N° 2522

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DIX-SEPTIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 25 février 2026.

RAPPORT

FAIT

AU NOM DE LA COMMISSION DES LOIS CONSTITUTIONNELLES,
DE LA LÉGISLATION ET DE L'ADMINISTRATION GÉNÉRALE
DE LA RÉPUBLIQUE, SUR LA PROPOSITION DE LOI, ADOPTÉE PAR LE SÉNAT,

relative à la **sécurisation** *des* **marchés publics numériques**,

PAR M. PHILIPPE LATOMBE

Député

Voir les numéros :

Sénat **: 8**, **199**, **200** et **T.A. 33** (2025-2026)

Assemblée nationale **: 2258**

SOMMAIRE

MESDAMES, MESSIEURS,

L'essor rapide de l'informatique en nuage, ou *cloud computing*, transforme profondément les modes d'hébergement et de traitement des données au sein des administrations publiques.

En effet, en externalisant les serveurs, les capacités de stockage, les bases de données ou encore les applications utilisées par les agents et les usagers au sein d'infrastructures distantes, l'État et les collectivités territoriales bénéficient de solutions souples et évolutives, devenues indispensables au fonctionnement quotidien de leurs systèmes d'information.

Cependant, ce mouvement s'accompagne d'enjeux croissants en matière de sécurisation des données publiques et de souveraineté numérique, car le marché du *cloud* est dominé par quelques acteurs américains, qui concentrent près de 70 % des parts de marché en Europe.

Cette dépendance soulève trois risques majeurs :

– un risque juridique, d'abord, lié à l'application potentielle de législations extraterritoriales pouvant conduire à la communication non autorisée de données sensibles à des puissances étrangères ;

– un risque opérationnel, ensuite, dans la mesure où la plupart des logiciels reposant sur ces infrastructures proviennent également d'acteurs extra-européens, posant la question de la continuité de nos systèmes en cas de rupture d'accès ;

– un risque industriel, enfin, car la puissance des grands acteurs déjà présents sur le marché entrave l'émergence de concurrents européens robustes et compétitifs.

Face à ces vulnérabilités, le législateur et le Gouvernement ont résolument engagé une politique visant à permettre le développement de solutions de confiance.

La doctrine « *cloud* au centre », traduite par deux circulaires successives, puis la loi « Sren » du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique ont ainsi posé un principe clair : les données sensibles de l'État doivent être hébergées auprès de prestataires garantissant un niveau élevé de sécurité et une protection contre les normes juridiques extraterritoriales.

Toutefois, et bien que la pleine effectivité de ce dispositif demeure conditionnée à la publication du décret d'application prévu à l'article 31 de la loi « Sren » qui est toujours en attente, de récents travaux d'enquête conduits par le Sénat ont mis en lumière la nécessité de renforcer le niveau d'exigences qui pèse actuellement sur nos administrations.

C'est dans ce contexte que s'inscrit la présente proposition de loi, qui vise à étendre l'obligation de recourir à un *cloud* de confiance aux administrations publiques locales.

Dans sa rédaction initiale, le texte imposait que, pour les marchés publics comportant des prestations d'hébergement et de traitement de données publiques en nuage, l'acheteur prévoie des conditions d'exécution excluant l'application de législations étrangères à portée extraterritoriale, et garantissant l'hébergement de ces données sur le territoire de l'Union européenne.

Tout en reconnaissant l'intention légitime du texte, la commission des Lois du Sénat s'est attachée à rechercher un meilleur équilibre entre la nécessaire protection des données publiques stratégiques et la prise en compte des difficultés juridiques soulevées par cette rédaction, au regard notamment des grands principes qui régissent le droit de la commande publique.

La rédaction issue de la première lecture au Sénat, qui adosse le dispositif à l'article 31 de la loi « Sren » et à la doctrine « *cloud* au centre », constitue ainsi une évolution bienvenue.

Afin de garantir l'efficacité du dispositif et sa pleine opérationnalité, et sur proposition de votre Rapporteur, la Commission a poursuivi ce mouvement. Elle a ainsi précisé et enrichi le champ des administrations publiques locales concernées, et elle a clarifié les conditions de mise en œuvre de ces nouvelles exigences.

COMMENTAIRE DE L'ARTICLE UNIQUE

Article unique
(art. 31-1 [nouveau] de la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique)

Extension aux offres souscrites par les collectivités territoriales des exigences de protection des données sensibles applicables aux services d'informatique en nuage

Adopté par la Commission avec modifications

➢ Résumé du dispositif et effets principaux

L'**article unique** de la proposition de loi crée un nouvel article L. 2112-4-1 dans le code de la commande publique qui dispose que, pour les marchés publics comportant des prestations d'hébergement et de traitement de données publiques en nuage, l'acheteur prévoit des conditions d'exécution excluant l'application de législations étrangères à portée extraterritoriale, et garantissant l'hébergement de ces données sur le territoire de l'Union européenne.

➢ Les modifications apportées par le Sénat

Le Sénat a intégralement réécrit l'article unique de la proposition de loi. Dans sa nouvelle rédaction, celui-ci étend les obligations actuellement prévues à l'article 31 de la loi « Sren » aux collectivités territoriales et établissements publics de coopération intercommunale à fiscalité propre, à l'exception des communes de moins de 30 000 habitants ainsi que les communautés de communes.

Le Sénat a par ailleurs prévu une date d'entrée en vigueur différée, fixée à un an après la promulgation de la loi.

➢ Les modifications apportées par la Commission

Sur proposition de votre Rapporteur, la Commission a adopté un amendement de rédaction globale qui complète et précise le dispositif adopté au Sénat, afin d'en garantir l'efficacité et la pleine opérationnalité.

L'amendement procède à quatre modifications principales :

– il étend le champ des administrations locales concernées, en le rapprochant de celui actuellement défini pour les entités dites « essentielles » par le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, en cours de discussion à l'Assemblée nationale ;

– il élargit la notion de données d'une sensibilité particulière, afin de l'adapter aux compétences des administrations locales concernées ;

– il encadre la clause dérogatoire, en prévoyant notamment un délai maximal de dix-huit mois ;

– il sécurise la possibilité pour l'administration locale concernée de résilier les contrats en cours.

I. L'ÉTAT DU DROIT

A. UNE DÉPENDANCE MARQUÉE DE LA FRANCE AUX SERVICES D'INFORMATIQUE EN NUAGE ÉTRANGERS, QUI POSE UN RISQUE POUR LA CONFIDENTIALITÉ DES DONNÉES

La notion de souveraineté numérique a émergé dans le débat public depuis le début des années 2010, à la suite, notamment, des révélations d'Edward Snowden concernant le programme de surveillance de masse mis en œuvre par les États-Unis, leur permettant de collecter des données auprès des grandes entreprises technologiques américaines.

Dans son acception traditionnelle, la **souveraineté** se « *définit […] comme la caractéristique par excellence d'un État, c'est-à-dire le contrôle effectif d'un territoire et d'une population, l'indépendance ou la non-sujétion à l'égard d'un pouvoir supérieur, ainsi que la liberté de pouvoir contracter un engagement avec d'autres États* » (1).

La notion de **souveraineté numérique** suppose quant à elle la maîtrise par l'État des technologies afin de conserver une capacité autonome d'appréciation, de décision et d'action dans le cyberespace, alors même que les entreprises dominantes dans le domaine du numérique sont américaines, et que les législations extraterritoriales se développent (2).

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).

En effet, si, en droit international public, et en application du principe de souveraineté, la compétence territoriale est la règle, un État reste libre d'établir une compétence extraterritoriale, sous réserve d'une norme de droit international l'interdisant explicitement. Un État peut ainsi étendre la portée de ses lois au-delà de ses frontières, à condition de respecter certains critères de rattachement : il peut notamment s'agir du rattachement « personnel », lié à la nationalité de l'auteur ou de la victime d'une infraction commise à l'étranger, ou du rattachement

---

(1) Conseil d'État, La souveraineté*, étude annuelle 2024.*

(2) Cour des comptes, Les enjeux de souveraineté des systèmes d'information civils de l'État*, octobre 2025.*

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

« matériel », prenant en considération l'objet de la norme, par exemple la préservation des intérêts fondamentaux de l'État, tel que la sécurité nationale (1).

La notion d'extraterritorialité est ancienne (2), mais elle s'est fortement **développée aux États-Unis** au tournant du XX^{ème} siècle, dans des domaines aussi divers que les sanctions internationales (3), la lutte contre la corruption (4), la lutte contre la fraude fiscale (5) et, plus récemment, dans le domaine du **numérique**.

Plusieurs législations peuvent ainsi être mobilisées pour imposer aux entreprises du numérique, et plus particulièrement aux prestataires de services d'informatique en nuage, ou *cloud computing*, de communiquer des données, y compris lorsque ces entreprises opèrent en dehors du territoire national. Il s'agit notamment :

– de l'***Executive Order 12333*** du 4 décembre 1981, complété par l'*Executive Order 13470* en 2008, qui organisent l'action des agences de renseignement des États-Unis. Si ce texte porte essentiellement sur les activités de renseignement dans un objectif de sécurité nationale, il autorise la collecte massive de renseignements à l'étranger, de manière unilatérale, en dehors de toute cadre judiciaire et sans voie de recours ;

– du ***Foreign Intelligence Surveillance Act*** (FISA), dont la section 702, introduite par amendement en 2008, permet aux agences américaines de renseignement de collecter, sans mandat individuel, les communications électroniques, y compris les données hébergées dans le *cloud*, de personnes étrangères situées hors des États-Unis, dès lors que ces données transitent par des serveurs exploités par des sociétés domiciliées aux États-Unis. Le FISA n'autorise cependant pas à cibler des personnes de manière individuelle, mais des catégories d'informations à collecter auprès des fournisseurs de services de communication électronique ;

– du ***Clarifying Lawful Overseas Use of Data Act*** (*Cloud Act*) de 2018, qui dispose que toute société incorporée aux États-Unis (et que toutes les sociétés qu'elle contrôle) doit communiquer aux autorités américaines les données de communication qu'elle contrôle sans considération du lieu où ces données se trouvent stockées. Cette obligation concerne également des filiales américaines d'entreprises étrangères. Un mandat ou une autorisation d'un juge est cependant nécessaire ;

---

(1) Voir par exemple le rapport de M. Raphaël Gauvain, « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale », remis au Premier ministre le 26 juin 2019.

(2) Voir l'arrêt de la Cour permanente de justice internationale rendu dans l'affaire dite du « Lotus », le 7 septembre 1927.

(3) La loi « Helms-Burton » de 1996 renforce l'embargo contre Cuba, tandis que la loi « Amato-Kennedy » adoptée la même année vise à sanctionner les entreprises investissant dans les secteurs énergétiques d'Iran et de Libye.

(4) Le Foreign Corrupt Pratices Act*, modifié en 1998.*

(5) Le Foreign Account Tax Compliance Act*, adopté en 2010.*

La portée de ces législations est d'autant plus importante en raison de la domination technologique et économique de certaines grandes entreprises américaines du numérique, et notamment des « GAFAM » (Google, Amazon, Facebook-Meta, Apple, Microsoft).

D'après la Cour des comptes, le marché du *cloud* européen est en forte augmentation ces dernières années : il a été multiplié par 5 entre 2017 et 2022. Ce marché est dominé par des acteurs américains dit *hyperscalers* (capables de s'adapter rapidement à des demandes importantes de ressources) : Amazon Web Services (AWS), Microsoft Azure et Google Cloud représentent ainsi 70 % des parts de marché en Europe. De plus, la part des fournisseurs de *cloud* européens a connu une diminution au cours des dernières années, passant de 27 % en 2017 à 16 % 2021, alors même que leur chiffre d'affaires augmentait de 167 %.

Bien que la législation extraterritoriale américaine occupe une place centrale dans les réflexions actuelles en raison de la puissance de l'industrie numérique des États-Unis, d'autres pays ont récemment adopté des textes dont la dimension extraterritoriale leur ouvre la possibilité de collecter des données étrangères, comme la Chine (1) ou l'Inde (2).

B. LE DROIT EUROPÉEN A PERMIS LA MISE EN PLACE D'UN CADRE PROTECTEUR POUR LES DONNÉES PERSONNELLES, BIEN QU'IMPARFAIT

Dès le milieu des années 1990, le droit de l'Union européenne a prévu des dispositions protectrices des données des individus. Ainsi, l'article 25 de la directive 95/46/CE du 24 octobre 1995 relative à la protection des données personnelles prévoyait-elle déjà 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* » (3).

C'est surtout à partir du règlement général sur la protection des données (RGPD) du 27 avril 2016 (4), adopté à la suite des révélations d'Edward Snowden, que l'Union européenne va renforcer les exigences relatives au contrôle des citoyens sur leurs données personnelles.

Le RGPD fait peser des obligations importantes sur le responsable de traitement de données à caractère personnel. Celui-ci doit ainsi mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un

---

(1) Loi sur le renseignement national de la République populaire de Chine, adoptée le 27 juin 2017.

(2) Digital Personal Data Protection Act (act n° 22 of 2023), 11 août 2023.

(3) Directive 95/46/CE du Parlement européen 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 de ces données

(4) 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).

niveau de sécurité adapté au risque pour les droits et libertés des personnes physiques dont il traite les données. Selon la nature et la finalité des données, il doit garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement (1). Toute violation de données doit être notifiée aux autorités de contrôle et communiquée à la personne physique concernée (2).

Le règlement encadre également les conditions dans lesquelles un transfert de données vers un pays extérieur à l'Union européenne est possible.

Ainsi, lorsque la Commission a constaté par une **décision d'adéquation** que le pays tiers en question assure un niveau de protection adéquat, le transfert ne nécessite **pas d'autorisation spécifique**. Lorsqu'elle évalue le caractère adéquat du niveau de protection, la Commission tient compte de nombre d'éléments, et notamment de l'état de droit, du respect des droits de l'homme et des libertés fondamentales, de la législation en matière de sécurité nationale ou encore de l'accès des autorités publiques aux données à caractère personnel (3).

En l'absence de décision d'adéquation, un transfert n'est possible que si le responsable du traitement a prévu des « *garanties appropriées* », qui peuvent notamment résulter de clauses types de protection des données adoptées par la Commission européenne, et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives. Des dérogations sont enfin possibles en cas de situations particulières (4).

Enfin, le règlement prévoit que **toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant un transfert de données à caractère personnel ne peut être 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 (5).

Le statut spécifique des États-Unis a fait l'objet de débats importants depuis le milieu des années 2010. Dans deux décisions de 2015 (6) et 2020 (7), la Cour de justice de l'Union européenne a ainsi invalidé les décisions d'adéquation rendues par la Commission, en raison d'un niveau insuffisant de protection des données personnelles dans le cas de leur transfert à finalité commerciale vers le sol américain.

---

(1) Article 32 du RGPD.

(2) Article 33 et 34 du RGPD.

(3) Article 45 du RGPD.

(4) Articles 46 et 49 du RGPD.

(5) Article 48 du RGPD.

(6) Arrêt de la Cour du 6 octobre 2015, Affaire C-362/14, Maximillian Schrems contre Data Protection Commissioner.

(7) Arrêt de la Cour du 16 juillet 2020, Affaire C-311/18, Data Protection Commissioner/ Facebook Ireland Limited, Maximillian Schrems.

Une nouvelle décision d'adéquation a finalement été rendue par la Commission européenne en juillet 2023, fondée sur un mécanisme d'auto-certification des entreprises américaines, le *Data Privacy Shield.* Les transferts de données opérés vers des entreprises certifiées sont considérés comme présentant un niveau de protection adéquat (1). Malgré un premier recours porté par votre Rapporteur devant le Tribunal de l'Union européenne, rejeté en septembre 2025 (2), **la décision *Data Privacy Shield* est toujours en vigueur**.

D'après la Cour des comptes, « *cette décision d'adéquation crée un cadre pour l'échange de données personnelles entre l'UE et les États-Unis, et facilite le travail des entreprises européennes* », mais « ***ne constitue toutefois pas un rempart sur les enjeux de souveraineté et l'application des lois extraterritoriales*** » (3).

Dernièrement, le règlement sur les marchés numériques (***Digital Markets Act***, ou *DMA*) de 2022 (4) et le règlement sur la protection des données (***Data Act***) de 2023 (5) ont renforcé les obligations pesant sur certains gestionnaires de données. En particulier, l'article 32 du *Data Act* a prévu que les fournisseurs de services de traitement de données prennent toutes les mesures techniques, organisationnelles et juridiques adéquates, afin d'empêcher l'accès international des autorités publiques et l'accès des autorités publiques des pays tiers aux **données à caractère non personnel** détenues dans l'Union, et le transfert de ces données lorsque ce transfert ou cet accès risque d'être en conflit avec le droit de l'Union ou le droit national de l'État membre concerné.

Enfin, depuis 2020, l'Agence de l'Union européenne pour la cybersécurité (ENISA) (6) élabore une **certification européenne relative aux prestataires de *cloud***, dite EUCS (pour *European Union Cybersecurity Certification Scheme for Cloud Services*). Dans le cadre de ces négociations, la France promeut la mise en place d'exigences permettant notamment d'assurer la protection des données les plus sensibles face à l'application de lois extraterritoriales par des autorités de pays non-européens. Cette position a conduit à une forte opposition des États membres au sein du Groupe européen de certification de sécurité, enceinte dédiée à l'élaboration des schémas de certification, et finalement au blocage des négociations.

---

(1) La liste des entreprises certifiées est consultable en ligne : https://www.dataprivacyframework.gov/list.

(2) Affaire T553-23 Philippe Latombe contre Commission européenne.

(3) Cour des comptes, op. cit., page 23.

(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) 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.

(6) European Union Agency for Network and Information Security*, devenue* European Union Agency for Cybersecurity.

C. LE DROIT DE LA COMMANDE PUBLIQUE NE PERMET PAS, EN PRATIQUE, D'ÉCARTER SYSTÉMATIQUEMENT LES SOLUTIONS D'INFORMATIQUE EN NUAGE QUI SONT POTENTIELLEMENT SOUMISES À DES LOIS EXTRATERRITORIALES

Le droit de la commande publique repose sur les principes d'égalité de traitement des candidats, de liberté d'accès à la commande publique et de transparence des procédures.

Ces principes bénéficient de **garanties constitutionnelles** (1), et ont été inscrits à l'article L. 3 du code de la commande publique (CCP).

Ils sont également protégés par les règles fondamentales du **Traité sur le fonctionnement de l'Union européenne** (TFUE) (2), et trouvent notamment à s'appliquer aux marchés d'un montant inférieur aux seuils européens pour peu qu'ils présentent un intérêt transfrontalier certain (3).

Enfin, l'article 25 de la directive du 26 février 2014 sur la passation des marchés publics (4) impose aux pouvoirs adjudicateurs d'accorder aux services et aux opérateurs économiques des États parties à l'**Accord sur les marchés publics de l'Organisation mondiale du Commerce** (OMC) un traitement non moins favorable que celui accordé aux services et aux opérateurs économiques de l'Union européenne. Ce principe, qui est également inscrit à l'article L. 2153-1 du CCP, **prohibe l'intégration de clauses relatives à la nationalité du répondant dans les appels d'offres**.

Le droit de la commande publique permet d'intégrer aux appels d'offres des clauses en matière de sécurité permettant de déroger à ces grands principes. Toutefois, de telles clauses sont très encadrées, et nécessitent un examen au cas par cas.

Ainsi, l'article L. 2512-3 du CCP permet de déroger à l'application du droit de la commande publique au stade de la passation des marchés, pour garantir la protection des **intérêts essentiels de l'État**.

---

(1) Décision n° 2003-473 DC du 26 juin 2003, Loi habilitant le Gouvernement à simplifier le droit.

(2) 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 et abrogeant la directive 2004/18/CE dispose ainsi : « La passation de marchés publics par les autorités des États membres ou en leur nom doit être conforme aux principes du traité sur le fonctionnement de l'Union européenne, notamment la libre circulation des marchandises, la liberté d'établissement et la libre prestation de services, ainsi qu'aux principes qui en découlent comme l'égalité de traitement, la non-discrimination, la reconnaissance mutuelle, la proportionnalité et la transparence. *»*

(3) Voir notamment la décision de la Cour de justice des communautés européennes (CJCE) du 20 octobre 2005, Commission c/ République française*, aff. C-264/03 : « le seul fait que le législateur communautaire a considéré que les procédures particulières et rigoureuses prévues par les directives relatives aux marchés publics ne sont pas appropriées lorsqu'il s'agit de marchés publics d'une faible valeur ne signifie pas que ces derniers sont exclus du champ d'application du droit communautaire ».*

(4) Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE.

Il ressort néanmoins de la jurisprudence de la CJUE relative aux entraves aux règles du marché intérieur que le recours à pareille justification suppose l'existence d'une **menace réelle et suffisamment grave affectant un intérêt fondamental de la société** (1).

Par ailleurs, l'article L. 2112-4 du CCP prévoit que 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.

Comme le rappelle la Cour de justice de l'Union européenne, les acheteurs ne peuvent toutefois recourir à cette disposition que lorsque cela est **justifié** par l'objet du marché, **nécessaire** et **proportionné** aux objectifs de bonne exécution du contrat (2). De plus, le règlement sur les données à caractère non personnel du 14 novembre 2018 interdit les exigences de localisation des données, sauf si elles sont justifiées par des motifs de sécurité publique dans le respect du principe de proportionnalité (3).

Pour mettre en œuvre cette dérogation, l'acheteur devrait donc pouvoir démontrer que seule la localisation des données sur le territoire de l'Union européenne lui permet d'atteindre ses objectifs en matière de sécurité des informations, ce qui n'est pas le cas : la localisation « physique » des serveurs ne peut à elle seule prémunir contre l'application des lois extraterritoriales.

Ainsi, les possibilités de dérogation au droit de la commande publique paraissent insuffisantes pour protéger durablement les administrations publiques des conséquences des lois extraterritoriales.

D. LA DOCTRINE « *CLOUD* AU CENTRE » ET LA LOI « SREN » ONT POSÉ UN CADRE AMBITIEUX

La loi du 7 octobre 2016 pour une République numérique (4) a constitué une première étape dans la reconnaissance de la notion de souveraineté numérique au sein des administrations publiques, en prévoyant notamment que celles-ci « *veillent à préserver la maîtrise, la pérennité et l'indépendance de leurs systèmes d'information* ».

---

(1) Voir par exemple la décision de la Cour de justice de l'Union européenne (CJUE) du 14 février 2019, Milivojević, aff. C-630/17, point 67).

(2) CJCE, 27 octobre 2005, Commission des Communautés européenne c/ Royaume d'Espagne*, Aff. C-158/03.*

(3) Article 4 du Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne.

(4) Article 16 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

La doctrine « *Cloud au centre* », qui a pris la forme de deux circulaires publiées en 2021 et 2023 [(1)], a par la suite posé des exigences fortes visant à assurer la pleine maîtrise par les administrations de leurs données hébergées par des prestataires privés d'informatique en nuage. Cette doctrine a été élevée au niveau législatif par la loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, dite loi « Sren » [(2)].

1. La reconnaissance de garanties fortes pour les données les plus sensibles avec la doctrine française du « *Cloud* au centre »

Annoncée par le Gouvernement en mai 2021, la stratégie nationale du *cloud* entendait répondre à un triple enjeu : un enjeu de transformation pour l'État, d'abord ; un enjeu de souveraineté et de sécurité des données, ensuite ; un enjeu industriel pour l'écosystème français et européen de l'informatique en nuage, enfin.

La **circulaire du 5 juillet 2021** invitait ainsi les administrations publiques à recourir à l'informatique en nuage pour l'hébergement de tout produit numérique nouveau ou faisant l'objet d'une évolution substantielle.

La circulaire édictait quinze règles que les administrations devaient suivre dans la mise en œuvre de cette doctrine. En particulier, la règle « R9 » prévoyait que dans le cas d'un recours à une offre de *cloud* commerciale, si le système ou l'application informatique manipulait des **données d'une sensibilité particulière**, qu'elles relèvent notamment des données personnelles des citoyens français, des données économiques relatives aux entreprises françaises, ou d'applications métiers relatives aux agents publics de l'État, l'offre de *cloud* commercial retenue devrait impérativement **respecter la qualification SecNumCloud**, ou une qualification européenne d'un niveau au moins équivalent, et **être immunisée contre toute réglementation extracommunautaire**.

(1) Circulaire n° 6282-SG du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État, et circulaire 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 »).*

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

La qualification SecNumCloud

La qualification SecNumCloud permet d'identifier des offres *cloud* dites « de confiance », dont l'utilisation est préconisée pour la protection des données sensibles.

Élaborée par l'Agence nationale de la sécurité des systèmes d'information (Anssi) et en vigueur depuis 2016, cette qualification est fondée sur un ensemble de règles de sécurité et de bonnes pratiques devant être respectées par le fournisseur du service, qui garantissent un haut niveau d'exigence aux plans technique, opérationnel et juridique. Celles-ci doivent permettre de protéger les données et les traitements sensibles face à la menace cybercriminelle et l'application de lois extraterritoriales.

Ces règles sont de nature très diverses, allant de l'encadrement des modalités de contrôle des accès et de gestion des identités aux mécanismes de chiffrement utilisés, en passant par la sécurité des ressources humaines, la localisation des données ou la composition de l'actionnariat.

Le référentiel a évolué à plusieurs reprises. La version 3.2, d'une longueur de 55 pages, a été publiée le 8 mars 2022.

La qualification est valable pour une durée de 3 ans. Elle est conditionnée au respect des engagements du prestataire durant toute la durée de la qualification.

À ce jour, 11 prestataires proposent une offre qualifiée SecNumCloud et 14 demandes supplémentaires de qualification sont en cours d'instruction.

La **circulaire du 31 mai 2023** a procédé à l'actualisation de la doctrine « *Cloud* au centre », afin, notamment, de mieux délimiter le périmètre des données d'une sensibilité particulière pour lesquelles le recours à une solution d'hébergement qualifiée SecNumCloud et immunisée au droit extracommunautaire est requise, et de préciser les modalités de demandes de dérogation à cette règle.

La nouvelle rédaction de la règle « R9 » prévoit désormais une **double condition** applicable aux données, à caractère personnel ou non, traitées par le système ou l'application informatique : d'une part, celles-ci doivent désormais être d'une **sensibilité particulière** ; d'autre part, leur violation doit être susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé et la vie des personnes ou à la protection de la propriété intellectuelle.

En présence de telles données, l'offre de *cloud* commerciale retenue devra impérativement respecter la qualification **SecNumCloud** (ou une qualification européenne garantissant un niveau au moins équivalent, notamment de cybersécurité) et **être immunisée contre tout accès non autorisé par des autorités publiques d'État tiers.**

2. L'article 31 de la loi du 21 mai 2024, dite loi « Sren », a élevé les exigences de la circulaire « *Cloud* au centre » au niveau législatif

L'article 31 de la loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, dite loi « Sren », a inscrit dans la loi les exigences de la circulaire « *Cloud* au centre » précitée.

Il tend ainsi à garantir la protection de données stratégiques et sensibles traitées par les administrations publiques, sur le marché de l'informatique en nuage.

Ainsi, lorsque le service d'informatique en nuage est fourni pour la mise en œuvre de systèmes ou d'applications informatiques, et que le système ou l'application informatique concerné traite de **données sensibles**, l'administration publique concernée veille à ce que le service de *cloud* mette en œuvre **des 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**.

Il s'agit de protéger les données concernées contre toute demande d'une autorité publique étrangère, judiciaire comme administrative, en dehors d'un accord international en vigueur entre le pays demandeur et l'Union ou un État membre.

La sensibilité des données est appréciée sur le fondement de **deux critères cumulatifs**, comme le prévoyait la circulaire « *Cloud* au centre » actualisée en 2023 :

– d'une part, **les données, qu'elles soient à caractère personnel ou non, doivent être d'une « *sensibilité particulière* »**, ce qui renvoie à deux grandes catégories :

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

* 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, la **violation de ces données doit être 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 articles L. 311-5 et L. 311-6 du code des relations entre le public et l'administration

L'article L. 311-5 du CRPA exclut la communication de certains documents administratifs, et notamment :

– les avis du Conseil d'État et des juridictions administratives, les mesures d'instruction, rapports et diverses communications des juridictions financières, certains documents élaborés ou détenus par des autorités administratives indépendantes (Autorité de la concurrence, Haute Autorité pour la transparence de la vie publique) les documents préalables à l'élaboration du rapport d'accréditation des établissements de santé et des personnels de santé, 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, au secret des délibérations du Gouvernement et des autorités responsables relevant du pouvoir exécutif, au secret de la défense nationale, à la conduite de la politique extérieure de la France, 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, à la monnaie et au crédit public, au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, sauf autorisation donnée par l'autorité compétente, à la recherche et à la prévention, par les services compétents, d'infractions de toute nature, ou aux autres secrets protégés par la loi.

L'article L. 311-6 du même code prévoit par ailleurs que 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 en question 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.

Un **vade-mecum** sur la sensibilité des données au sens de l'article 31 de la loi SREN, qui présente notamment des exemples concrets, a été publié au mois de février 2026 sur le site de la direction interministérielle du numérique (Dinum) [(1)].

En revanche, si les données concernées ne sont pas considérées comme des données sensibles, c'est-à-dire si elles ne respectent pas l'un ou l'autre des critères, la loi n'exige pas le recours à une offre commerciale sécurisée.

(1) https://www.numerique.gouv.fr/offre-accompagnement/reference-vade-mecum-sensibilite-donnees/

L'article 31 de la loi « Sren » détermine précisément les **personnes publiques concernées**. Il s'agit :

– des **administrations de l'État** ;

– de leurs **opérateurs**, dont la liste est année au projet de loi de finances. Dans le PLF pour 2026, 431 opérateurs étaient recensés dans le « jaune budgétaire » *Opérateurs de l'État* (1) ;

– des **groupements d'intérêt public** comprenant les administrations ou les opérateurs mentionnés ci-dessus, et dont la liste est fixée par décret en Conseil d'État ;

– de la **Plateforme des données de santé** (2).

L'article 31 de la loi « Sren » prévoit enfin des **dérogations**. Ainsi, lorsque, à la date d'entrée en vigueur de cette disposition, l'administration publique concernée a **déjà engagé un projet nécessitant le recours à un service d'informatique en nuage**, cette administration peut solliciter une dérogation.

La dérogation est accordée par le ministre dont relève le projet déjà engagé, après validation par le Premier ministre ; elle doit être motivée et rendue publique.

La dérogation **ne peut excéder dix-huit mois à compter de la date à laquelle une offre de service d'informatique en nuage « *acceptable* » est disponible en France**, et fixe éventuellement les critères selon lesquels une telle offre peut être considérée comme telle. La circulaire du 31 mai 2023 précisait qu'une offre « *acceptable* » devait être entendue comme une offre « *dont les éventuels inconvénients sont supportables ou compensables* ».

Les modalités d'application de cet article doivent encore être **précisées par décret** en Conseil d'État, qui doit notamment préciser les critères de sécurité et de protection, y compris en termes de détention du capital, les conditions dans lesquelles les dérogations peuvent être accordées, ainsi que la liste des GIP entrant dans le champ du dispositif. Bien que la loi ne le précise pas, il est également attendu que le décret précise le champ des données sensibles.

Si l'article 31 de la loi « Sren » prévoyait que le décret d'application soit pris dans un délai de six mois à compter de sa promulgation, **celui-ci n'a toujours pas été pris**.

---

(1) Voir le « jaune budgétaire » Opérateurs de l'État.

(2) Aux termes de l'article L. 1462-1 du code de la santé publique, le groupement d'intérêt public « Plateforme des données de santé » est constitué entre l'État, des organismes assurant une représentation des malades et des usagers du système de santé, des producteurs de données de santé et des utilisateurs publics et privés de données de santé, y compris des organismes de recherche en santé. Il est notamment chargé de réunir, d'organiser et de mettre à disposition les données du système national des données de santé (SNDS) et de promouvoir l'innovation dans l'utilisation des données de santé.

La Cour des comptes relevait dans le rapport précité qu'un projet de décret avait été transmis par la France à la Commission européenne en janvier 2025. 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'avait été émise dans ce délai (1).

Plus récemment, le ministre de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique, M. Roland Lescure, indiquait devant le Sénat que le décret d'application était est actuellement examiné par le Conseil d'État, et qu'il pourrait être publié **avant le mois de mai 2026** (2).

II. LE DISPOSITIF PROPOSÉ

La proposition de loi traduit les recommandations du rapport de la commission d'enquête du Sénat sur les coûts et les modalités effectifs de la commande publique et la mesure de leur effet d'entraînement sur l'économie française, qui insistait sur la nécessité d'assurer la protection des données détenues par les services de l'État contre le droit extraterritorial étranger (3).

La commission d'enquête constatait notamment « *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* ».

Elle insistait en particulier sur la nécessité 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* (4).

L'**article unique** de la proposition de loi traduit cet objectif. Il tend à renforcer substantiellement les exigences en matière de sécurité et de protection des données pesant sur les offres de *cloud*, en confiant les données de l'ensemble des acheteurs publics à des prestataires français ou européens.

Il crée pour cela un nouvel article L. 2112-4-1 dans le code de la commande publique qui dispose que, pour les marchés comportant des prestations d'hébergement et de traitement de données publiques en nuage, l'acheteur prévoit des conditions 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, et **garantissant l'hébergement**

---

(1) Le projet de décret, notifié sous le numéro 2025/0041/FR, est consultable sur le site de la Commission européenne : https://technical-regulation-information-system.ec.europa.eu/fr/notification/26621.

(2) Séance de questions au Gouvernement du 11 février 2026, en réponse à une question de M. Dany Wattebled.

(3) Rapport n° 830 fait au nom 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, par M. Dany Wattebled, rapporteur, enregistré à la Présidence du Sénat le 8 juillet 2025.

(4) Recommandation n° 24.

de ces données sur le territoire de l'Union européenne dans des conditions assurant leur protection contre toute ingérence par des États tiers.

Ce dispositif renforce significativement les exigences prévues par le texte initial, à plusieurs égards.

Ainsi, concernant la nature des données concernées, le dispositif de la proposition de loi étend ces exigences à l'**ensemble des données**, qu'elles présentent ou non une sensibilité particulière.

Par ailleurs, s'agissant des personnes concernées, le dispositif est applicable à l'ensemble des acheteurs et autorités concédantes soumis au code de la commande publique. Seraient ainsi notamment concernées l'ensemble des **personnes morales de droit public.**

Enfin, le dispositif ne prévoit **pas de mécanisme de dérogation, ni d'entrée en vigueur différée** conditionnée à la publication du décret d'application.

III. LES MODIFICATIONS APPORTÉES PAR LE SÉNAT

Tout en reconnaissant l'intention légitime du texte, la commission des Lois du Sénat s'est attachée à rechercher un meilleur équilibre entre la nécessaire protection des données publiques stratégiques, et la prise en compte des difficultés juridiques et opérationnelles soulevées par la rédaction initiale.

La rapporteure, Mme Olivia Richard, relevait en effet que, tel qu'il était rédigé, l'article unique présentait **plusieurs difficultés**.

Premièrement, les obligations nouvelles que l'article unique entendait imposer présentaient un **risque de contrariété aux normes supérieures**. En effet, en écartant les acteurs non-européens de la commande publique de *cloud*, le dispositif pourrait s'apparenter à une discrimination en raison de la nationalité du fournisseur, ce qu'interdisent le droit européen et les engagements internationaux de la France traduits dans le code de la commande publique [(1)].

Deuxièmement, le dispositif proposé demeurait **imprécis sur plusieurs points**. Ces imprécisions laissaient craindre une insécurité juridique pour les contrats conclus sur son fondement, sans permettre de garantir pleinement la sécurité des données concernées.

D'une part, la notion de « *données publiques* » ne faisant actuellement pas l'objet d'une définition juridique, le dispositif était susceptible de donner lieu à **confusion pour les acheteurs quant au périmètre des données à héberger sur un *cloud* souverain**.

(1) Cf. infra.

Le manque de précision de ces exigences aurait par ailleurs rendu complexe la passation et la mise en œuvre des marchés concernés, en particulier pour les acheteurs publics de petite taille, qui ne disposent pas nécessairement d'expertise en la matière, tandis que le caractère étendu de l'obligation aurait très probablement occasionné des surcoûts pour les acheteurs, car les offres souveraines actuellement disponibles sont sensiblement plus chères.

D'autre part, le dispositif ne mentionnait **aucune exigence particulière en matière de sécurité** (contre le piratage ou le vol de données par exemple), alors que les attaques « cyber » constituent pourtant une menace grandissante.

Troisièmement, le dispositif pourrait produire des **effets contre-productifs sur le secteur du *cloud* français et européen**, en excluant de l'ensemble des marchés publics de *cloud* les acteurs qui ne disposent pas encore de la qualification « SecNumCloud » déployée par l'Anssi, ou qui ne peuvent pas procéder aux lourds investissements nécessaires.

Sur proposition de sa rapporteure, **la commission des Lois du Sénat a donc intégralement réécrit l'article unique de la proposition de loi**.

Plutôt qu'une modification du code de la commande publique, dont la portée aurait été trop large et peu proportionnée aux risques encourus, la nouvelle rédaction de l'article propose d'étendre les obligations actuellement prévues à l'article 31 de la loi « Sren » à certaines collectivités territoriales ainsi qu'à certains établissements publics de coopération intercommunale.

L'amendement adopté procède ainsi à quatre évolutions [(1)] :

– il restreint 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 » ;

– il recentre le dispositif sur les collectivités territoriales et les établissements publics de coopération intercommunale, en **excluant 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* ». Le seuil de 30 000 est défini par analogie à celui retenu dans le projet de loi « cyber-résilience » [(2)], qui vise à imposer de nouvelles mesures en matière de cybersécurité aux seules collectivités territoriales et EPCI de taille significative ;

– il prévoit un **mécanisme de dérogation**, lorsque la collectivité ou l'établissement public de coopération intercommunale a « *déjà engagé un projet nécessitant le recours à un service d'informatique en nuage ou [justifie] de difficultés techniques ou d'un risque de surcoût important* » ;

---

(1) Amendement COM-1 de Mme Olivia Richard, rapporteure.

(2) Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

– il prévoit une **entrée en vigueur du dispositif le 1er janvier 2028**.

En séance publique, sur proposition de M. Dany Wattebled [(1)], suivant l'avis de sa rapporteure et malgré l'avis défavorable du Gouvernement, le Sénat a modifié les modalités d'entrée en vigueur du dispositif en prévoyant une date d'entrée en vigueur « glissante » et non plus fixe, un **an après la promulgation de la loi.**

IV. LES MODIFICATIONS APPORTÉES PAR LA COMMISSION

Sur proposition de votre Rapporteur, la commission des Lois a adopté un **amendement de rédaction globale de l'article unique** [(2)].

En effet, si la nouvelle écriture proposée par le Sénat constituait une évolution bienvenue, des précisions devaient encore être apportées afin de garantir l'efficacité du dispositif et sa pleine opérationnalité.

L'amendement adopté procède à **quatre évolutions principales**.

Premièrement, il étend le champ des administrations locales concernées, en le rapprochant de celui actuellement défini pour les entités dites « *essentielles* » par le projet de loi « cyber-résilience » en cours de discussion à l'Assemblée nationale [(3)].

Concrètement, l'amendement tend à imposer les obligations de protection des données sensibles :

– aux collectivités territoriales et à leurs établissements publics administratifs ;

– aux groupements de collectivités, c'est-à-dire aux établissements publics de coopération intercommunale à fiscalité propre (communautés de communes, communautés d'agglomération, communautés urbaines et métropoles – ainsi qu'à leurs établissements publics administratifs), aux syndicats de communes, aux syndicats mixtes et aux institutions ou organismes interdépartementaux ;

– aux services départementaux d'incendie et de secours ;

– aux centres de gestion.

Afin de tenir compte des contraintes qui pèsent sur les petites communes, et par cohérence avec le projet de loi « cyber-résilience » précité, la nouvelle rédaction de l'article maintient le seuil de 30 000 habitants qu'avait introduit le

---

(1) Amendement n° 1 rect. *De M. Dany Wattebled.*

(2) Amendement CL13 de M. Philippe Latombe, rapporteur.

(3) Article 8 du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité. L'article 9 définit quant à lui les infrastructures critiques.

Sénat pour les communes, qu'il étend aux communautés de communes, aux syndicats mixtes et aux syndicats de communes. Ainsi, **seules les communes, les communautés de communes, les syndicats mixtes et les syndicats de communes de plus de 30 000 habitants seraient concernés par ces exigences nouvelles.**

Deuxièmement, l'amendement complète la notion de données d'une sensibilité particulière, afin de l'adapter aux compétences des administrations publiques locales.

En plus des catégories déjà consacrées par la doctrine « *cloud* au centre » et l'article 31 de la loi « Sren », seraient également qualifiées de données sensibles « *les données nécessaires à la mise en œuvre des compétences essentielles des collectivités territoriales, notamment la prévention des risques de toute nature, la gestion des crises, le maintien de l'ordre public et la protection de la santé et de la vie des personnes* ».

Troisièmement, l'amendement encadre la clause dérogatoire qui avait été introduite par le Sénat.

En effet, si la possibilité de déroger à ces obligations nouvelles paraît pertinente pour permettre une transition harmonieuse vers des infrastructures d'informatique en nuage sécurisées, il est ressorti de l'ensemble des auditions conduites par votre Rapporteur que la rédaction adoptée par le Sénat était trop vague. Elle risquait de réduire significativement la portée du dispositif en ouvrant largement la possibilité de se soustraire aux exigences posées par le texte.

Afin d'éviter cet écueil, l'amendement propose que la décision de déroger à ces obligations nouvelles, prise par l'administration locale concernée, soit motivée et rendue publique, et que les conditions et modalités dans lesquelles les dérogations peuvent être décidées soient précisées par décret en Conseil d'État, par analogie au cadre prévu par l'article 31 de la loi « Sren ».

Surtout, la dérogation serait encadrée dans le temps : celle-ci ne pourrait dépasser dix-huit mois. Un tel mécanisme paraît plus pertinent qu'une entrée en vigueur différée, car il incite et contraint l'administration locale concernée à planifier la migration de ses données sensibles, tout en lui apportant la souplesse nécessaire à cette opération.

Enfin, l'amendement sécurise la possibilité pour l'administration locale concernée de résilier les contrats en cours, dans le cas où le prestataire auprès duquel elle héberge déjà ses données ne présenterait pas les garanties de sécurité exigées.

*

* *

COMPTE RENDU DES DÉBATS

Lors de sa réunion du mercredi 25 février à 9 heures, la commission examine la proposition de loi, adoptée par le Sénat, relative à la sécurisation des marchés publics numériques (n° 2258) (M. Philippe Latombe, rapporteur).

Lien vidéo : https://assnat.fr/wOGuMs

Mme Agnès Firmin Le Bodo, présidente. Cette proposition de loi, présentée par le groupe Démocrates dans le cadre de sa journée de niche parlementaire, a été déposée par le sénateur Dany Wattebled le 7 octobre 2025 et adoptée par le Sénat le 17 décembre.

M. Philippe Latombe, rapporteur. Je souhaiterais d'abord présenter la démarche que nous avons suivie avec le Sénat sur ce sujet. À l'issue des travaux de la commission d'enquête qu'ils ont consacrée à la commande publique, les sénateurs ont relevé plusieurs éléments qui mériteraient de faire l'objet de modifications législatives, parmi lesquels figure l'utilisation du *cloud* par les collectivités. Dans un monde où l'extraterritorialité du droit – notamment américain – et la captation économique de la donnée sont devenues la règle, la maîtrise de nos données et de celles de nos concitoyens est également un enjeu capital. Ce constat nous avait conduits à adopter de façon consensuelle la loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, dite Sren – y compris, pour certaines de ses dispositions, contre l'avis du Gouvernement et des administrations.

Les sénateurs souhaitent étendre l'article 31 de la loi Sren aux collectivités : c'est l'objet de la proposition de loi. Si l'idée est bonne, elle nécessite une rédaction suffisamment fine pour respecter nos obligations conventionnelles et constitutionnelles. Le principe de libre administration des collectivités territoriales notamment nous interdit d'imposer à ces dernières les mêmes conditions qu'à l'État.

C'est dans cet esprit que les sénateurs ont adopté le texte à l'unanimité en première lecture et que le groupe Démocrates l'a repris dans le cadre de sa niche parlementaire. Notre méthode a consisté à mener les auditions les plus larges possible, malgré le délai assez court dont nous avons disposé, puis à identifier les points de fragilité du texte – les types de collectivités et de données concernés – et à dégager les points d'accord entre l'ensemble des parties prenantes, pour proposer à la commission l'écriture la plus consensuelle possible.

Nous avons ainsi auditionné des représentants des collectivités, mais aussi des groupements d'achat nationaux comme locaux, des fournisseurs de suites collaboratives – notamment les acteurs français et le comité stratégique de filière – et des fournisseurs d'informatique en nuage, qu'il s'agisse d'entreprises

françaises, des Gafam ou de sociétés *ad hoc* comme Bleu ou S3NS. Plusieurs constats en ressortent.

D'abord, le délai de publication du décret d'application de l'article 31 de la loi Sren – deux ans – est déraisonnable. Cette lenteur ne se justifie ni par l'instabilité gouvernementale des deux dernières années, ni par la nécessité d'obtenir un avis de la Commission européenne. La plupart des acteurs ont demandé que le décret paraisse le plus vite possible. La Commission européenne en a été saisie et n'a pas émis d'observations ; le texte est désormais soumis au Conseil d'État et le ministre de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique a annoncé au Sénat qu'il serait publié d'ici à la fin du mois d'avril.

Ensuite, nous devons retenir une rédaction simple et efficace. Une écriture proche de l'article 31 de la loi Sren applicable à l'État, et étendue aux collectivités, est une bonne idée. Il faut par ailleurs que les obligations de sécurité prévues par la proposition de loi soient cohérentes par rapport à celles imposées dans le cadre de la directive NIS 2 relative à la sécurité des réseaux et des systèmes d'information. Bien évidemment, le texte devra également être conforme au cadre conventionnel et constitutionnel pour prévenir les recours, notamment ceux des Gafam, qui pourraient estimer qu'il leur porte un préjudice économique.

C'est pour cette raison que j'ai déposé un amendement de réécriture de l'article unique. Son adoption ferait tomber tous les autres, ce dont je suis désolé, car mon objectif n'est nullement d'esquiver le débat. J'ai d'ailleurs tenu à partager cette proposition de rédaction avec vous le plus rapidement et le plus largement possible, afin que nous puissions travailler dans un esprit d'ouverture. Quatre points méritent d'être précisés concernant cet amendement.

Premièrement, s'agissant du champ des communes auxquelles la proposition de loi sera applicable, je propose de retenir le même seuil que le texte visant à transposer la directive NIS 2, à savoir 30 000 habitants, conformément à la demande unanimement formulée dans le cadre des auditions et à la volonté initiale du Sénat : la consolidation des deux textes offrira une cohérence législative bienvenue. Les obligations prévues par la proposition de loi s'appliqueraient ainsi aux grandes communes et aux grands établissements publics de coopération intercommunale à fiscalité propre de taille significative, qui rassemblent un peu plus de 80 % de la population, étant entendu que les collectivités non concernées pourront s'y conformer si elles le souhaitent. L'extension aux communes de moins de 30 000 habitants pourra aussi être envisagée dans un deuxième temps, en fonction du bilan de l'application des deux premières lois – nous y reviendrons au moment d'examiner la demande de rapport déposée par M. Coulomme.

Deuxièmement, l'objectif est d'appliquer la loi Sren aux collectivités, donc de faire en sorte que les critères de sécurité et de protection s'appliquent aux seules données sensibles, comme c'est le cas pour l'État. Cette rédaction est conforme à la demande de la Commission européenne.

Troisièmement, eu égard au principe de libre administration des collectivités, nous prévoyons la possibilité pour ces dernières – y compris pour les syndicats et les conseils d'administration des établissements publics – de déroger à leurs obligations dans des conditions très strictes, c'est-à-dire pendant dix-huit mois au maximum et par une décision publique et motivée.

Quatrièmement, nous rappelons que les collectivités pourront résilier les contrats déjà conclus avec des fournisseurs qui ne respecteraient pas le nouveau cadre.

Nous nous appliquerons ainsi une forme de sobriété législative. Le fait de nous appuyer sur la loi Sren, déjà approuvée par la Commission européenne, écarte tout risque de d'inconventionnalité. Nous souhaitons aussi nous montrer pragmatiques en retenant le même seuil que celui qui s'imposera aux collectivités en application de la directive NIS 2 lorsque le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité aura été adopté, c'est-à-dire avant l'été. Les collectivités seront libres du chemin à adopter pour s'y conformer, même si le cap est tracé et similaire à celui que nous avions fixé pour l'État.

La future loi aura vocation à s'appliquer dès sa promulgation. Même si nous modifions le texte adopté par les sénateurs, ces derniers, ainsi que le Gouvernement, se sont engagés à inscrire rapidement le texte à l'ordre du jour, en vue d'une adoption en seconde lecture par la Chambre haute d'ici à la fin du mois d'avril. La rédaction envisagée semble recueillir l'approbation de l'auteur et de la rapporteure de la proposition de loi au Sénat, ainsi que du Gouvernement, ce qui devrait permettre d'avancer le plus rapidement possible.

Enfin, pour en revenir au rapport qui sera demandé par amendement, nous avons proposé que celui-ci traite également de l'application de la directive NIS 2 et qu'il soit rédigé par les sénateurs – ce que ces derniers ont accepté –, ce qui permettra d'en disposer beaucoup plus rapidement que si le Gouvernement devait nous le fournir.

Mme Agnès Firmin Le Bodo, présidente. Nous en venons aux interventions des orateurs des groupes.

Mme Monique Griseti (RN). Le texte dont nous sommes saisis vise à soumettre les principales collectivités territoriales aux mêmes exigences que l'État en matière de sécurisation des données, dans l'hypothèse où elles recourraient à des services informatiques en nuage dans le cadre de leurs activités administratives.

Nos données sont une mine d'or pour des sociétés ou des États qui peuvent les utiliser pour servir leurs intérêts ou nuire aux nôtres. La dématérialisation croissante des services publics et des démarches administratives conduit nos concitoyens à confier leurs données personnelles à diverses entités qui doivent les stocker, l'informatique en nuage étant, en la matière, la solution la plus pratique.

Cependant, les services publics ne sont pas des entreprises d'informatique et ont recours à des prestataires privés. Des garanties doivent donc être apportées pour protéger ces données, ceux à qui elles appartiennent et notre propre sécurité.

La loi Sren transposant la réglementation européenne sur les services numériques a imposé la sécurisation des marchés publics numériques, mais uniquement pour l'État. La proposition de loi adoptée par le Sénat permettrait donc de compléter la législation, en étendant l'obligation de protection des données d'une particulière sensibilité aux collectivités territoriales qui sont, au quotidien, amenées à gérer les données personnelles des administrés, mais aussi des données nécessaires à la sauvegarde de la sécurité nationale, à la protection de la santé et de la vie des personnes ou au maintien de l'ordre public.

Il est regrettable que ce devoir de vigilance vis-à-vis des opérateurs du *cloud* ne s'impose qu'aux 300 communes de plus de 30 000 habitants, ce qui exposera un trop grand nombre de nos concitoyens à un risque de fuite de leurs données personnelles. Le groupe Rassemblement national soutiendra néanmoins cette proposition de loi, tout en espérant que les débats permettront de supprimer ou d'abaisser ce seuil afin que davantage de communes soient concernées et que nos données soient protégées.

M. Paul Midy (EPR). Étant évidemment favorables à la sécurisation des données de nos concitoyens et au renforcement de notre souveraineté en la matière, nous voterons pour ce texte, tout en restant très attentifs à ce qu'il soit applicable et n'induise pas de lourdeurs supplémentaires : il ne s'agirait pas que des communes de 100 ou 1 000 habitants soient contraintes de se doter d'outils complexes et coûteux. Si nous voulons embarquer le maximum de collectivités, il faudra trouver le bon équilibre entre protection des données, souveraineté et vie réelle.

M. Jean-François Coulomme (LFI-NFP). Cette proposition de loi s'inscrit dans le contexte d'une dépendance croissante des acteurs publics aux services de *cloud*, dans un marché dominé par quelques grands groupes extra-européens. Près de 70 % des parts de marché du *cloud* en Europe sont captées par trois entreprises américaines, tandis que la part des fournisseurs européens a fortement diminué au cours des dernières années. Cette situation, loin d'être anodine, soulève une question centrale : quel est notre degré de souveraineté numérique ?

De nombreuses législations étrangères – aux États-Unis, en Chine ou en Inde – comportent des dispositions à portée extraterritoriale permettant aux États concernés d'obtenir les données détenues par des entreprises soumises à leur droit, y compris lorsque lesdites données sont collectées ou stockées à l'étranger. Des données publiques françaises peuvent ainsi être exposées à des demandes d'autorités étrangères.

Face à cela, l'objectif de la proposition de loi est clair : renforcer la protection des données numériques stockées dans les services d'hébergement en nuage utilisés par les acheteurs publics. Nous partageons pleinement ce but.

Dans sa version initiale, le texte prévoyait une obligation large, puisqu'il imposait aux acheteurs publics de s'assurer qu'aucune législation extraterritoriale imposant des transferts de données ne s'applique et de veiller à ce que toutes les données publiques qu'ils détiennent soient hébergées sur le territoire de l'Union européenne. Malheureusement, l'examen en commission au Sénat a largement réduit son ambition : seules les données sensibles doivent désormais être protégées, et non plus les données publiques ; le périmètre des acheteurs publics concernés a été réduit aux seules communes de plus de 30 000 habitants ; des dérogations aux contours très larges ont été prévues.

De ce fait, le texte nous semble passer à côté de plusieurs sujets. D'abord, alors que le recours à des solutions souveraines nécessitera des moyens financiers et humains, rien n'est prévu pour les augmenter. Ensuite, il n'est nullement fait mention de l'usage obligatoire de solutions techniques réellement susceptibles de préserver la souveraineté numérique, comme les logiciels libres et les services de *cloud* réversibles, qui permettraient de lutter contre le pouvoir monopolistique des Gafam et surtout d'aider les utilisateurs à préserver leur autonomie technologique, puisqu'ils pourraient récupérer les données stockées à tout moment et les transférer vers un autre service.

L'amendement de réécriture déposé par notre rapporteur nous conduit à atténuer certaines de ces critiques. La nouvelle rédaction prévoirait ainsi un léger élargissement de l'obligation, puisque les communautés de communes de plus de 30 000 habitants y seraient assujetties. Elle modifierait également le régime des dérogations : alors que la version du Sénat permettait à une collectivité territoriale de s'exonérer de la loi au motif de difficultés techniques ou d'un risque de surcoût important, la dérogation ne serait désormais possible que dans des conditions et selon des critères définis par décret en Conseil d'État, et elle ne pourrait excéder dix-huit mois.

Toutefois, un élément central demeure absent du texte : la nécessité de protéger les données stockées contre les effets extraterritoriaux liés à l'utilisation de solutions développées hors de l'Union européenne et soumises à des législations étrangères. Or c'est précisément le cœur du problème identifié dans l'exposé des motifs et au cours des travaux préparatoires : l'accès à nos données publiques par des autorités étrangères via l'application de législations extraterritoriales. Par ailleurs, à l'heure où de lourdes contraintes budgétaires pèsent sur les collectivités territoriales, la question des moyens financiers et humains nécessaires pour les accompagner dans le respect de cette nouvelle obligation reste posée.

Si nous partageons l'objectif de la proposition de loi et reconnaissons les avancées introduites par la réécriture proposée par le rapporteur, nous considérons donc que le dispositif reste insuffisant au vu des enjeux identifiés.

M. Sacha Houlié (SOC). Il faut d'abord saluer l'initiative parlementaire qui a permis d'aboutir à ce texte, issu des travaux de la commission d'enquête sénatoriale sur les coûts et les modalités effectifs de la commande publique. Cette dernière, dans sa recommandation n° 24, préconisait de *« rendre obligatoire 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 *»*. Au fond, cette proposition de loi est même en quelque sorte la traduction de tous nos travaux, y compris de ceux que j'avais conduits en tant que président de la délégation parlementaire au renseignement, lorsque j'avais appelé l'État et ses démembrements – les collectivités, au sens du droit international – à se montrer moins naïfs vis-à-vis des ingérences étrangères ou des tentatives d'extraterritorialité.

Celles-ci peuvent d'ailleurs être le fait de nos alliés aussi bien que de nos compétiteurs. La commission d'enquête sénatoriale avait ainsi notamment auditionné le directeur des affaires publiques et juridiques de Microsoft France, qui n'avait pas été en mesure d'exclure toute fuite de données vers les plateformes ou le gouvernement américains dans le cadre de marchés français. Je songe notamment au *Health Data Hub* pour les données de santé, au marché public passé par l'éducation nationale ou encore au contrat conclu entre la direction générale de la sécurité intérieure (DGSI) et Palantir – sans parler de celui passé par l'Union des groupements d'achats publics, qui concerne directement les collectivités.

Derrière son apparence technique, la proposition de loi que vous présentez en vue d'étendre l'obligation de sécurisation des données aux marchés publics locaux est donc essentielle. La commande publique en France représente 400 milliards d'euros – 14 % du PIB national – et les collectivités territoriales y occupent une très grande place. Or, comme cela a été souligné, le recul des plateformes européennes sur le marché est indéniable.

Vous privilégiez dans votre réécriture une extension de l'article 31 de la loi Sren. Elle serait effectivement préférable au dispositif sénatorial, puisque seraient ainsi protégées les données d'une sensibilité particulière dont la violation est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé et à la vie des personnes ou à la protection de la propriété intellectuelle. À ce stade, je tiens à faire valoir deux éléments.

D'abord, comme vous l'avez relevé, le Gouvernement n'a pas respecté les six mois impartis pour publier le décret d'application de l'article 31. J'aimerais croire la promesse du ministre, mais elle n'engage que ceux qui y croient et je crains que ce décret ne soit toujours pas publié en mai prochain, deux ans après la promulgation de la loi. Je le regrette profondément, car cela signifie que les

marchés conclus dans le cadre de la commande publique de l'État resteront privés de protection.

Ensuite, l'article 31 prévoit une obligation de « veiller » à ce que les services informatiques en nuage se conforment à des critères de sécurité. Or veiller, ça n'est pas garantir : il y a une différence entre l'obligation de moyens prévue à l'article 31 et l'obligation de résultat que le groupe Socialistes et apparentés avait réclamée lors de l'examen de la loi Sren. C'est le sens de l'amendement que j'ai déposé après l'article 1er.

Pour le reste, je salue la réécriture proposée, qui élargit le champ des personnes visées par le futur article 31-1, restreint les motifs de dérogation au fait d'être déjà engagé dans un marché et limite la durée de ladite dérogation à dix-huit mois.

Au fond, ce texte s'inscrit dans la stratégie numérique nationale, qui fait de la souveraineté numérique un enjeu très important. Il contribue à la réponse qu'on est en droit d'attendre de l'État pour protéger nos concitoyens et les collectivités qui passent des marchés publics. Nous soutiendrons donc naturellement cette proposition de loi.

Mme Lisa Belluco (EcoS). La souveraineté numérique des administrations et des collectivités n'est plus un sujet technique réservé aux spécialistes ou aux directeurs de services informatiques : c'est un enjeu stratégique, démocratique et politique. Chacun en a désormais conscience.

Les institutions publiques tout comme nos entreprises dépendent encore massivement de solutions proposées par les Gafam, comme en témoignent le recours à Palantir par la DGSI ou le fiasco du *Health Data Hub* avec Microsoft. Au total, près de 265 milliards d'euros de dépenses numériques européennes bénéficient à ces acteurs, soit 80 % du total des dépenses liées aux logiciels et services de *cloud* à usage professionnel en Europe.

Un des principaux problèmes posés par cette situation tient à l'extraterritorialité du droit, en vertu de laquelle les données de nombreuses organisations sont légalement accessibles à des autorités étrangères : la seule localisation géographique des serveurs sur le sol européen ne constitue plus un rempart juridique suffisant. Ces mécanismes juridiques ont parfois été utilisés à des fins économiques et géopolitiques, et ont donné lieu à d'importantes sanctions financières contre des entreprises européennes.

Il est donc légitime que l'État et les collectivités cherchent à s'en protéger. Plusieurs avancées législatives récentes, notamment la loi Sren, vont dans ce sens en renforçant les exigences d'indépendance et de sécurité, même si l'on peut effectivement regretter la lenteur avec laquelle leurs décrets d'application sont publiés. Dans ce contexte, nous saluons la présente proposition de loi et soutiendrons la réécriture générale proposée par le rapporteur.

Mais une question se pose : quelle souveraineté voulons-nous ? Une souveraineté de substitution, consistant simplement à remplacer des géants américains par des géants européens, ou une souveraineté de transformation qui repense en profondeur notre modèle numérique ?

La droite française et européenne reste enfermée dans une logique de compétition industrielle : il s'agit de créer des champions européens pour rivaliser avec les géants américains et chinois, afin de participer à la compétition mondiale et de renforcer les positions d'oligopoles. Cette approche peut sembler pragmatique, mais elle comporte un risque majeur : reproduire les mêmes dépendances structurelles, les mêmes vulnérabilités systémiques et les mêmes logiques de concentration du pouvoir technologique. Or la souveraineté d'aujourd'hui ne doit pas se construire au détriment de la résilience de demain, car les incertitudes sont nombreuses : tensions géopolitiques croissantes, ruptures d'approvisionnement, crise énergétique, impacts du changement climatique, voire effondrements systémiques partiels.

Dans cette optique, la démarche *low-tech* peut apporter quelques réponses. Contrairement à une idée reçue, elle ne consiste pas à rejeter le numérique, mais à l'utiliser en partant du juste besoin. Simplifier les systèmes, privilégier la maintenabilité, réduire la dépendance à des infrastructures complexes, favoriser l'interopérabilité et l'*open source* : tous ces leviers renforcent la résilience des organisations face aux chocs. Au fond, la véritable souveraineté numérique implique un retour aux principes fondateurs d'internet : décentralisation, coopération, interopérabilité, communs numériques et *open source*.

Une question doit nous guider : que restera-t-il de nos systèmes numériques lorsque l'énergie, les matières premières ou les infrastructures deviendront rares ou intermittentes ? Surtout, comment préparer des réponses crédibles et désirables ?

M. Nicolas Turquois (Dem). Sous ses abords très techniques, ce texte soulève une question majeure pour l'action publique. Au-delà des serveurs, des prestataires ou du code de la commande publique, il est question en fait de la sécurité numérique de nos territoires, de la protection de l'intimité de nos concitoyens et, *in fine*, de la souveraineté de la France.

La loi Sren du 21 mai 2024 constitue un acte fondateur : l'État a enfin exigé des garanties de cybersécurité de très haut niveau, comme la qualification SecNumCloud pour héberger ses données les plus sensibles. C'était indispensable, mais ce n'était qu'une première étape. En effet, la République ne s'incarne pas que dans l'État central : elle vit aussi dans les territoires, et les collectivités locales sont en première ligne. Par le jeu de la décentralisation, elles brassent, stockent et gèrent au quotidien des données d'une sensibilité absolue – données d'état civil, dossiers d'aide sociale, prévention des risques, plans de sauvegarde. Or l'actualité montre chaque semaine que les hôpitaux, les mairies, les départements et les

régions sont devenus les cibles privilégiées et régulières de cyberattaques dévastatrices.

Face à cette menace devenue systémique, la naïveté n'est plus permise. Continuer à confier ces données critiques à des prestataires d'informatique en nuage qui ne présentent pas de garanties d'immunité aux législations extraterritoriales, c'est accepter de placer une épée de Damoclès au-dessus des collectivités. La donnée publique est le nouveau territoire stratégique : la laisser à la merci des lois étrangères, même celles de pays alliés, c'est renoncer à notre indépendance.

Il est donc urgent d'étendre le bouclier protecteur de la loi aux grandes collectivités. Tel est l'objectif de cette proposition de loi ; nous saluons cette initiative du Sénat. Toutefois, pour qu'un bouclier soit véritablement efficace, il ne doit comporter aucune faille. Le rapporteur vient de présenter les détails de sa proposition de réécriture avec une grande clarté. Je me contenterai donc d'en souligner la justesse politique.

D'abord, elle colmatera des brèches dangereuses en incluant explicitement les données des services départementaux d'incendie et de secours (Sdis) et celles des centres de gestion de la fonction publique territoriale. Comment pouvions-nous imaginer protéger les données d'une région en laissant celles des pompiers vulnérables ?

Ensuite, en remplaçant la dérogation prévue par le Sénat par une période de transition stricte et limitée à dix-huit mois, elle permet de trouver un juste point d'équilibre : nous ne prenons pas les élus locaux en traître – ils auront le temps d'adapter les contrats en cours – mais nous fixons un cap ferme dont ils ne pourront plus dévier. Enfin, nous leur donnons une véritable arme juridique pour résilier les contrats conclus avec des prestataires qui refuseraient de se mettre aux normes.

La souveraineté numérique n'est pas qu'un concept réservé aux sommets internationaux : elle est une pratique quotidienne et s'exerce à travers les choix des maires et des présidents de région en matière de commande publique. Avec ce texte amendé, nous donnerons aux collectivités les outils pour protéger efficacement leurs données ainsi que celles de nos concitoyens.

Le groupe Démocrates votera avec conviction pour cette proposition de loi.

M. Jean Moulliere (HOR). Les travaux de la commission d'enquête sur les coûts et les modalités de la commande publique, conduits en 2025 sous l'égide du sénateur Dany Wattebled, ont rappelé un constat connu : certains pays peuvent, grâce à une législation à portée extraterritoriale, intercepter des données hébergées en cloud par les acheteurs publics. Cette situation constitue un risque majeur pour la souveraineté de notre pays.

Elle n'a rien de nouveau : depuis le *Foreign Intelligence Surveillance Act* de 1978, et plus encore depuis le *Cloud Act* de 2018, les autorités américaines peuvent contraindre un fournisseur de services informatiques à leur dévoiler toute communication ou information dont il dispose concernant un de ses clients. L'Inde et la Chine se sont dotées de dispositions similaires.

Ce qui a changé, c'est notre perception de cette situation. Depuis la réélection du président Donald Trump aux États-Unis, de plus en plus de pays assument de faire fi du multilatéralisme pour ne faire valoir que leurs intérêts nationaux, y compris aux dépens de leurs alliés. Dans ce contexte, chaque outil de la puissance publique devient un nouvel instrument de défense ou de coercition.

Les marchés publics ne font pas exception. La commande publique est un instrument de souveraineté majeur. Elle représente 400 milliards d'euros par an, soit 14 % du PIB, et 80 % des marchés sont passés par les collectivités. Parce qu'elle fournit les communes, les préfectures, les écoles ou encore les tribunaux en biens et services indispensables, la commande publique est un outil crucial pour la puissance publique. Elle doit donc contribuer à la préservation, et même au renforcement, de notre souveraineté.

Si beaucoup a été fait à cet égard depuis 2021, en particulier avec la loi Sren, acte fondateur de la souveraineté numérique qui impose aux administrations et aux opérateurs de l'État d'héberger leurs données sensibles dans un cloud souverain, la réalité n'est pas à la hauteur des objectifs. Les fournisseurs de prestations de *cloud* souverain ne représentent par exemple que 63 % des commandes des administrations publiques.

Cette proposition de loi vise à imposer, dans les marchés publics de cloud, des conditions excluant l'application des mesures extraterritoriales imposant la transmission de données à l'étranger, et à garantir l'hébergement de ces dernières au sein de l'Union européenne. Elle étend cette exigence, actuellement limitée aux données les plus sensibles de l'État, à l'ensemble des données publiques détenues par les acheteurs publics, y compris par les collectivités locales. Si cette obligation est une première étape essentielle pour sécuriser les marchés publics numériques, elle ne devra pas rigidifier le droit de la commande publique. Le texte présente à ce titre les garanties nécessaires, puisqu'il exclut les communes de moins de 30 000 habitants et prévoit un mécanisme dérogatoire en cas de difficulté.

Nous voterons donc en faveur de cette proposition de loi pour une France plus souveraine.

Mme Elsa Faucillon (GDR). Cette proposition de loi s'inscrit dans le prolongement des travaux de la commission d'enquête du Sénat sur la commande publique. Celle-ci, qui représente 400 milliards d'euros par an, soit 14 % du PIB, constitue un levier économique majeur ainsi qu'un outil stratégique. Or les travaux des sénateurs ont mis en lumière un angle mort préoccupant concernant la

protection des données publiques dans le cadre de prestations numériques, notamment de leur hébergement et de leur traitement en cloud.

Les services numériques représentent une part croissante des marchés publics. Dans ce domaine, les trois principaux fournisseurs américains – Amazon Web Services, Microsoft Azure et Google Cloud – concentrent environ 70 % du marché européen des infrastructures. Les administrations françaises utilisent donc massivement leurs services. Le problème n'est pas seulement économique, mais aussi juridique et stratégique : ces entreprises sont soumises à des législations à portée extraterritoriale, en particulier au *Foreign Intelligence Surveillance Act* et au *Cloud Act* américains, qui permettent aux autorités des États-Unis d'exiger que leur soient communiquées des données stockées hors du territoire américain. D'autres puissances disposent de dispositifs comparables.

Lors de son audition par la commission d'enquête du Sénat, un dirigeant de Microsoft France a reconnu ne pas pouvoir garantir que des données de citoyens français ne seraient jamais transmises à une autorité étrangère sans l'accord des autorités françaises – une réponse qui dit tout de la vulnérabilité actuelle. Ce débat n'a donc rien de théorique : les données publiques hébergées auprès de prestataires soumis à de telles législations peuvent, en toute légalité, faire l'objet de transferts sur lesquels nous n'avons aucune maîtrise. Les sénateurs y voient un risque juridique majeur, mais aussi un risque stratégique.

La version initiale du texte tirait les conséquences de ce constat en imposant des garanties fortes pour les marchés comportant des prestations de *cloud*. Les modifications adoptées au Sénat ont réduit la portée du dispositif – limitation des obligations aux seules données dites sensibles, exclusion de certaines collectivités, mécanisme de dérogation en cas de difficultés techniques ou financières –, mais je suis sûr que nos débats permettront de renouer avec l'ambition originelle.

Dans un contexte géopolitique marqué par la multiplication des ingérences et des tensions internationales, la protection des données publiques ne peut pas être partielle. La dépendance fonctionnelle de nos administrations à des environnements technologiques soumis à des législations étrangères est devenue la norme. La commande publique représente des centaines de milliards d'euros. Elle peut et doit être un instrument d'orientation stratégique. Si nous ne l'utilisons pas pour exiger des garanties effectives contre les ingérences juridiques étrangères et pour soutenir l'émergence d'offres de *cloud* françaises et européennes crédibles, nous pérenniserons une situation de dépendance.

Nous sommes bien conscients qu'une exclusion immédiate et générale des grands fournisseurs internationaux soulèverait des difficultés opérationnelles. La sécurisation de la commande publique numérique doit s'inscrire dans un développement progressif de solutions alternatives pleinement souveraines. Mais un encadrement à la marge ne suffira pas : si nous voulons faire de la commande

publique un levier de souveraineté numérique, nous devons en assumer pleinement l'ambition.

M. Philippe Gosselin (DR). Le sujet peut paraître anecdotique, mais il ne l'est pas du tout. Le contexte nous rappelle la nécessité d'assurer notre souveraineté sous toutes ses formes, y compris en matière numérique. Le fait que nous examinions un tel texte aujourd'hui n'est d'ailleurs pas un hasard. L'Assemblée nationale vient elle-même de constituer une commission d'enquête sur les vulnérabilités systémiques de la France dans le secteur du numérique, présidée par M. le rapporteur.

Nous sommes exposés à des influences diverses et les donneurs d'ordres ne sont pas toujours en mesure de protéger nos données ni de faire appel à des sociétés qui assureraient cette protection dans les meilleures conditions. Cette difficulté ne tient pas seulement au manque d'entreprises à même de répondre à nos attentes, mais aussi à l'existence d'un droit exorbitant qui permet à l'État américain, sous certaines conditions parfois bien lâches, d'accéder à des données considérables.

Il est donc primordial d'appeler les collectivités, les départements, les régions, les intercommunalités et les agglomérations de plus de 30 000 habitants à se préoccuper de la protection de leurs données – pas simplement celles qui concernent leurs finances ou leurs marchés publics, mais aussi celles qui ont trait à la santé, à la recherche ou encore à l'enseignement supérieur. Comme la République, la souveraineté est une et indivisible.

Assurément, le texte qui nous est proposé, sans être l'alpha et l'oméga de la politique à conduire en la matière, donne une orientation ferme, avec des délais d'application et en tenant compte de la situation des collectivités ayant déjà engagé des travaux. Il signifie clairement que chacun doit se saisir de cette question : l'État, les collectivités, les établissements publics, et même les entreprises privées de secteurs sensibles comme la défense ou la stratégie économique, même s'il est juridiquement plus difficile de les y contraindre.

Le groupe Droite républicaine votera évidemment pour ce texte, qui ne doit pas être regardé comme une fin en soi, mais comme une pierre supplémentaire à un édifice qui reste à consolider et à parfaire – car la souveraineté numérique est un élément de la souveraineté, à laquelle nous sommes particulièrement attachés.

M. Philippe Latombe, rapporteur. Madame Griseti, le seuil de 30 000 habitants est celui qui s'imposera dans le cadre de la directive NIS 2. Comme il s'appliquera aussi aux communautés de communes de plus de 30 000 habitants, aux communautés d'agglomération, aux communautés urbaines et aux métropoles, il permettra de couvrir l'essentiel de la population française. Seules quelques petites communautés de communes, dans des zones rurales, ne seront pas

couvertes. Elles pourront néanmoins choisir d'opter pour de telles solutions de façon volontaire, en espérant que l'effet d'entraînement les y incitera.

Je confirme d'ailleurs à M. Midy que si nous avons retenu ce seuil de 30 000 habitants, c'est pour permettre aux collectivités d'appliquer de façon homogène les politiques qui s'imposent à elles en matière de cybersécurité et d'hébergement des données sensibles.

Monsieur Coulomme, les services en nuage comprennent non seulement l'hébergement, mais aussi les logiciels dits en Saas (logiciels en tant que services), qui incluent les suites collaboratives. Le texte ne porte que sur l'hébergement et l'utilisation de logiciels en Saas privés. Les collectivités qui souhaiteraient faire de l'hébergement public ne sont pas concernées. Nous avons essayé de définir les données sensibles, pour aller plus loin que ne l'a fait le Sénat. La définition que nous proposons, bien que ramassée, recouvre les données les plus importantes : nous y avons intégré l'ordre public, la santé et la vie de nos concitoyens. Cette approche nous permet d'être en conformité avec les demandes de la Commission européenne. Nous étendons l'application de l'article 31 de la loi Sren, qui nous prémunit contre l'application de règles extraterritoriales, afin de répondre aux interrogations qui se sont fait jour.

Monsieur Houlié, nous nous inscrivons en effet dans la droite ligne de la réflexion qui avait été engagée et que vous aviez alimentée par votre rapport. Ce sont des questions importantes, qui recueillent un large accord, comme le montre le fait que le Sénat ait adopté ce texte à l'unanimité. De même, à l'Assemblée comme au Sénat, puis en commission mixte paritaire, nous nous étions prononcés très majoritairement en faveur de l'article 31. Mme Chatelain a, pour sa part, lancé une commission d'enquête sur le sujet. Cela devient une question transpartisane, sur laquelle nous arrivons à avancer.

Vous regrettez que, selon l'article 31, l'administration de l'État et ses opérateurs doivent « veiller » à ce que le service d'informatique en nuage applique les critères de sécurité et de protection des données. Mais vous voyez que l'emploi de ce terme n'empêche pas les réversibilités, puisqu'un appel d'offres souverain a été lancé il y a trois semaines pour le *Health Data Hub*, et que l'hébergement des données de l'État connaît des évolutions.

La proposition de loi n'a pas pour objet de rouvrir le débat sur l'article 31, dont la rédaction avait fait l'objet d'une notification à la Commission européenne et d'un aller-retour un peu douloureux pour le Gouvernement de l'époque. Nous étions parvenus à une rédaction efficace – comme l'illustre l'exemple du *Health Data Hub* – et conforme à nos obligations conventionnelles. Nous aurons l'occasion de discuter de votre amendement, qui trouverait peut-être davantage sa place dans un autre véhicule législatif. Je rappelle que la Commission et le Parlement européens mènent actuellement des travaux concernant la modification des directives, qui pourraient donner l'occasion de modifier la loi Sren.

Madame Belluco, l'un des objectifs de la proposition de loi est de nous conduire à repenser notre modèle. Il s'agit de ne pas imposer aux collectivités leur mode de fonctionnement. Quelques collectivités pionnières réfléchissent à l'utilisation de la donnée – je pense à la Côte-d'Or, à Lyon ou encore aux Pays de la Loire, où la région a participé à la création d'un opérateur, Gigalis, qui met des services numériques à la disposition des collectivités qui le souhaitent. La proposition de loi offre aux collectivités un éventail de possibilités. Certaines voudront avoir des *data centers* à proximité, d'autres préféreront l'échelle régionale ou nationale. Nous leur offrons la possibilité de repenser leur modèle en fonction de leurs besoins, sans leur imposer une façon de faire.

Monsieur Turquois, certains systèmes d'information ne sont pas concernés par la proposition de loi car leurs données ne sont pas la propriété de la collectivité. Celles de l'état civil, par exemple, sont abritées par le réseau sécurisé du ministère de l'Intérieur. Le texte ne s'applique qu'aux données collectées et conservées par les collectivités : je pense par exemple aux données des centres communaux d'action sociale, qui présentent une sensibilité particulière dans la mesure où il s'agit de données financières qui ont partie liée à la santé et au handicap. D'autres systèmes ont été pensés avec l'État pour éviter ce genre de difficultés. Cela étant, vous avez raison de souligner que nos collectivités connaissent des fuites de données importantes. Le projet de loi sur la résilience des infrastructures critiques et la présente proposition de loi, conjugués, permettraient de couvrir l'intégralité du champ et d'accroître la protection de nos concitoyens.

Monsieur Moulliere, nous nous efforçons de conserver de la souplesse. Le texte assigne un objectif aux collectivités mais, conformément au principe de libre administration, ne leur dit pas comment elles doivent procéder. Les petites collectivités pourront, si elles le souhaitent, bénéficier de ses dispositions. Des solutions très souples d'utilisation du *cloud*, fondées sur le paiement à l'utilisation, offriront des solutions financières aux petites communes.

Madame Faucillon, nous avons étendu la définition des données sensibles concernées, en nous inspirant des dispositions de la loi Sren applicables à l'État, et en y intégrant les éléments nécessaires au fonctionnement des collectivités et à l'exercice de leurs compétences, tout en mentionnant les notions d'ordre public et de protection de la santé et de la vie des personnes. Cette approche permet de garantir la conventionnalité du dispositif : les collectivités souhaitaient en effet que nous aboutissions à la rédaction la plus précise possible pour éviter les recours, en particulier des Gafam.

Monsieur Gosselin, il ne s'agit pas, en effet, de la fin du processus. Ce texte constitue une brique supplémentaire, il n'a pas pour objet de tout révolutionner. Il dit aux collectivités qu'elles doivent prendre leur part de l'évolution en cours, tout en leur laissant le choix des moyens à employer. L'ensemble de la sphère publique doit se mettre en mouvement sur cette question. Les collectivités nous demandent que la directive NIS 2 et donc le projet de loi sur la résilience entrent en application le plus vite possible. Elles ont besoin de se

projeter. En effet, lorsque les élus municipaux prendront leurs fonctions, dans quelques semaines, ils devront définir des budgets en conformité avec ces textes.

Je prie donc instamment le Gouvernement d'inscrire le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité à l'ordre du jour dès que possible. De même, les décrets d'application des lois que nous votons doivent être pris dans les meilleurs délais. Le décret d'application de l'article 31 a été soumis à la Commission européenne, qui n'a pas formulé de remarques particulières, et est actuellement examiné par le Conseil d'État. Nous arrivons au terme du processus. Logiquement, comme l'a dit le ministre, le texte devrait entrer en vigueur d'ici à la fin avril.

Article unique (art. 31-1 [nouveau] de la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique)

Amendement CL13 de M. Philippe Latombe, sous-amendements CL15 et CL16 de Mme Monique Griseti

M. Philippe Latombe, rapporteur. Il s'agit de la réécriture globale que j'ai évoqué. Je n'ai pas souhaité diviser cet amendement en trois ou quatre dispositions distinctes, même si cela aurait pu favoriser le débat, car il forme un tout cohérent.

Dans une première partie, l'amendement vise à redéfinir le champ des collectivités concernées. La loi devait déjà s'appliquer aux régions, aux départements et aux communes de plus de 30 000 habitants. Nous y ajoutons leurs établissements publics administratifs, les centres de gestion de la fonction publique territoriale, les services départementaux d'incendie et de secours – qui détiennent eux aussi des données très sensibles –, les communautés de communes de plus de 30 000 habitants, ainsi que les communautés d'agglomération, les communautés urbaines et les métropoles.

Ensuite, la réécriture définit les données présentant une sensibilité particulière.

Enfin, l'amendement énonce les conditions de dérogation aux règles posées. La dérogation ne pourra dépasser dix-huit mois et devra résulter d'une délibération rendue publique et motivée, par parallélisme avec ce que nous avons imposé à l'État dans l'article 31 de la loi Sren. En effet, lorsqu'un ministère veut déroger à la loi, c'est le Premier ministre, sur avis du ministre concerné, qui peut accepter la dérogation, par une décision motivée et rendue publique et pour une durée maximale de dix-huit mois. Nous n'imposons donc rien de plus ni rien de moins aux collectivités qu'à l'État. Ce parallélisme des formes est facteur de simplicité.

Mme Monique Griseti (RN). Le sous-amendement CL15 vise à supprimer le seuil de 30 000 habitants à partir duquel les communes devront respecter la loi. Si les communes ayant une population inférieure peuvent

demander à bénéficier de ces règles protectrices, pourquoi ne pas étendre le texte à l'ensemble des communes ? Cela permettrait de protéger partout de la même manière les données d'une particulière sensibilité.

Le sous-amendement CL16 vise au moins à ramener le seuil à 10 000 habitants. En effet, certaines communes dont la population est comprise entre 10 000 et 30 000 habitants abritent des données sensibles, telles Oissel, en Normandie, qui accueille une école de police, Rognac, une ville de 11 000 habitants de ma région Provence-Alpes-Côte d'Azur, Chantilly et bien d'autres.

M. Philippe Latombe, rapporteur. Comme je l'ai dit, la fixation du seuil de 30 000 habitants s'explique par deux raisons. Premièrement, c'est le seuil qui avait été défini dans le projet de loi sur la résilience des infrastructures critiques ; nous aurions ainsi un parallélisme des formes qui faciliterait les choix d'architecture informatique.

Deuxièmement, au cours des auditions que nous avons menées, les collectivités ont été unanimes pour dire que le seuil de 30 000 habitants était adapté, en ce qu'il permettait de couvrir l'immense majorité de la population. Elles ont relevé que le petit nombre de communes appartenant à des communautés de communes de moins de 30 000 habitants auraient la possibilité de bénéficier de ces règles protectrices. En revanche, l'extension de l'obligation à l'ensemble des communes pourrait engendrer des surcoûts extraordinairement élevés, les systèmes d'information devant être modifiés substantiellement. Or les petites communes n'ont pas nécessairement la capacité budgétaire d'assumer les investissements nécessaires. C'est aussi pour cette raison que nous avons élargi l'application de la loi aux Sdis et aux centres de gestion afin d'étendre la protection des données sensibles et, partant, de la population. Demande de retrait ou avis défavorable.

*La commission **rejette** successivement les sous-amendements.*

*Elle **adopte** l'amendement.*

*En conséquence, l'article unique est **ainsi rédigé** et les amendements suivants **tombent**.*

Après l'article unique

Amendement CL12 de M. Sacha Houlié

M. Sacha Houlié (SOC). Cet amendement a pour objet de remplacer, à l'article 31 de la loi Sren, les mots « veillent à ce » par les mots « garantissent ». Cette précision n'a pas seulement une portée sémantique : il s'agit de passer d'une obligation de moyens à une obligation de résultat. Un pouvoir adjudicateur aurait ainsi la possibilité d'écarter, sur le fondement de cette disposition, un candidat à un marché de prestation de services de données en *cloud*.

M. Philippe Latombe, rapporteur. D'abord, la proposition de loi vise à étendre l'application de l'article 31, non à le modifier. Je considère votre amendement comme un amendement d'appel à l'égard du Gouvernement : c'est plutôt avec lui qu'il faudra en discuter.

En outre, si nous procédions à la modification que vous proposez, il faudrait à nouveau solliciter l'accord de la Commission européenne. Or celle-ci nous avait dit que le mot « garantissent », qui figurait dans la première version du projet de loi Sren, ne pouvait pas être employé. Cela ne nous empêche pas d'être très vigilants quant à l'obligation imposée par l'État à ses opérateurs, par exemple concernant le *Health Data Hub*, de rendre leur stockage souverain.

J'ajoute que la Commission européenne mène des travaux qui permettront, dans le cadre des textes sur la souveraineté européenne, de modifier l'article 31 sans s'exposer à un problème de conventionnalité. Ces pistes d'évolution pourraient vous donner satisfaction d'ici à la fin de l'année. Avis défavorable.

M. Sacha Houlié (SOC). Ayant entendu l'avis du rapporteur, je retire l'amendement mais le redéposerai en séance afin de connaître celui du Gouvernement.

L'amendement est ***retiré****.*

Amendement CL7 de M. Jean-François Coulomme

M. Jean-François Coulomme (LFI-NFP). Le projet de loi de finances pour 2026, imposé par 49.3, amputant de plus de 2 milliards d'euros le budget des collectivités territoriales, nous sommes légitimement en droit de nous demander où nous allons trouver l'argent nécessaire pour que nos collectivités se conforment aux bonnes idées de ce texte. En effet, les bonnes intentions ne sont pas suffisantes : encore faut-il avoir les moyens de les concrétiser. Aussi demandons-nous par cet amendement un rapport afin de connaître les moyens alloués aux collectivités pour se conformer à la loi.

Nous déposerons d'autres demandes de rapport en séance publique car des zones d'ombre demeurent concernant l'application de la loi. Par exemple, comment évaluera-t-on le bilan carbone des fournisseurs ? On sait que le *cloud* et les gros serveurs consomment des ressources énergétiques considérables. Par ailleurs, plusieurs services publics, jusqu'au ministère de l'intérieur, ont connu, au cours des derniers mois, des fuites massives de données, ce qui nous laisse perplexe quant aux performances techniques des systèmes auxquels nous confions les données des citoyens. Ceux-ci n'ont aucune envie de voir leurs données sensibles diffusées en France ou à l'étranger.

M. Philippe Latombe, rapporteur. S'agissant du dernier point, nos concitoyens s'interrogent effectivement sur la protection des données, y compris celles confiées à la sphère publique. La Commission nationale de l'informatique et des libertés a demandé que l'utilisation d'un numéro de certification multifacteurs

soit obligatoire en cas de recours à une base de données de grande ampleur. Or cela n'était pas le cas dans un certain nombre des fuites constatées : celles-ci étaient liées, dans la plupart des cas, à des attaques d'ingénierie sociale, à la récupération d'identifiants et de mots de passe sans authentification multifacteurs. Il faut sans doute développer une certaine hygiène numérique, mais cette préoccupation trouvera davantage sa place dans la réflexion autour de NIS 2 et de la cybersécurité.

S'agissant de votre amendement, je propose que ce soient les sénateurs qui établissent le rapport que vous demandez, dans le cadre du contrôle de l'application de la loi. Ils en ont en effet émis le souhait, et nous obtiendrions les résultats plus rapidement que si nous confiions ce travail au gouvernement. En outre, une analyse menée par la chambre issue des collectivités pourrait être plus objective. Par conséquent, demande de retrait ou avis défavorable, mais pas sur le fond.

La commission ***rejette*** *l'amendement.*

Elle ***adopte*** *l'ensemble de la proposition de loi* ***modifiée****.*

*En conséquence, la commission des Lois constitutionnelles, de la législation et de l'administration générale de la République vous demande d'***adopter*** *la proposition de loi, relative à la sécurisation des marchés publics numériques (n° 2258) dans le texte figurant dans le document annexé au présent rapport.*

PERSONNES ENTENDUES

Table ronde d'associations d'élus locaux

- **Régions de France**
  — Mme Constance Nebbula, vice-présidente de la région Pays de la Loire, en charge du numérique et de l'intelligence artificielle
- **Intercommunalités de France**
  — Mme Marlène Le Dieu de Ville, vice-présidente en charge du numérique
  — Mme Montaine Blonsard, responsable des relations avec le Parlement
  — M. Jules Podczaski, conseiller numérique

*

Table ronde d'acheteurs publics

- **Union des groupements d'achats publics (UGAP)**
  — M. Edward Jossa, président
- **Centrale d'achat du numérique et des télécoms (Canut)**
  — M. Vincent Deleau, directeur général
  — M. Christophe Lombard, président
  — M. Sébastien Déon, vice-président
  — M. Yannick Giquel, administrateur
- **Association pour l'achat dans les services publics (ASASP)**
  — M. Jean Pierre Gohon, administrateur

*

Table ronde d'acteurs de la filière du numérique

- **Comité stratégique de filière « Logiciels et solutions numériques de confiance »**
  — M. Michel Paulin, Président
- **Jalios**
  — M. Vincent Bouthors, président

- **Linagora**
  — M. Alexandre Zapolsky, président
- **Jamespot**
  — M. Alain Garnier, président
- **Netframe**
  — M. Valentin Przyluski, fondateur et président-directeur général
- **Whaller**
  — M. Thomas Fauré, président
  — M. Grégory Saccomani, directeur marketing et communication
  — Mme Suzanne Vermote, chargée de communication
- **Wimi**
  — M. Antoine Dubosq, président
  — M. Thimothée Demoures, *chief of staff*
- **Talkspirit**
  — M. Philippe Pinault, co-fondateur et *chief executive officer*
- **Exo Platform**
  — M. Benjamin Mestrallet, président
  — Mme Veronika Mazour, directrice générale

*

Table-ronde de sociétés d'informatique en nuage n° 1

- **Amazon Web Services**
  — M. Arnaud David, directeur affaires publiques européennes
  — M. Cédric Mora, responsable affaires publiques
- **Google**
  — M. Fred Geraud de Lescazes, directeur des affaires publiques

*

Table-ronde de sociétés d'informatique en nuage n° 2

- **CleverCloud**
  — M. Quentin Adam, président-directeur général
  — M. Axel Laniez, responsable des affaires publiques

- **Numspot**

  — Mme Servane Augier, directrice des affaires publiques

- **Cloud Temple**

  — Mme Julie Latawiec, directrice des Affaires publiques

- **OVH cloud**

  — Mme Blandine Eggrickx, responsable des affaires publiques

- **Outscale**

  — M. David Chassan, *chief strategy officer*

  — M. Maxime Donadille, conseiller

- **Orange Business Services**

  — M. Alexandre Bord, directeur *cloud* France

- **Scaleway (Free)**

  — Mme Ombeline Bartin, directrice des affaires extérieures

  — M. Alexandre Durand, responsable des affaires publiques

*

- **Thales SA / S3NS**

  — M. Cyprien Falque, directeur général

  — Mme Caroline Morenas, responsable des affaires publiques

CONTRIBUTIONS ÉCRITES

- **Réponse commune :**

  — Direction interministérielle du numérique (Dinum)

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

  — Direction générale des entreprises (DGE)

  — Direction des affaires juridiques (DAJ)

- **Commission nationale de l'informatique et des libertés (Cnil)**
- **Départements de France**
- **Bleu SAS**