Proposition de loi, adoptée par le Sénat, relative à la sécurisation des marchés publics numériques (n° 2258)

Document faisant état de l'avancement des travaux de
M. Philippe Latombe, rapporteur

Mercredi 25 février 2025

COMMENTAIRE DES ARTICLES

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

➢ 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, en excluant les 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.

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 « matériel », prenant en considération l'objet de la norme, par exemple la préservation des intérêts fondamentaux de l'État, tel que la sécurité nationale (4).

La notion d'extraterritorialité est ancienne (5), mais elle s'est fortement **développée aux États-Unis** au tournant du XX^{ème} siècle, dans des domaines aussi divers que les sanctions internationales (6), la lutte contre la corruption (7), la lutte contre la fraude fiscale (8) et, plus récemment, dans le domaine du **numérique**.

---

(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 ».

(4) 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.

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

(6) 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.

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

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

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*, 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 ;

La portée de ces législations est d'autant plus importante en raison de la domination technologique et économique de certaines grandes entreprises américaines du numériques, 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 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 (5). Toute violation de données doit être notifiée aux autorités de contrôle et communiquée à la personne physique concernée (6).

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

---

(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).

(5) Article 32 du RGPD.

(6) Article 33 et 34 du RGPD.

fondamentales, de la législation en matière de sécurité nationale ou encore de l'accès des autorités publiques aux données à caractère personnel [1].

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 [2].

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 [3].

Le statut spécifique des États-Unis a fait l'objet de débats importants depuis le milieu des années 2010. Dans deux décisions de 2015 [4] et 2020 [5], 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.

Un 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 [6]. Malgré un premier recours porté par votre Rapporteur devant le Tribunal de l'Union européenne, rejeté en septembre 2025 [7], **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*** » [8].

---

(1) Article 45 du RGPD.

(2) Articles 46 et 49 du RGPD.

(3) Article 48 du RGPD.

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

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

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

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

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

Dernièrement, le règlement sur les marchés numériques (***Digital Markets Act***, ou *DMA*) de 2022 [1] et le règlement sur la protection des données (***Data Act***) de 2023 [2] 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.

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 permet d'intégrer aux appels d'offres des clauses en matière de sécurité, mais paraît insuffisant pour protéger durablement les administrations publiques des conséquences des lois extraterritoriales.

En effet, l'article L. 2153-1 du code de la commande publique prévoit le **principe d'égalité de traitement** des opérateurs économiques issus de l'Union européenne avec ceux issus d'États faisant partie de l'accord sur les marchés publics conclu dans le cadre l'Organisation mondiale du commerce (OMC). Ce principe **prohibe l'intégration de clauses relatives à la nationalité du répondant dans les appels d'offres**.

Par ailleurs, l'article L. 2112-4 du même code 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.

Toutefois, si cet article peut trouver à s'appliquer en matière de marché public de *cloud*, cela doit être à la condition de démontrer l'existence d'un risque en matière de sécurité des informations, condition qui n'est pas applicable à l'ensemble des données détenues par les administrations publiques [3].

---

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

(2) 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.

(3) Rapport fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale du Sénat sur la proposition de loi relative à la sécurisation des marchés publics numériques, par Mme Olivia Richard, déposé le 10 décembre 2025 (n° 199).

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 (1) 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* ».

La doctrine « *Cloud au centre* », qui a pris la forme de deux circulaires publiées en 2021 et 2023 (2) , 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 » (3) .

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**.

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

---

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

(2) 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 »).

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

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'Etat, 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 concernés 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 « 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.**

*

* *

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