrice ou que pouvoir adjudicateur. Aussi, l'ensemble des collectivités territoriales, y compris les plus petites d'entre elles, entre dans le champ du dispositif proposé.

3. L'avis de la commission : une ambition politique légitime qui doit néanmoins se conformer aux exigences européennes et tenir compte des difficultés des petites collectivités territoriales afin de sécuriser les acheteurs dans la passation de leurs marchés

a) L'exposition réelle des entités publiques aux risques de captation de leurs données

Les travaux de la rapporteure ont démontré **la véracité du phénomène de dépendance** des acteurs français aux solutions d'hébergement étrangères, **bien que ce constat soit à nuancer s'agissant des entités publiques**.

De fait, la Cour des comptes, dans son avis sur les enjeux de souveraineté des systèmes d'information civils de l'État[1], indique que les trois grandes entreprises américaines Amazon Web Services (AWS), Microsoft Azure et Google Cloud – désignées sous le terme d'*hyperscalers* – 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. L'Autorité de la concurrence précise en outre que **80 % de la croissance des dépenses en services d'hébergement en France serait captée par les trois entreprises précitées**, l'entreprise Amazon Web Services bénéficiant à elle seule de 46 % des revenus du secteur[2].

L'Autorité de la concurrence a par ailleurs identifié des risques concurrentiels sur le marché de l'hébergement en nuage, certains fournisseurs de services *cloud*, en particulier les *hyperscalers* prémentionnés, facturant à leurs clients leurs transferts de données vers un fournisseur concurrent. Ces pratiques renforcent **la situation de dépendance des clients du marché**, en tant qu'elles rendent plus difficiles le changement de prestataire ou le recours à des prestataires multiples.

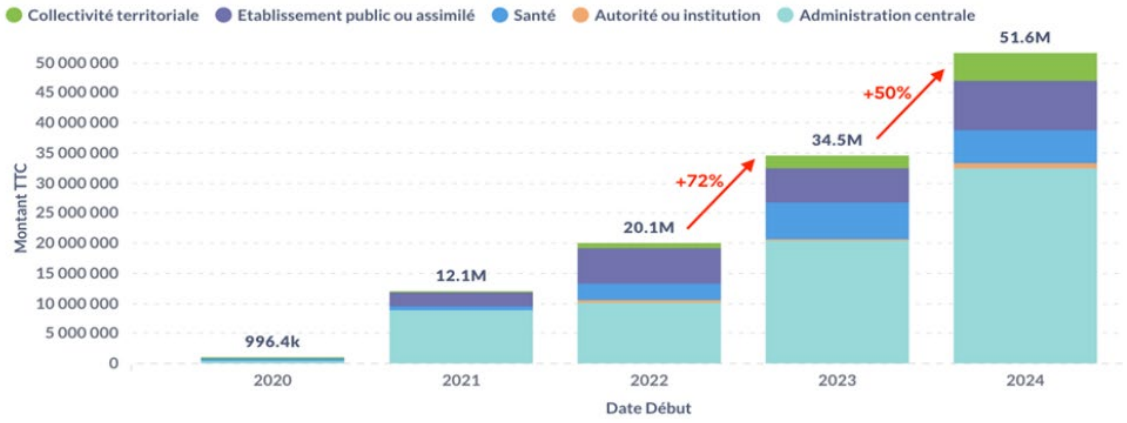
---

[1] *Avis rendu public au sein du rapport de la Cour des comptes sur les enjeux de souveraineté des systèmes d'informations civils de l'État, publié le 31 octobre 2025.*

[2] *Contribution de l'Autorité de la concurrence, s'agissant des services IaaS et Paas.*

La Cour des comptes observe également une augmentation significative des dépenses publiques en matière d'hébergement en nuage, passant d'un million d'euros en 2020 à 52 millions d'euros en 2024, pour un montant de 120 millions d'euros dépensés en cinq ans. Les services de l'État représentent les deux tiers de la commande publique totale de *cloud* en 2024 (32 millions d'euros). Toutefois, sur cette période, elle indique que **les fournisseurs français ont représenté 63 % de la commande publique, dont la moitié relevait de la certification SecNumCloud**, témoignant d'une sensibilisation accrue des administrations aux enjeux de souveraineté numérique. La direction interministérielle du numérique a également indiqué à la rapporteure que s'agissant du recours à des prestations *cloud* par les administrations de l'État *via* les marchés de l'union des groupements d'achats publics (UGAP), **90 % des commandes retiennent des prestataires français**[1].

Évolution des dépenses publiques en matière de *cloud* par les administrations publiques entre 2020 et 2024



Source : Cour des comptes, selon les données de la Dinum.

En revanche, ni les administrations centrales, ni les associations d'élus n'ont été en mesure de fournir des indications quant **aux fournisseurs de solutions d'hébergement retenus par les collectivités territoriales**. Cette absence de visibilité sur le niveau de dépendance de ces dernières aux solutions extra-européennes est regrettable à double titre, en premier lieu parce qu'il n'est en conséquence pas possible **d'évaluer le niveau d'exposition des collectivités au risque d'interception de données**, et en second lieu parce qu'il est dès lors difficile de **déterminer l'effort que représentera l'application du dispositif proposé**.

Quant à l'évaluation du risque réel que fait peser l'extraterritorialité du droit auquel sont soumis certains fournisseurs étrangers, la Cour des comptes note que les chiffres disponibles font état **d'un nombre très faible de rejets des demandes émises au titre du FISA par les agences fédérales de**

[1] *Audition de la direction interministérielle du numérique, le 19 novembre 2025.*

renseignement. La Cour constate par ailleurs une forte augmentation des comptes faisant l'objet de requêtes administratives émises par des agences fédérales américaines auprès de Google, passant de moins de 5 000 avant 2010 à près de 120 000 au second semestre 2023, et de Microsoft, qui ne recevait en 2011 que 12 000 demandes, et en traitait désormais 25 000 en 2023[1].

b) Le dispositif proposé soulève néanmoins des inquiétudes quant à ses modalités d'application

Néanmoins, en dépit de la légitimité de l'objectif poursuivi par la proposition de loi, les travaux conduits par la rapporteure ont permis de mettre en lumière certaines limites du dispositif proposé.

(1) Le risque de non-conformité du texte au cadre juridique de la commande publique et aux engagements internationaux de la France

Les obligations nouvelles que l'article unique entend imposer dans tous les marchés publics présentent premièrement **un risque d'inconventionnalité** au regard du droit de la commande publique.

De fait, en imposant des conditions d'exécution conduisant à écarter les acteurs extra-européens de l'ensemble des marchés publics d'hébergement de données, le dispositif proposé pourrait s'apparenter à **une discrimination des opérateurs sur la base de leur nationalité** non-justifiée par un motif impérieux d'intérêt général. En effet, comme l'a précisé l'ANSSI à la rapporteure, le risque d'interception des données ne pèse pas de manière égale sur l'ensemble des acheteurs publics : d'une part, certains d'entre eux n'ont pas à traiter de données susceptibles d'intéresser des autorités tierces, d'autre part, le volume de données traitées est à prendre en compte pour évaluer l'attrait que ces dernières constituent en cas d'interception. À titre d'exemple, il pourrait être estimé que les données détenues par une petite commune ne représentent pas un intérêt justifiant d'un tel niveau de protection.

Le dispositif proposé pourrait donc s'apprécier, à l'aune des engagements internationaux de la France en matière de commerce, et du droit communautaire et interne rappelés en première partie de ce rapport, comme **une entrave disproportionnée au libre accès des opérateurs économiques à la commande publique en matière d'hébergement en nuage**.

(2) Le périmètre large du dispositif est susceptible d'engendrer des situations d'insécurité juridique pour les acheteurs publics

Deuxièmement, pour la rapporteure, l'article unique, s'il était adopté, ferait peser **de lourdes obligations sur les acheteurs publics** – au premier rang desquels, les petites collectivités territoriales – alors même que la commission d'enquête l'ayant inspiré avait appelé à **la simplification du droit de la commande publique**.

---

[1] *Avis rendu public au sein du rapport de la Cour des comptes sur les enjeux de souveraineté des systèmes d'informations civils de l'État, publié le 31 octobre 2025.*

Le dispositif proposé demeure en effet imprécis sur un certain nombre de paramètres, laissant craindre une **insécurité juridique** pour les marchés conclus sur son fondement :

Comme cela a été mentionné précédemment, **l'absence de définition de la donnée publique est susceptible de donner lieu à confusion pour les acheteurs** quant au périmètre réel des données à héberger sur un *cloud* souverain, et ainsi être source de contentieux.

En outre, les exigences s'appliquant à ce type de marché sont moins lisibles que celles prévues par la loi SREN. De fait, la rédaction d'une condition d'exécution « *excluant l'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* » suppose de solides connaissances de l'acheteur en matière de législation internationale extraterritoriale. Comme l'a rappelé le rapport de la commission d'enquête sur les coûts et les modalités effectifs de la commande publique, en dépit de la professionnalisation des missions de la commande publique, celle-ci repose encore, en large partie, et notamment dans les petites collectivités territoriales, sur des profils ne disposant pas d'une formation initiale dédiée aux achats : **seules 9,74 % des communes sollicitées dans le cadre de la consultation des élus locaux réalisée par la commission d'enquête disposent d'un acheteur professionnel**[1]. Pour les autres, une telle évolution juridique est de nature à susciter de fortes difficultés, laissant craindre une application erronée pouvant avoir des effets contreproductifs en matière de cybersécurité, ainsi que des contentieux juridiques. À l'inverse, selon les informations transmises à la rapporteure, le décret d'application de l'article 31 de la loi SREN devrait fournir des indications claires sur la manière d'évaluer les conditions de sécurité requises par l'article pour les solutions d'hébergement, notamment en renvoyant à la qualification SecNumCloud, ce qui facilitera sa mise en application par les administrations de l'État et ses opérateurs.

De plus, l'obligation de recourir à un prestataire souverain et présentant de fortes garanties en matière de sécurisation risque d'engendrer un surcoût pour ces acheteurs. Pour la Cour des comptes, 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 %[2]. Au regard de l'état des finances des collectivités territoriales, l'application indifférenciée du dispositif proposé semble dès lors démesurée.

(3) Des effets incertains sur le marché français de l'hébergement en nuage

En outre, la proposition de loi, par la définition peu précise des exigences qu'elle crée, et le périmètre maximaliste des marchés concernés, pourrait produire **des effets contre-productifs sur le marché du *cloud* français et européen**.

---

[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) déposé le 8 juillet 2025, page 149.

[2] *Avis rendu public au sein du rapport de la Cour des comptes sur les enjeux de souveraineté des systèmes d'informations civils de l'État, publié le 31 octobre 2025.*

En effet, alors que l'auteur du texte souhaite mobiliser la commande publique à des fins d'entraînement du tissu d'entreprises français, les acheteurs publics seraient certainement amenés, pour répondre aux exigences du dispositif, à se tourner exclusivement vers les offres SecNumCloud. Or, comme l'a fait valoir l'autorité de la concurrence auprès de la rapporteure, le dispositif pourrait en conséquence **limiter l'offre au niveau national et européen,** en excluant du marché les acteurs ne disposant pas de cette qualification : les petits acteurs français et européens du secteur, dans l'incapacité de faire les investissements nécessaires à court terme pour proposer de telles prestations, se verraient évincés du marché, compromettant directement leur modèle économique. Comme l'a démontré la Cour des comptes, l'investissement nécessaire pour obtenir la qualification SecNumCloud est en effet très conséquent, puisqu'il représente 1 à 2 millions d'euros sur une période de 18 mois environ, afin d'opérer une mise à niveau technique, une refonte des politiques et des procédures de sécurité, de produire une documentation détaillée et de mettre en œuvre des contrôlés poussés[1].

Par ailleurs, au vu des investissements requis et des barrières à l'entrée très élevées sur le marché du *cloud,* et *a fortiori*, sur le marché du *cloud* souverain, à mettre en regard avec la taille relativement réduite du marché français, il est peu probable que de nouveaux acteurs entrent sur ce marché. Dès lors, les prestataires existants déjà en mesure de fournir les services répondant aux exigences du dispositif envisagé jouiraient d'**un avantage économique significatif**, avec des clients captifs qui, pour se conformer aux nouvelles obligations, ne pourraient faire appel à d'autres fournisseurs.

c) L'avis de la commission

Devant les difficultés soulevées par le dispositif proposé à l'article unique, la rapporteure a soumis **un amendement COM-1** à la commission visant à faciliter l'appropriation de ces exigences nouvelles par les collectivités territoriales, ainsi qu'à garantir le caractère équilibré de ce nouveau dispositif.

La réécriture proposée **restreint, premièrement, le périmètre des données faisant l'objet de mesures de protection aux seules données sensibles** telles que définies à l'article 31 de la loi SREN. En effet, la création d'une nouvelle catégorie de données à protéger (les « données publiques ») pourrait susciter de nombreuses interrogations de la part des entités publiques, en l'absence d'une définition précise, tandis que le périmètre défini par la loi SREN est clairement arrêté et qu'il fait l'objet d'un travail pédagogique de la Dinum et de la direction des affaires juridiques du ministère de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique auprès des acheteurs depuis l'entrée en vigueur du texte.

[1] *Avis rendu public au sein du rapport de la Cour des comptes sur les enjeux de souveraineté des systèmes d'informations civils de l'État, publié le 31 octobre 2025.*

Cette évolution du périmètre assure en outre **la conformité de l'article au droit de la commande publique et aux engagements internationaux de la France et de l'Union européenne**, puisque les restrictions apportées à l'accès aux marchés publics seraient strictement justifiées par la sensibilité des données protégées.

Deuxièmement, **l'amendement de la rapporteure vise à exclure du dispositif les communes de moins de 30 000 habitants ainsi que les communautés de communes** afin de tenir compte des difficultés que celles-ci pourraient rencontrer dans la mise en œuvre de ces normes, du fait des moindres moyens qu'elles sont en mesure d'allouer à la mission d'achat au sein de leur équipe.

Pour la rapporteure, imposer ces normes complexes aux petits acheteurs publics présente en effet trois risques importants :

- **un risque juridique**, en raison d'une mauvaise application des obligations nouvelles ;
- **un risque de surcoût** pour des collectivités au cadre budgétaire déjà contraint ;
- **un risque en matière de cybersécurité**, puisque les collectivités pourraient se tourner vers un prestataire souverain mais insuffisamment robuste technologiquement alors que, comme le souligne l'ANSSI, les collectivités font l'objet de nombreuses cyberattaques et tentatives de piratage.

Par souci de clarté et de cohérence, la rapporteure a donc proposé de reprendre **le seuil défini au sein du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité** (excluant les communes de moins de 30 000 habitants et les communautés de communes), qui vise à imposer aux seules grandes collectivités locales de nouvelles mesures en matière de cybersécurité.

Par ailleurs, au regard des éventuelles difficultés mentionnées pour les collectivités, l'amendement de réécriture contient **un mécanisme de dérogation** : lorsqu'une collectivité a déjà engagé un projet nécessitant un recours à un service d'informatique en nuage, lorsqu'elle rencontre des difficultés techniques pour se conformer au dispositif ou qu'elle justifie d'un surcoût important causé par le changement de prestataire, elle pourrait dès lors décider d'échapper à l'obligation créée par la loi. Ce mécanisme de dérogation vise ainsi à **favoriser un déploiement progressif et respectueux des possibilités de chacun de l'ambitieuse stratégie de protection des données** portée par le texte.

Enfin, la rapporteure a proposé **une entrée en vigueur différée du dispositif, au 1er janvier 2028**. En effet, le marché du *cloud* français et européen est en pleine phase de développement, et les surcoûts constatés aujourd'hui pour certaines offres SecNumCloud pourraient en conséquence être amenés à s'atténuer dans les prochaines années.

La commission a adopté l'amendement COM-1 de la rapporteure.

La commission a **adopté** l'article unique **ainsi modifié**.

EXAMEN EN COMMISSION

MERCREDI 10 DÉCEMBRE 2025

Mme Muriel Jourda, présidente. – Nous en venons au rapport de notre collègue Olivia Richard sur la proposition de loi relative à la sécurisation des marchés publics numériques, dont l'auteur, Dany Wattebled, nous expose d'abord les motivations.

M. Dany Wattebled, auteur de la proposition de loi. – Cette proposition de loi prolonge les travaux 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, dont j'étais le rapporteur. Mon collègue Simon Uzenat, qui en assurait la présidence, et moi-même avons conduit pendant plusieurs mois cinquante-huit auditions, effectué trois déplacements et rencontré les représentants de centre trente-quatre structures.

Notre point de départ était simple : forte d'un enjeu de 400 milliards d'euros chaque année et équivalant à 14 % du PIB national, la commande publique est un moteur de notre économie.

Dans nos territoires, élus et entreprises témoignent de procédures lourdes, complexes, parfois anxiogènes ; s'y associent la crainte du contentieux et du pénal, l'impression d'un empilement des règles et, parfois, le sentiment d'une déconnexion de la réalité.

Au fil des auditions, un sujet s'est imposé, celui de la commande publique numérique, devenue un enjeu de souveraineté. Certaines des réponses que nous avons reçues ont été très éclairantes. Ainsi, lorsque nous avons demandé à l'entreprise Microsoft France si elle pouvait nous garantir que les données françaises hébergées en France ne seraient jamais transmises à une autorité étrangère sans l'accord de notre pays, sa réponse a été clairement négative. Et cette impossibilité résulte de l'existence dans le droit américain de lois fédérales extraterritoriales, spécialement le *Cloud Act*, qui permettent d'exiger la communication des données hébergées par toute entreprise américaine sur le sol français.

Nous avons étudié plusieurs dossiers. Le premier est aberrant. Il concerne la plateforme des données de santé ou *Health Data Hub*, c'est-à-dire l'hébergement sur une plateforme unique de l'intégralité des données de santé des Français – une idée en elle-même remarquable. Pour sa concrétisation, la puissance publique a investi 80 millions d'euros et s'est adressée à… Microsoft ! Or, avec l'essor de l'intelligence artificielle, ces données représentent le pétrole de demain.

On a ensuite récidivé avec l'enseignement supérieur et la pépite qu'est l'École polytechnique, en engageant 130 millions d'euros pour l'hébergement des données auprès d'acteurs américains. On marche sur la tête. Notre constat est le suivant : il n'y a aujourd'hui plus aucune souveraineté française ni européenne sur nos données numériques.

L'Union des groupements d'achats publics (Ugap) reconnaît elle-même qu'elle n'a pas assez conseillé la puissance publique sur les aspects de souveraineté numérique. Elle a laissé le champ libre à Microsoft et au développement d'autres acteurs étrangers.

La commission d'enquête a, en conséquence, conclu à l'existence d'un risque majeur et stratégique pour la souveraineté numérique des entités publiques françaises. La présente proposition de loi s'inspire de la recommandation n° 24 formulée par la commission d'enquête au terme de ses travaux et l'intention première qui la sous-tend est simple : protéger les données françaises publiques, et particulièrement les données sensibles. Ce texte n'est dirigé contre personne en particulier, c'est un texte de protection et de bon sens. Si nous poursuivons d'abord l'objectif de sécuriser les acheteurs publics, nous ne négligeons pas non plus celui d'envoyer un signal clair aux acteurs français et européens, pour qui l'obtention de tels marchés publics représenterait un levier considérable de développement économique.

Je salue le travail et l'écoute de Mme la rapporteure Olivia Richard, qui a su renforcer juridiquement le dispositif que nous proposons, en en préservant l'objectif essentiel. Inscrite à la suite de l'article 31 de la loi du 21 mai 2024 visant à sécuriser et réguler l'espace numérique (Sren), cette proposition de loi est une étape nécessaire pour que nous recouvrions notre souveraineté numérique, qu'elle soit française ou européenne. Il en est grand temps dans le monde de guerre économique qui est le nôtre, et c'est pourquoi je vous invite à l'adopter.

Mme Olivia Richard, rapporteure. – Je salue l'initiative de notre collègue Dany Wattebled ainsi que son engagement, que je pourrais qualifier de passionné, sur le sujet qui nous occupe ce matin. Ses travaux ont révélé de véritables failles dans la protection et la confidentialité des données de nos acteurs publics, lorsqu'elles sont hébergées en nuage auprès de prestataires étrangers.

Comme l'a démontré la commission d'enquête dont il a été le rapporteur, ces entreprises, notamment les géants américains, ne sont pas en mesure de garantir la pleine protection du contenu qu'elles hébergent, en raison de leur soumission à des lois extraterritoriales étrangères.

Aux États-Unis, par exemple, le *Foreign Intelligence Surveillance Act* (Fisa) et le *Cloud Act* permettent aux autorités américaines de contraindre les entreprises à leur révéler le contenu d'une communication ou d'une information qu'elles détiennent ; et cela y compris lorsque ces données sont

hébergées sur des serveurs situés hors de leur territoire national. Elles y sont soumises même lorsqu'elles sont en France.

Lorsqu'une telle demande leur est adressée, les entreprises ne sont en outre pas tenues d'en informer leurs clients. Un rapport de la Cour des comptes, paru en octobre dernier, atteste ces pratiques, et fait même état d'une hausse alarmante des requêtes auprès de certaines entreprises américaines, dont notamment Google et Microsoft.

Depuis quelques années, la Chine et l'Inde consolident également leurs outils juridiques extraterritoriaux, permettant de la même manière des détournements de données stockées en nuage.

Face à ces menaces, l'Agence nationale de la sécurité des systèmes d'information (Anssi) tient un discours très clair : ni le chiffrement ni la segmentation du contenu ne sont en mesure d'assurer pleinement la sécurisation des données ; seul le choix d'un prestataire français ou européen constitue une véritable garantie de la souveraineté des données hébergées.

Depuis quelques années, la France a, en conséquence, entrepris de consolider son cadre juridique afin de limiter l'exposition de données stratégiques au risque de captation par des autorités étrangères.

Premièrement, depuis 2021, la doctrine « *cloud* au centre » soutient le développement des solutions *cloud* par et pour l'État. Ces serveurs ont vocation à héberger certaines données, dont la compromission nuirait au bon fonctionnement du pays. Elles sont à la disposition du ministère de l'intérieur – il partage d'ailleurs cet espace de stockage avec le ministère des affaires étrangères – et du ministère de l'économie et des finances.

Deuxièmement, l'article 31 de la loi Sren impose désormais aux administrations publiques et aux opérateurs de l'État d'héberger leurs données sensibles dans un *cloud* souverain, c'est-à-dire un *cloud* privé français ou européen qui présente de fortes garanties de sécurité. Le périmètre des données jugées sensibles correspond, aux termes de cette loi, aux données nécessaires à l'accomplissement des missions essentielles de l'État, dont la violation serait susceptible de causer une atteinte à l'ordre public, à la sécurité publique, à la santé des personnes ou encore à la propriété intellectuelle.

Pourtant, les travaux de la commission d'enquête ont permis de démontrer que ces exigences de protection ne sont encore que partiellement appliquées. C'est notamment ce qui explique que certains marchés publics d'hébergement hautement stratégiques, comme celui de la plateforme des données de santé, ou celui du ministère de l'éducation nationale, soient encore confiés à de grandes entreprises américaines, en dépit de la loi.

Par ailleurs, si un suivi du recours à des *clouds* souverains est effectué par la Dinum, nous ne disposons d'aucun élément pour évaluer le niveau de protection des données détenues par les autres acheteurs publics, notamment par les collectivités territoriales.

Pour répondre à ces défaillances, la proposition de loi de notre collègue vise à renforcer substantiellement notre cadre juridique de protection des données, en confiant les données de l'ensemble des acheteurs publics à des prestataires français ou européens.

Concrètement, l'article unique rend obligatoire, dans les marchés publics contenant des prestations d'hébergement en nuage, la présence de conditions d'exécution garantissant l'immunité du prestataire à toute législation extraterritoriale et l'hébergement des données sur le territoire de l'Union européenne.

Au regard des risques dont je viens de vous faire part, nul ne peut remettre en cause l'intention légitime du texte. Nous ne devons pas être naïfs. Il est grand temps que les entités publiques prennent la mesure de leur vulnérabilité face à des législations puissantes, notamment dans un contexte géopolitique très incertain, et qu'elles agissent pour garantir leur souveraineté numérique.

Toutefois, le dispositif soulève des difficultés d'ordre juridique et opérationnel ; c'est la raison pour laquelle je vous proposerai un amendement visant à le rendre plus soutenable.

En effet, dans sa rédaction actuelle, le texte soumet l'ensemble des données publiques aux obligations d'hébergement souverain. Si l'on comprend tout à fait l'intention de l'auteur, cette restriction systématique d'accès aux marchés pour les prestataires non européens pourrait s'apparenter à une discrimination sur la base de l'origine géographique, ce qui est strictement interdit par les directives européennes. Cette mesure contreviendrait également aux engagements internationaux de la France, qui, dans le cadre de l'accord sur les marchés publics de l'Organisation mondiale du commerce (OMC), prohibe toute inégalité de traitement d'opérateurs économiques de pays signataires, tels que les États-Unis.

Par ailleurs, les auditions menées laissent à penser que ces obligations nouvelles seront difficilement mises en œuvre par les petits acheteurs publics, parmi lesquels les petites communes. De fait, le plus souvent, leurs équipes ne comptent pas d'acheteur public professionnel, et il est à craindre que les agents de mairie ne rencontrent des difficultés pour inclure ou contrôler les garanties apportées quant aux conditions d'exécution ayant trait au droit international. Pour le dire autrement, les acheteurs ne disposent pas nécessairement des moyens techniques et humains nécessaires pour se conformer au dispositif.

En outre, le recours à un prestataire souverain et sécurisé, disposant par exemple de la qualification SecNumCloud délivrée par l'Anssi, représente des coûts importants. La Cour des comptes estime ainsi qu'une offre SecNumCloud a un coût de l'ordre de 25 % à 40 % supérieur à une offre standard. Là encore, au regard du contexte budgétaire contraint qu'elles connaissent, le dispositif semble problématique pour les petites collectivités.

Enfin et surtout, différents acteurs, dont l'Anssi, ont souligné l'impératif de proportionnalité que nous devons observer. Nous pouvons convenir que les données détenues par une petite commune ne représentent pas nécessairement un intérêt substantiel pour des autorités publiques étrangères et que ce risque ne les concerne pas au premier chef.

En accord avec l'auteur du texte, j'ai souhaité parvenir à un équilibre entre la protection nécessaire des données publiques stratégiques et la prise en compte des difficultés des petits acheteurs publics.

L'amendement que je vous soumets prévoit donc plusieurs évolutions du dispositif sans, je le crois, le dénaturer ou en compromettre l'objet.

Tout d'abord, alors que le dispositif crée une nouvelle catégorie de données à protéger – les « données publiques » – qui n'est pas définie en droit, je vous propose, pour faciliter sa mise en œuvre, de revenir au périmètre des données sensibles telles que définies par la loi Sren. Restreindre les obligations d'hébergement souverain aux seules données sensibles semble être plus proportionné au regard des risques réels encourus, et permet de conserver la définition inscrite dans la loi Sren, qui est en cours d'appropriation par les acheteurs publics et dont le décret d'application devrait bientôt être publié. De plus, le périmètre des données sensibles inscrit dans la loi Sren a d'ores et déjà été validé par la Commission européenne et n'est donc pas susceptible d'être qualifié de restriction d'accès disproportionnée aux marchés publics. Cet amendement conforterait ainsi la validité juridique des marchés publics d'hébergement, et permettrait aux acheteurs d'assurer une transition progressive en matière de protection des données.

En outre, afin de tenir compte des difficultés techniques et financières que pourraient rencontrer les petits acheteurs publics dans la mise en œuvre de ce texte, l'amendement que je vous soumets prévoit d'exclure du dispositif les communes de moins de 30 000 habitants et les communautés de communes. Ces dernières risquent en effet de ne pas disposer des ressources humaines et techniques suffisantes pour adapter leurs marchés publics, et les données qu'elles détiennent sont moins susceptibles de faire l'objet de détournements.

Je vous propose de reprendre le seuil de 30 000 habitants, figurant au sein d'un autre texte que nous avons adopté au Sénat en séance publique et qui crée des obligations nouvelles en matière de cybersécurité, le projet relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, en cours d'examen par l'Assemblée nationale. Cet alignement permettra de constituer un ensemble cohérent de mesures nouvelles afin de sécuriser les systèmes d'information des grandes collectivités.

Les acteurs de terrain rencontrés dans le cadre des auditions ont également souligné que le marché français du *cloud* est en plein essor, mais n'est pas encore arrivé à maturité, ce qui explique notamment les surcoûts des offres constatés par la Cour des comptes. Dès lors, afin de laisser le temps aux

entreprises de développer leurs technologies et de faire face à la hausse des sollicitations, je propose une entrée en vigueur différée du texte, au 1er janvier 2028.

Ces deux années devront également permettre aux acheteurs publics d'anticiper ces nouvelles exigences de protection, bien que, devant les difficultés soulevées par le dispositif, je vous propose également de prévoir un mécanisme de dérogation. Grâce à celui-ci, toute collectivité ayant déjà engagé un projet nécessitant un recours à un service d'informatique en nuage qui rencontrerait des difficultés techniques pour se conformer au dispositif proposé ou qui justifierait de surcoûts importants pourrait déroger temporairement au respect de ses obligations.

Mon objectif est à la fois de rassurer et d'avancer résolument dans la direction indiquée par notre collègue. Loin de trahir l'esprit initial du texte, je propose une évolution du périmètre de l'amendement afin d'inciter l'ensemble des entités concernées à développer progressivement leur stratégie de protection des données. Sans ajouter de complexité démesurée aux missions des acheteurs, ces évolutions doivent néanmoins garantir de réels progrès pour la souveraineté de nos données dans les années à venir.

M. Marc-Philippe Daubresse. – Si la rapporteure n'avait pas présenté d'amendement, j'aurais moi-même proposé de limiter le champ d'application de la proposition de loi aux communautés d'agglomération et aux communes d'une certaine importance, en cohérence avec les seuils déjà définis par ailleurs.

Pour avoir beaucoup travaillé, avec Jérôme Durain, sur les questions de cybersécurité, je constate que nous sommes confrontés à une triple contrainte.

Premièrement, nous sommes, mes chers collègues, en guerre ! C'est une guerre économique qui nous oppose aux deux superpuissances, les États-Unis et la Chine. Je comprends les raisons d'un report du nouveau dispositif au 1er janvier 2028, liées à sa complexité. Toutefois, pendant ce temps, la guerre s'intensifie, la puissance des deux géants s'accentue et les spécialistes de la cybersécurité que sont les Russes, les Chinois et, dans une moindre mesure, les Américains et les Israéliens progressent beaucoup plus vite que nous.

Deuxièmement, les collectivités locales, en particulier les petites communes et les communautés de communes, ne disposent pas à l'évidence des moyens pour mettre en œuvre un tel dispositif. Il est cependant exact qu'elles sont aussi moins exposées au risque contre lequel il vise à lutter.

Troisièmement, nous sommes confrontés à la complexité de notre système normatif, avec la prise en compte de la législation européenne. Les simplifications que nous souhaitons entreprendre, à grand renfort de discours, se traduisent invariablement par un surcroît de complexification ! Tel a déjà été le résultat de la récente « simplification » du droit de l'urbanisme.

Je soutiens la démarche de Dany Wattebled et l'amendement de la rapporteure, tout à fait pertinent en l'état de la législation, mais nous ne ferons pas l'économie d'aller plus loin sur ces questions, et peut-être nous faudra-t-il envisager une mission plus globale. Nous n'avons pas réuni en effet, tant s'en faut, les munitions qui nous permettront de gagner la guerre. Nous sommes plutôt en train de la perdre !

M. Christophe Chaillou. – Pour notre part, nous accueillons très favorablement la proposition de loi issue des travaux de la commission d'enquête présidée par Simon Uzenat. Si elle ne répond sans doute pas complètement aux enjeux, elle constitue une première étape importante dans l'élaboration de cette réponse.

L'enjeu essentiel est celui de notre souveraineté et de la sécurisation de nos données numériques. S'y ajoute la nécessité de soutenir nos acteurs européens.

L'amendement proposé nous semble concilier la réalité des normes déjà applicables, notamment à l'échelle européenne, nos contraintes nationales, spécialement celles de nos petites collectivités, et la préoccupation d'aboutir à un dispositif véritablement opérationnel. Nous sommes en particulier favorables au report d'un an de l'entrée en vigueur du dispositif.

Mme Audrey Linkenheld. – Pour avoir été membre de la commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, ayant pour objet la transposition de trois directives européennes, dont la directive NIS 2, je ne peux que constater que nous avons pris du retard. Cette transposition, qui devait être effective en octobre 2024, n'est ainsi toujours pas réalisée. C'est fâcheux au regard des enjeux majeurs qui s'imposent à nous.

Il est indispensable que toutes les institutions publiques et que tous les acteurs privés aient conscience de la menace qui pèse sur eux. À cet égard, contrairement à ce qu'a dit Marc-Philippe Daubresse, je ne crois pas que certains y soient moins exposés que d'autres ; la différence tient de mon point de vue davantage, en fonction de leur importance respective, au poids des conséquences en cas de perte de données. Aussi, il est pertinent que vous proposiez d'adapter les mesures opérationnelles à la nature et à la taille de ces institutions et de ces acteurs.

Sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, notre collègue Florence Blatrix Contat a fait adopter un amendement sur la question spécifique de la souveraineté numérique, afin d'encourager le recours à des infrastructures et à des solutions, en particulier des solutions de *cloud*, françaises ou européennes.

Il importe que nous nous assurions de la convergence de l'ensemble des textes et des propositions sur lesquels nous travaillons, tant sur le fond que sous l'angle du calendrier. Nos collectivités et nos entreprises doivent en effet pouvoir disposer d'un minimum de visibilité sur ce que nous attendons

d'elles. Pour l'heure, ces exigences demeurent assez obscures ; quant à l'accompagnement de l'État, notamment auprès des collectivités, il reste relativement faible. Le Gouvernement sait dire ce qu'il faut faire, beaucoup moins comment il convient d'accompagner, y compris financièrement, les collectivités pour y parvenir. Nous pourrons pour notre part encore travailler au texte du projet de loi sur ces aspects.

Mme Dominique Vérien. –Au sein de notre groupe politique, Catherine Morin-Desailly nous alerte depuis des années sur le sujet de la souveraineté de nos données. Elle s'est opposée à la volonté du Gouvernement de confier l'hébergement de nos données de santé à Microsoft et a fait adopter plusieurs propositions de résolution sur le sujet. Avec la présente proposition de loi, elle peut enfin avoir l'impression d'être entendue par le Sénat.

C'est une bonne chose, car je confirme que nous sommes en guerre et que la souveraineté de nos données est primordiale.

Se posent des problèmes de complexité juridique et de conformité au droit européen. Nous avons souvent souligné que le *Digital Services Act* (DSA) ou la loi Sren, pour importants qu'ils soient, n'allaient pas encore assez loin. La rapporteure, dont je salue le travail comme je salue celui de l'auteur du texte, a su définir la bonne ligne de crête pour progresser autant qu'il était possible sur ces questions de souveraineté. Nous en suivrons les propositions.

M. Dany Wattebled. – La rapporteure a réussi un bel équilibre en s'adossant à la loi Sren, en ménageant les collectivités de moins de 30 000 habitants et en ne heurtant pas de plein front le nouveau projet de loi de simplification des normes en cours d'élaboration.

Cependant, une entrée en vigueur du dispositif en 2028 me paraît trop éloignée. Marc-Philippe Daubresse a rappelé que nous étions en guerre. Je proposerai de nous en tenir impérativement au 1er janvier 2027. Cette commission a permis d'affirmer la volonté de rapatriement des données de santé des Français dans des *clouds* souverains et l'on parle également de revenir sur l'hébergement des données de l'enseignement supérieur. Nous voyons l'intérêt qu'il y a de provoquer au plus tôt de telles initiatives. Une guerre se gagne aussi par la rapidité de manœuvre. Ne donnons pas un an de plus à nos adversaires. La loi proposée n'est pas une loi de circonstance, elle est importante, et tous les jours nous déplorons la fuite de données, tandis que nos start-up font l'objet de rachats et que la commande publique ne s'adresse pas non plus aux acteurs français d'importance européenne tels que les hébergeurs Scaleway ou OVH.

Mme Olivia Richard, rapporteure. – Merci de votre soutien tant à la proposition de loi qu'à l'amendement que je vous propose.

L'initiative de notre collègue est heureuse, ne serait-ce que parce qu'elle permet d'ouvrir le débat. Les travaux de la commission d'enquête sénatoriale avaient déjà provoqué une sorte d'électrochoc auprès des acteurs économiques concernés. Avant même l'adoption d'un texte législatif, le seul

fait de poser des questions, de mettre en lumière les difficultés et de tirer la sonnette d'alarme permet de faire avancer les lignes.

Nous sommes nombreux à partager la préoccupation d'une autonomie stratégique. Les auditions que j'ai conduites se sont tenues en parallèle du sommet organisé à Berlin, où la France a clamé haut et fort son souhait d'une souveraineté numérique. Nous allons dans la bonne direction, mais nous butons, c'est exact, sur la complexité du système normatif en vigueur. Ne cédons pas pour autant au sentiment d'impuissance qui, parfois, peut nous gagner. Trouver un équilibre était pour moi prioritaire.

Votre souhait, monsieur Wattebled, d'une mise en œuvre la plus rapide possible de nouvelles dispositions législatives, et en tout cas anticipée par rapport à la proposition que je formule, présente de mon point de vue certains inconvénients. L'échéance des élections municipales nous occupera en mars prochain. Les communes de plus de 30 000 habitants seront concernées par ce texte et elles disposeraient alors de moins d'un an pour former leurs agents puis organiser des procédures de passation de marchés et sélectionner de nouveaux prestataires. Ce délai paraît très court. Il importe qu'elles puissent se préparer et avancer de façon prudente, sans s'exposer au risque de contentieux. Une entrée en vigueur du dispositif au 1er janvier 2028, une date du reste pas excessivement éloignée, semble préférable.

M. Dany Wattebled. – L'Ugap est l'un des principaux donneurs d'ordre en matière de marchés publics. Forte d'un effectif de 2 000 professionnels, capable d'engager quelque 200 millions d'euros pour les marchés relatifs à l'hébergement des données de santé et de l'enseignement supérieur, elle a sans conteste les moyens de se mettre en ordre de marche sans retard. De plus, tous les acteurs sont aujourd'hui alertés sur les enjeux de la souveraineté numérique. Il est possible de les mettre en branle progressivement en fonction de leur poids et de leurs moyens respectifs. Je m'en tiens à ma position et je proposerai, si nécessaire, un amendement en ce sens.

Mme Muriel Jourda, présidente. – Le débat pourra se poursuivre en séance. Le sujet est en effet d'importance et chacun doit prendre le temps de la réflexion.

Concernant le périmètre de ce projet de loi, en application du vade-mecum sur l'application des irrecevabilités au titre de l'article 45 de la Constitution, adopté par la Conférence des présidents, je vous propose de considérer que le périmètre de la proposition de loi inclut les dispositions relatives aux modalités de sélection des titulaires et d'exécution des marchés publics comportant des prestations d'hébergement et de traitement de données publiques en nuage.

EXAMEN DE L'ARTICLE UNIQUE

Article unique

L'amendement COM-1 est adopté.

L'article unique constituant l'ensemble de la proposition de loi est adopté dans la rédaction issue des travaux de la commission.

Le sort de l'amendement examiné par la commission est retracé dans le tableau suivant :

Auteur	N°	Objet	Sort de l'amendement
Article unique			
Mme Olivia RICHARD, rapporteure	1	Amendement de réécriture globale	**Adopté**

RÈGLES RELATIVES À L'APPLICATION DE L'ARTICLE 45 DE LA CONSTITUTION ET DE L'ARTICLE 44 BIS DU RÈGLEMENT DU SÉNAT

Si le premier alinéa de l'article 45 de la Constitution, depuis la révision du 23 juillet 2008, dispose que « tout amendement est recevable en première lecture dès lors qu'il présente un lien, même indirect, avec le texte déposé ou transmis », le Conseil constitutionnel estime que cette mention a eu pour effet de consolider, dans la Constitution, sa jurisprudence antérieure, reposant en particulier sur « la nécessité pour un amendement de ne pas être dépourvu de tout lien avec l'objet du texte déposé sur le bureau de la première assemblée saisie » [1].

De jurisprudence constante et en dépit de la mention du texte « transmis » dans la Constitution, le Conseil constitutionnel apprécie ainsi l'existence du lien par rapport au contenu précis des dispositions du texte initial, déposé sur le bureau de la première assemblée saisie[2]. Pour les lois ordinaires, le seul critère d'analyse est le lien matériel entre le texte initial et l'amendement, la modification de l'intitulé au cours de la navette restant sans effet sur la présence de « cavaliers » dans le texte[3]. Pour les lois organiques, le Conseil constitutionnel ajoute un second critère : il considère comme un « cavalier » toute disposition organique prise sur un fondement constitutionnel différent de celui sur lequel a été pris le texte initial[4].

En application des articles 17 bis et 44 bis du Règlement du Sénat, il revient à la commission saisie au fond de se prononcer sur les irrecevabilités résultant de l'article 45 de la Constitution, étant précisé que le Conseil constitutionnel les soulève d'office lorsqu'il est saisi d'un texte de loi avant sa promulgation.

---

[1] Cf. *commentaire de la décision n° 2010-617 DC du 9 novembre 2010 - Loi portant réforme des retraites.*

[2] Cf. *par exemple les décisions n° 2015-719 DC du 13 août 2015 - Loi portant adaptation de la procédure pénale au droit de l'Union européenne et n° 2016-738 DC du 10 novembre 2016 - Loi visant à renforcer la liberté, l'indépendance et le pluralisme des médias.*

[3] *Décision n° 2007-546 DC du 25 janvier 2007 - Loi ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le code de la santé publique.*

[4] *Décision n° 2020-802 DC du 30 juillet 2020 - Loi organique portant report de l'élection de six sénateurs représentant les Français établis hors de France et des élections partielles pour les députés et les sénateurs représentant les Français établis hors de France.*

En application du *vademecum* sur l'application des irrecevabilités au titre de l'article 45 de la Constitution, adopté par la Conférence des Présidents, la commission des lois **a arrêté,** lors de sa réunion du mercredi 10 décembre 2025, **le périmètre indicatif de la proposition de loi n° 008 (2025-2026), relative à la sécurisation des marchés publics numériques**

Elle a considéré que **ce périmètre incluait** des dispositions relatives **aux modalités de sélection des titulaires et d'exécution des marchés publics comportant des prestations d'hébergement et de traitement de données publiques en nuage**.

LISTE DES PERSONNES ENTENDUES ET DES CONTRIBUTIONS ÉCRITES

M. Dany Wattebled, sénateur du Nord, auteur de la proposition de loi

Mme Catherine Morin-Desailly, sénatrice de la Seine-Maritime

M. Olivier Cadic, sénateur représentant les Français établis hors de France

Cabinet de la Ministre chargée de l'intelligence artificielle et du numérique

M. Adrien Laroche, directeur de cabinet

M. Loic Théréau, conseiller parlementaire

M. Samy Imourra, conseiller cybersécurité et régulation du numérique

Cabinet du Ministre chargé de la fonction publique et de la réforme de l'État

M. Emmanuel Constantin, directeur de cabinet

M. Jacques Meurin, conseiller parlementaire et chargé des relations avec les élus

M. Arthur Hatchuel, conseiller transformation numérique, qualité des services publics et simplification

Direction interministérielle du numérique

Mme Stéphanie Schaer, directrice interministérielle du numérique

M. Jérémie Vallet, directeur adjoint

Direction du numérique du ministère de l'Europe et des affaires étrangères

Mme Virginie Rozière, directrice

Direction des affaires juridiques (DAJ) des ministères économiques et financiers

Mme Clémence Olsina, directrice

Mme Céline Frackowiak, sous-directrice du droit de la commande publique

Mme Catherine Mansoux, adjointe à la sous-directrice du droit des régulations économiques

Direction générale des collectivités territoriales (DGCL)

M. Florentin Bertheas, chef du bureau du contrôle de légalité et du conseil juridique

Mme Julie Assemat, adjointe au chef du bureau du contrôle de légalité et du conseil juridique

Commission nationale de l'informatique et des libertés (CNIL)

M. Michel Combot, directeur des technologies, de l'innovation et de l'intelligence artificielle

M. Florent Della Valle, chef du service de l'expertise technologique

Mme Anne Fontanille, juriste au service des affaires européennes et internationales

Mme Chirine Berrichi, conseillère pour les questions parlementaires et institutionnelles

Audition conjointe

Agence nationale de la sécurité des systèmes d'information (ANSSI)

M. Vincent Strubel, directeur général

Mme Juliette Péron, conseillère

Direction générale des entreprises (DGE)

M. Loïc Duflot, chef du service de l'économie numérique

M. Renaud Rodenas, chef de projet « réglementation du *cloud* et de l'économie de la donnée »

Table ronde de représentants des acheteurs publics

Union des groupements d'achats publics (UGAP)

M. Edward Jossa, président-directeur général

Clusif

Mme Odile Duthil, présidente

Mme Florence Puyrabeau, directrice

Association pour l'achat dans les services publics (APASP)

M. Jean-Pierre Gohon, administrateur

Table ronde de sociétés d'informatique en nuage européennes

Hexatrust

Mme Dorothée Decrop, déléguée générale

Outscale

M. David Chassan, chef du bureau de la stratégie

M. Livio Klein-Clerc, chargé d'affaires publiques

OVH

Mme Blandine Eggrickx, responsable des affaires publiques

Personnalité qualifiée

M. Pierre-Ange Zalcberg, avocat

CONTRIBUTIONS ÉCRITES

Autorité de la concurrence

Association des maires de France et des présidents d'intercommunalité

Départements de France

Régions de France

Conseil national des achats

France Digitale

Groupe Iliad – Free

Amazon Web services

Google

Microsoft

LA LOI EN CONSTRUCTION

Pour naviguer dans les rédactions successives du texte, visualiser les apports de chaque assemblée, comprendre les impacts sur le droit en vigueur, le tableau synoptique de la loi en construction est disponible sur le site du Sénat à l'adresse suivante :

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