Août 2026

Synthèse de la commission d'enquête menée à l'Assemblée nationale sur les dépendances et les vulnérabilités du numérique français

Sommaire

I- Un audit de la filière numérique française et européenne à l'heure d'une rupture grandissante avec les États-Unis 2

6 mois de travaux parlementaires 2

L'objet de la commission d'enquête 2

Pourquoi avons-nous suivi cette commission d'enquête ? 3

II- Synthèse des auditions 4

Définition de la souveraineté numérique 4

L'état de la menace 4

Les moyens d'actions envisageables 5

III- Les conclusions du rapport 8

Les recommandations 8

Les propositions 9

Les recommandations et les propositions qui concernent spécifiquement les collectivités territoriales 11

IV- Synthèse 12

V- Annexes 13

Annexe 1 : composition de la commission d'enquête 13

Annexe 2 : liste des recommandations du rapport 14

Annexe 3 : liste des propositions du rapport 16

VI- Bibliographie 19

I- Un audit de la filière numérique française et européenne à l'heure d'une rupture grandissante avec les États-Unis

6 mois de travaux parlementaires

Le 8 juillet 2026, la commission d'enquête menée de l'Assemblée nationale sur **« les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France »**, a adopté son rapport.[1] Le document ainsi rendu public a mis fin au processus d'audit et d'investigation amorcé le 3 février 2026. Durant ces 6 mois, 74 organisations ont été auditionnées[2], le président et la rapporteure ont rencontré 15 interlocuteurs clés de l'administration européenne à Bruxelles[3] et 36 entités majeures de la filière numérique française ont répondu aux questionnaires de la commission d'enquête.[4]

L'objet de la commission d'enquête

La création de cette commission d'enquête s'inscrit dans un contexte de tensions entre l'Europe et les États-Unis. Le deuxième mandat de Donald Trump crée une prise de conscience chez les acteurs privés et publics français du besoin urgent de gagner en autonomie stratégique pour se libérer des dépendances aux solutions numériques américaines. **C'est sur ces vulnérabilités critiques que la commission s'est concentrée.**

Plus spécifiquement, elle a mis l'accent sur les enjeux du déploiement du cloud (data centers, stockage de données, etc…). Cette thématique est structurante pour les acteurs technologiques et économiques du pays, dans la mesure où cette technologique sous-tend le fonctionnement de l'ensemble des applications informatiques, y compris l'IA.[5] Deuxièmement, elle s'est intéressée à un deuxième type de vulnérabilités qui découle des situations de monopole dont jouissent

[1] Rapport de la commission d'enquête : « Tome 1 - Rapport ». s. d. Consulté le 27 août 2026. https://www.assemblee-nationale.fr/dyn/17/rapports/cenum/l17b3054-t1_rapport-enquete.
[2] Rapport de la commission d'enquête p.431-437 : « Tome 1 - Rapport ». s. d. Consulté le 27 août 2026. https://www.assemblee-nationale.fr/dyn/17/rapports/cenum/l17b3054-t1_rapport-enquete.
[3] Rapport de la commission d'enquête P.439-440 : « Tome 1 - Rapport ». s. d. Consulté le 27 août 2026. https://www.assemblee-nationale.fr/dyn/17/rapports/cenum/l17b3054-t1_rapport-enquete.
[4] Rapport de la commission d'enquête Annexe 1 et 2 p.447-451 : « Tome 1 - Rapport ». s. d. Consulté le 27 août 2026. https://www.assemblee-nationale.fr/dyn/17/rapports/cenum/l17b3054-t1_rapport-enquete.
[5] Rapport de la commission d'enquête p.27 : « Tome 1 - Rapport ». s. d. Consulté le 27 août 2026. https://www.assemblee-nationale.fr/dyn/17/rapports/cenum/l17b3054-t1_rapport-enquete.

certains acteurs sur une grande partie de la chaîne de valeur de l'économie numérique.[6]

Enfin, **la commission a traité très partiellement** des sujets de cybersécurité, d'ingérences informationnelles ou encore de production de composants numériques (semi-conducteurs, puces).[7] Un intérêt pour ces thématiques aurait pu faire ressortir des dépendances à l'égard d'autres États comme la Chine et la Russie.

Pourquoi avons-nous suivi cette commission d'enquête ?

La gouvernance des données s'est imposée comme une thématique centrale des travaux d'OpenDataFrance. Pour la mettre en place et optimiser ses politiques publiques, il faut s'assurer en premier lieu de la bonne maîtrise de ses données. Cette commission d'enquête nous a semblé parfaitement couvrir ces enjeux.

De plus, une commission d'enquête prépare le terrain, via ses propositions, pour de futures législations. Or, pour les appréhender au mieux, il est crucial de comprendre le contexte dans lequel elles s'inscrivent.

Dans la suite de ce document, nous réaliserons une synthèse des thèmes abordés par les auditions. Puis, nous analyserons les recommandations et les propositions formulées par le rapport.

[6] Rapport de la commission d'enquête p.27 : « Tome 1 - Rapport ». s. d. Consulté le 27 août 2026. https://www.assemblee-nationale.fr/dyn/17/rapports/cenum/l17b3054-t1_rapport-enquete.

[7] Rapport de la commission d'enquête p.28-29 : « Tome 1 - Rapport ». s. d. Consulté le 27 août 2026. https://www.assemblee-nationale.fr/dyn/17/rapports/cenum/l17b3054-t1_rapport-enquete.

II- Synthèse des auditions

Définition de la souveraineté numérique

Lors des auditions, la plupart des interlocuteurs interrogés ont proposé leur définition de la souveraineté numérique. Celles-ci reprenaient en permanence les mêmes éléments avec une formulation différente. La définition de la DINUM nous semble la plus complète pour appréhender cette notion.

Définition de la DINUM[8]: capacité d'une Nation à agir de façon autonome dans les domaines stratégiques en maîtrisant les dépendances technologiques, opérationnelles et réglementaires envers des acteurs non européens sur l'ensemble de la chaîne technologique : infrastructure, logiciel, service, hébergement et matériel. En pratique, cela s'appuie sur deux notions clés : l'immunité au droit extraterritorial et la capacité de l'État à substituer une composante de ses systèmes numériques par une autre face à une menace pour son autonomie.

L'état de la menace

À l'exception des représentants des GAFAM, les interlocuteurs auditionnés s'accordent pour considérer que les dépendances actuelles sont des conséquences de choix politiques réalisés depuis la fin des années 1980. De plus, ils s'accordent sur le fait qu'aucun acteur et, par extension, aucun État ne peut contrôler à 100% la chaîne de valeur technologique. Dans l'état actuel des choses, nous importons près de 80% de nos infrastructures technologiques et numériques auprès de fournisseurs américains.[9] Cela nous rend vulnérable à des menaces très concrètes :

- La perspective d'un « kill switch » qui correspond à la capacité de l'État américain à contraindre ses entreprises à déconnecter tous leurs services et leurs logiciels opérant dans tel ou tel pays **(dépendance technologique)**.[10]

[8] Audition de la DINUM : videos.assemblee-nationale.fr. s. d.-g. « Vulnérabilités systémiques dans le secteur du numérique : Mme Stéphanie Schaer, directrice interministérielle du numérique - Mardi 14 avril 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18661157_69de4db03f9fa.vulnerabilites-systemiques-dans-le-secteur-du-numerique--mme-stephanie-schaer-directrice-intermini-14-avril-2026.

[9] Audition de la DINUM : videos.assemblee-nationale.fr. s. d.-g. « Vulnérabilités systémiques dans le secteur du numérique : Mme Stéphanie Schaer, directrice interministérielle du numérique - Mardi 14 avril 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18661157_69de4db03f9fa.vulnerabilites-systemiques-dans-le-secteur-du-numerique--mme-stephanie-schaer-directrice-intermini-14-avril-2026.

[10] Audition d'OVH : videos.assemblee-nationale.fr. s. d.-j. « Vulnérabilités systémiques dans le secteur du numérique : Table ronde réunissant des fournisseurs de cloud - Mardi 21 avril 2026 ».

- La perspective d'un recours par le gouvernement américain à des lois extraterritoriales (Cloud Act), qui mettraient à mal le respect du caractère privé des données des citoyens européens **(dépendance légale)**.[11]
- La perspective d'une montée incessante des prix des solutions technologiques par des entreprises qui se savent en position de quasi-monopole **(dépendance économique)**.[12]

Les auditions ont confirmé que ces 3 menaces conduisent les organisations à prendre conscience de la nécessité de faire évoluer leurs pratiques pour mieux prendre en compte ces enjeux de souveraineté et d'autonomie.

Les moyens d'actions envisageables

Les personnes interrogées ont détaillé les leviers mobilisables pour bâtir cette souveraineté et se libérer du spectre de ces menaces.

Elles s'accordent sur le **besoin d'augmenter les investissements publics et privés dans la filière**. Cela est plutôt logique dans la mesure où les organisations interrogées sont majoritairement des offreurs.[13] Néanmoins, **le point de divergence porte sur les solutions techniques que ces investissements devraient soutenir**.

En effet, **l'administration défend la constitution de communs numériques avec le recours aux logiciels libres** pour moins dépendre de solutions propriétaires.[14] Le cas de la gendarmerie est souvent cité comme un exemple de réussite de l'open

---

Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18716690_69e7657677c30.vulnerabilites-systemiques-dans-le-secteur-du-numerique--table-ronde-reunissant-des-fournisseurs-de-21-avril-2026.

[11] Audition d'OVH : videos.assemblee-nationale.fr. s. d.-j. « Vulnérabilités systémiques dans le secteur du numérique : Table ronde réunissant des fournisseurs de cloud - Mardi 21 avril 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18716690_69e7657677c30.vulnerabilites-systemiques-dans-le-secteur-du-numerique--table-ronde-reunissant-des-fournisseurs-de-21-avril-2026.

[12] Audition d'OVH : videos.assemblee-nationale.fr. s. d.-j. « Vulnérabilités systémiques dans le secteur du numérique : Table ronde réunissant des fournisseurs de cloud - Mardi 21 avril 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18716690_69e7657677c30.vulnerabilites-systemiques-dans-le-secteur-du-numerique--table-ronde-reunissant-des-fournisseurs-de-21-avril-2026.

[13] Rapport commission d'enquête p.431-437 : « Tome 1 - Rapport ». s. d. Consulté le 27 août 2026. https://www.assemblee-nationale.fr/dyn/17/rapports/cenum/l17b3054-t1_rapport-enquete.

[14] Audition d'Henri Verdier : videos.assemblee-nationale.fr. s. d.-d. « Vulnérabilités systémiques dans le secteur du numérique : M. Henri Verdier, directeur général de la fondation Inria ; M. David Chavalarias, directeur de recherche au CNRS et M. Robin Berjon, directeur de l'agence Supramundane - Mardi 10 mars 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18435565_69b00684b06ed.vulnerabilites-systemiques-dans-le-secteur-du-numerique--m-henri-verdier-directeur-general-de-la--10-mars-2026.

source dans l'administration.[15] Pour Philippe Gosset de Framasoft, le logiciel libre français doit s'inspirer de l'approche allemande et néerlandaise de cet outil, notamment sur le sujet de l'interopérabilité des données.[16] Au cours de ces auditions, il n'est pas le seul à évoquer la pertinence des modèles allemand et néerlandais. De plus, ils préconisent de sortir d'un rapport de consommation avec l'open source pour adopter un état d'esprit de participant à une communauté d'éditeurs de logiciels. Comme le résume l'Abril : « l'État doit produire du code public ».[17]

Néanmoins, ces acteurs du logiciel libre reconnaissent qu'une telle migration pose des problématiques en matière de formation des agents et d'internalisation des compétences.[18] Pour y répondre, les ministres David Amiel et Anne Le Hénanff proposent de revoir les programmes de l'éducation nationale afin de limiter au maximum les « adhérences culturelles » qui nous familiarise dès le milieu scolaire aux outils des géants américains.[19]

Les acteurs privés quant à eux considèrent qu'il faut davantage soutenir leur offre de services, notamment via la commande publique et les subventions. Il a ainsi été proposé que l'Europe, sur le modèle du Buy American Act, se dote d'un Buy European Act pour modifier les règles des marchés publics et ne plus recourir aux solutions américaines.[20] En ce qui concerne la commande privée, il est clair que

---

[15] Audition de la gendarmerie : videos.assemblee-nationale.fr. s. d.-b. « Vulnérabilités systémiques dans le secteur du numérique : Auditions diverses - Jeudi 7 mai 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18856181_69fc36ed23f6b.vulnerabilites-systemiques-dans-le-secteur-du-numerique--auditions-diverses-7-mai-2026.

[16] Audition Framasoft (Table ronde) : videos.assemblee-nationale.fr. s. d.-k. « Vulnérabilités systémiques dans le secteur du numérique : Table ronde sur le logiciel libre - Mercredi 6 mai 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18843051_69fb3ac192f70.vulnerabilites-systemiques-dans-le-secteur-du-numerique--table-ronde-sur-le-logiciel-libre-6-mai-2026.

[17] Audition Abril (Table ronde) : videos.assemblee-nationale.fr. s. d.-k. « Vulnérabilités systémiques dans le secteur du numérique : Table ronde sur le logiciel libre - Mercredi 6 mai 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18843051_69fb3ac192f70.vulnerabilites-systemiques-dans-le-secteur-du-numerique--table-ronde-sur-le-logiciel-libre-6-mai-2026.

[18] Audition Echirolles (Table ronde) : videos.assemblee-nationale.fr. s. d.-k. « Vulnérabilités systémiques dans le secteur du numérique : Table ronde sur le logiciel libre - Mercredi 6 mai 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18843051_69fb3ac192f70.vulnerabilites-systemiques-dans-le-secteur-du-numerique--table-ronde-sur-le-logiciel-libre-6-mai-2026.

[19] Audition David Dmiel et Anne Le Hénanff : videos.assemblee-nationale.fr. s. d.-c. « Vulnérabilités systémiques dans le secteur du numérique : M. David Amiel, ministre de l'action et des comptes publics ; Mme Anne Le Hénanff, ministre déléguée auprès du ministre de l'économie - Mercredi 20 mai 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18960105_6a0dc7442e4ff.vulnerabilites-systemiques-dans-le-secteur-du-numerique--m-david-amiel-ministre-de-l-action-et-de-20-mai-2026.

[20] Audition de France digitale : videos.assemblee-nationale.fr. s. d.-f. « Vulnérabilités systémiques dans le secteur du numérique : Mme Maya Noël, directrice générale de France Digitale - Jeudi 16

les entreprises et les individus changeront leurs habitudes de consommation lorsque le rapport coût/avantage sera plus intéressant pour eux.[21]

L'opposition entre ces deux modèles n'est pas si frontale que ce que l'on pourrait imaginer. Globalement, **tous les acteurs de la filière s'accordent pour considérer que les deux leviers peuvent être mobilisés conjointement si cela se fait à l'échelle européenne.** Elle seule dispose des capacités normatives et des moyens financiers nécessaires pour bâtir l'autonomie stratégique du continent. [22] Néanmoins, pour y parvenir, il faut réduire la fragmentation du cadre juridique européen.

Enfin, un élément qui vaut la peine d'être mentionné, est la possibilité de mobiliser l'épargne des citoyens. Cela libérerait des volumes financiers à même de concurrencer ceux présents sur le marché américain ou chinois. En effet, comme l'a rappelé Arthur Mensch (Mistral AI), les entreprises qui souhaitent innover ont besoin, pour la R&D, de financements colossaux afin d'atteindre la masse critique. Or, dans l'état actuel des marchés financiers, seul un déplacement des activités aux USA le permet.[23]

---

avril 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18700603_69e0cdbfb436a.vulnerabilites-systemiques-dans-le-secteur-du-numerique--mme-maya-noel-directrice-generale-de-fran-16-avril-2026.

Audition du collectif Eurostack : videos.assemblee-nationale.fr. s. d.-a. « Vulnérabilités systémiques dans le secteur du numérique : Audition du collectif Eurostack - Jeudi 26 mars 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18498860_69c53a0a4d17a.vulnerabilites-systemiques-dans-le-secteur-du-numerique--audition-du-collectif-eurostack-26-mars-2026.

Audition du CIGREF : videos.assemblee-nationale.fr. s. d.-h. « Vulnérabilités systémiques dans le secteur du numérique : Représentants de l'Anssi et du Cigref - Jeudi 30 avril 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18789257_69f2fbf68cae3.vulnerabilites-systemiques-dans-le-secteur-du-numerique--representants-de-l-anssi-et-du-cigref-30-avril-2026.

[21] Audition du CIGREF : videos.assemblee-nationale.fr. s. d.-h. « Vulnérabilités systémiques dans le secteur du numérique : Représentants de l'Anssi et du Cigref - Jeudi 30 avril 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18789257_69f2fbf68cae3.vulnerabilites-systemiques-dans-le-secteur-du-numerique--representants-de-l-anssi-et-du-cigref-30-avril-2026.

[22] Audition d'Orange : videos.assemblee-nationale.fr. s. d.-e. « Vulnérabilités systémiques dans le secteur du numérique : Mme Christel Heydemann, directrice générale du groupe Orange - Jeudi 16 avril 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18695953_69e09c20f2cf9.vulnerabilites-systemiques-dans-le-secteur-du-numerique---mme-christel-heydemann-directrice-genera-16-avril-2026.

[23] Audition de Mistral AI : videos.assemblee-nationale.fr. s. d.-i. « Vulnérabilités systémiques dans le secteur du numérique : Représentants de Mistral AI ; M. Fabrice Coquio, pdg de Digital Realty - Mardi 12 mai 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18888392_6a0330a9d4404.vulnerabilites-systemiques-dans-le-secteur-du-numerique--representants-de-mistral-ai--m-fabrice-c-12-mai-2026.

III- Les conclusions du rapport

Les conclusions du rapport prennent la forme de **18 recommandations et de 29 propositions**. Les premières traitent des mesures qui peuvent être mises en œuvre dans les plus brefs délais pour remédier rapidement aux dysfonctionnements de dispositifs existants.[24] Les secondes concernent les mesures qui peuvent nous engager sur la voie d'un changement de modèle.[25]

Les recommandations

À la lecture des 18 recommandations du rapport, nous constatons **qu'elles se concentrent sur 6 domaines d'actions** qui représentent 6 leviers mobilisables pour combattre les vulnérabilités et les dépendances du numérique français :

1. **Le soutien à l'écosystème du logiciel libre.** Il repose sur des investissements publics pour développer des briques technologiques open source. Il est envisagé d'orienter une partie des fonds France 2030 et du dispositif French 120 vers des sociétés qui développent ces solutions dans le respect des standards européens d'interopérabilités.[26] De plus, il est proposé de faciliter les contributions des agents de l'État aux communs numériques à hauteur d'une journée par an.[27] Sur le plan juridique, le rapport préconise dans la loi d'aligner la définition d'open source avec celle de l'OSAID 1.0, afin d'éviter les abus.[28]
2. **L'évolution des règles des marchés publics.** Il s'agit de s'assurer que la commande publique soutienne davantage le développement d'une offre de service souveraine. La principale mesure préconisée est d'étendre les principes de la doctrine Cloud au centre[29], à l'ensemble des entreprises publiques en plus des services administratifs de l'État.[30]
3. **Le soutien des pouvoirs publics aux entreprises.** L'État devrait se montrer proactif pour inciter les acteurs privés à migrer des solutions américaines vers des offres d'hébergements SecNumCloud, sans

[24] Annexe 2 du document
[25] Annexe 3 du document
[26] Annexe numéro 2 du document, recommandation numéro 11
[27] Annexe numéro 2 du document, recommandation numéro 15
[28] Annexe numéro 2 du document, recommandation numéro 18
[29] La doctrine Cloud au centre introduite par circulaire le 5 juillet 2021 impose aux administrations de recourir à des solutions cloud qui disposent de la qualification SecNumCloud de l'ANSSI pour tous leurs nouveaux projets numériques.
[30] Annexe numéro 2 du document, recommandation numéro 1

attendre que cela soit économiquement rentable.[31] De plus, une révision du crédit d'impôt recherche est envisagée pour que les entreprises innovantes en bénéficient prioritairement.[32] Une autre recommandation allant dans ce sens porte sur la possibilité de limiter les actions agressives de lobbying menées par les géants américains à Bruxelles.[33] Ainsi, la Commission européenne devrait consulter une plus grande diversité d'acteurs technologiques lors de ses travaux.

4. **L'éducation et la formation des individus aux outils numériques.** L'objectif serait de rompre nos habitudes d'usage qui nous poussent vers les solutions américaines. Ainsi, il est recommandé de mieux diffuser, dans le milieu scolaire, les outils de sensibilisation développés par la CNIL[34] et les outils de la forge numérique développés par l'éducation nationale.[35]
5. **La protection des données des citoyens.** Cela passe par la suppression de l'article 60 du RGPD qui instaure une règle de guichet unique pour le traitement des litiges liés aux données transfrontalières. Le défaut de cette règle étant qu'elle dirige les plaintes vers les États où les sièges sociaux se concentrent, ce qui complique l'application uniforme du droit européen. Pour résoudre ce problème, le traitement de ces plaintes serait confié à une entité centrale comme le comité européen de protection des données.[36]
6. **La gouvernance.** Il est recommandé de créer des organes d'évaluation de l'impact d'un « kill switch » sur notre économie pour assurer une meilleure préparation des services de l'État.[37]

Les propositions

À la lecture des 29 propositions du rapport, nous constatons **qu'elles se concentrent autour des 6 mêmes axes d'actions** avec l'objectif de bâtir un numérique français souverain :

[31] Annexe numéro 2 du document, recommandation numéro 3
[32] Annexe numéro 2 du document, recommandation numéro 8
[33] Annexe numéro 2 du document, recommandation numéro 10
[34] Annexe numéro 2 du document, recommandation numéro 4
[35] Annexe numéro 2 du document, recommandation numéro 17
[36] Annexe numéro 2 du document, recommandation numéro 5
[37] Annexe numéro 2 du document, recommandation numéro 6

1. **La dynamisation de l'écosystème européen du logiciel libre.** Elle passe par la création d'organisations et d'instruments qui soutiendraient politiquement et économiquement le développement des communs numériques : Edic Digital Commons[38], fondation France Libre Open Source (Flos)[39], fond Logic[40], syndicat de données[41].
2. **Le recours à la commande publique.** La commission souhaite que l'État aligne sa doctrine en matière de commande publique avec ses nouveaux objectifs en matière d'open source, en rendant obligatoire le recours à des solutions open source dans les marchés publics d'ici au 1er janvier 2030.[42] Une autre proposition très forte est l'adoption d'un Buy European Act qui privilégiera l'accès aux marchés publics de l'Europe à ses entreprises.[43]
3. **La refonte du soutien public au secteur privé.** Il est envisagé de créer un dispositif d'aide à destination des PME qui conçoivent des logiciels libres.[44] De plus, pour inciter les entreprises françaises à rester sur le marché européen, il est préconisé de rendre obligatoire le remboursement des aides à l'amorçage et des crédits impôt-recherche en cas de vente d'une entreprise à un acteur extra-européen.[45] L'État pourrait également détenir des actions spécifiques dans des entreprises innovantes (Mistral AI et ChapsVision).[46] Enfin, la rapporteure souhaite la création d'une banque publique, totalement indépendante du marché américain.[47]
4. **L'éducation et la formation.** Pour mettre fin à l'adhérence culturelle aux solutions américaines, l'éducation nationale pourrait se fixer comme objectif de ne pas mettre à disposition des élèves des outils Microsoft.[48]
5. **La protection des données.** Au niveau européen, cela passerait de nouveau par une modification du RGPD avec la création d'une procédure de recours collective.[49] Le rapport évoque aussi la possibilité de considérer comme une

[38] Annexe numéro 3 du document, proposition numéro 1
[39] Annexe numéro 3 du document, proposition numéro 2
[40] Annexe numéro 3 du document, proposition numéro 3
[41] Annexe numéro 3 du document, proposition numéro 4
[42] Annexe numéro 3 du document, proposition numéro 10
[43] Annexe numéro 3 du document, proposition numéro 15
[44] Annexe numéro 3 du document, proposition numéro 16
[45] Annexe numéro 3 du document, proposition numéro 18
[46] Annexe numéro 3 du document, proposition numéro 19
[47] Annexe numéro 3 du document, proposition numéro 24
[48] Annexe numéro 3 du document, proposition numéro 5
[49] Annexe numéro 3 du document, proposition numéro 25

infraction pénale l'irrespect par une grande plateforme de la dignité de ses utilisateurs.[50]

6. **La gouvernance.** La commission souhaite que l'Europe renforce son arsenal juridique de lutte contre les lois extraterritoriales[51], en allant jusqu'à suspendre les plateformes qui s'y soumettent.[52] Enfin, le gouvernement pourrait s'étoffer avec la création d'un ministère du numérique de plein exercice.[53] Cette nouvelle entité aurait notamment la charge de mener un moratoire sur les projets de data centers dans le pays.[54]

Les recommandations et les propositions qui concernent spécifiquement les collectivités territoriales

- La recommandation numéro 16 est en faveur d'un meilleur suivi des dépenses numériques des collectivités territoriales, notamment en ayant recours à des partenariats d'innovation et à des achats groupés inter collectivités.
- La proposition numéro 2 soutient la création d'une fondation France Libre Open Source (Flos) qui assurerait la pérennité des briques open source développées par l'État et les collectivités.
- La proposition numéro 11 défend l'intégration d'une clause d'entiercement dans les contrats signés entre une structure publique, ce qui comprend les collectivités et un fournisseur, afin d'éviter les situations de vendor lock-in et de garantir la continuité de service.
- La proposition numéro 13 souhaite que les dépenses d'open source des collectivités territoriales soient considérées comme des dépenses d'investissement.
- La proposition numéro 14 conseille d'interdire aux institutions publiques de communiquer sur des réseaux sociaux qui ne sont pas interopérables et décentralisés.

[50] Annexe numéro 3 du document, proposition numéro 26
[51] Annexe numéro 3 du document, proposition numéro 23
[52] Annexe numéro 3 du document, proposition numéro 27
[53] Annexe numéro 3 du document, proposition numéro 28
[54] Annexe numéro 3 du document, proposition numéro 21

IV- Synthèse

En résumé, les travaux de la commission d'enquête nous renseignent sur le rôle de meneur que les institutions publiques, sous toutes leurs formes (administration, entreprises publiques, agences publiques, collectivités territoriales), devraient endosser pour bâtir notre souveraineté numérique. La lecture du rapport laisse peu de doutes sur le fait que les députés considèrent que **les actions décisives doivent être menées prioritairement par le secteur public** puisque seul ce dernier disposerait des leviers pour engager le reste de la société sur la voie de l'autonomie technologique.

Le deuxième enseignement majeur concerne la volonté de **ne pas recréer en Europe le modèle américain qui ne produirait que de « nouveaux tyrans »**[55] sur notre sol. Il s'agit plutôt d'en inventer un nouveau qui reposerait, avant tout, sur des communs numériques.

[55] Audition d'Henri Verdier : videos.assemblee-nationale.fr. s. d.-d. « Vulnérabilités systémiques dans le secteur du numérique : M. Henri Verdier, directeur général de la fondation Inria ; M. David Chavalarias, directeur de recherche au CNRS et M. Robin Berjon, directeur de l'agence Supramundane - Mardi 10 mars 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18435565_69b00684b06ed.vulnerabilites-systemiques-dans-le-secteur-du-numerique--m-henri-verdier-directeur-general-de-la--10-mars-2026.

V- Annexes

Annexe 1 : composition de la commission d'enquête

La présidence qui organise et mène les auditions : Philippe Latombe, membre du groupe politique « les démocrates », de la 1ère circonscription de Vendée.

Les vice-présidents soutenant la mission de la présidence : Philippe Gosselin, membre du groupe politique « droite républicaine », de la 1ère circonscription de la Manche. Sacha Houlié, membre du groupe politique « socialistes et apparentés », de la 2ème circonscription de Vienne, Isabelle Rauch, membre du groupe politique « Horizon et Indépendants », de la 9ème circonscription de la Moselle. Sophie-Laurence Roye, membre du groupe politique « Rassemblement National », de la 2ème circonscription de l'Yonne.

La rapporteure en charge de la rédaction du rapport devant clôturer la commission : Cyrielle Chatelain, membre du groupe politique « écologiste et social », de la 2ème circonscription de l'Isère.

À cela s'ajoute 4 secrétaires et 16 membres simples qui complètent la composition de la commission d'enquête. Ils participent au processus d'audition des personnes invitées à s'exprimer devant la commission et ils jouent un rôle en votant l'adoption du rapport rédigé par la rapporteure.

Annexe 2 : liste des recommandations du rapport

La rapporteure formule 18 recommandations qui visent à remédier rapidement à des dysfonctionnements constatés ou à apporter des évolutions aux dispositifs existants.

Recommandation n° 1 : Étendre les principes de la doctrine Cloud au centre à l'ensemble des entreprises publiques.

Recommandation n° 2 : Compléter l'indice de résilience numérique par l'édiction de grilles d'achat et de clauses types à destination des acheteurs privés.

Recommandation n° 3 : Inviter instamment l'ensemble des entreprises à migrer immédiatement le stockage de leurs données sensibles vers des offres d'hébergement qualifiées SecNumCloud et à renoncer à recourir aux prestations d'acteurs états-uniens.

Recommandation n° 4 : Mieux valoriser et diffuser les outils de sensibilisation développés par la Cnil, notamment dans le cadre scolaire.

Recommandation n° 5 : Supprimer la règle du guichet unique prévue par le RGPD et confier au Comité européen de protection des données le contrôle des traitements transfrontaliers de données personnelles réalisés par les plus grandes plateformes.

Recommandation n° 6 : Faire évaluer par un comité d'économistes l'état de nos dépendances et l'impact sur nos économies d'un kill switch généralisé de la part des États-Unis.

Recommandation n° 7 : Adopter le décret d'application de la loi Sren visant à encadrer le recours aux crédits cloud.

Recommandation n° 8 : Revoir le critère d'attribution du crédit d'impôt recherche pour mieux soutenir les entreprises innovantes et réduire les montants attribués aux entreprises de services numériques.

Recommandation n° 9 : Exiger que les centrales d'achat informent leurs clients sur la nationalité de l'éditeur des solutions logicielles qu'elles proposent, en se fondant sur une méthodologie solide qui tienne compte de la soumission de l'éditeur à des législations étrangères.

Recommandation n° 10 : Assurer la représentativité des consultations menées par la Commission européenne en limitant le nombre d'interactions directes ou indirectes avec des représentants des grandes entreprises numériques.

Recommandation n° 11 : Flécher une partie des fonds France 2030 et du dispositif French 120 à destination des sociétés développant des solutions open source et respectant les standards d'interopérabilité.

Recommandation n° 12 : Créer une cellule de suivi de l'impact de l'IA sur l'emploi réunissant les partenaires sociaux et les chercheurs.

Recommandation n° 13 : Défendre au niveau européen l'obligation pour les data centers de fournir des certificats d'achat d'électricité renouvelable à une maille horaire.

Recommandation n° 14 : Déployer la politique du ministère de l'éducation nationale en faveur des communs numériques.

Recommandation n° 15 : Permettre aux agents de l'État de contribuer, l'équivalent d'une journée par an, à des communs numériques de leur choix dans une logique d'intérêt général.

Recommandation n° 16 : Développer les partenariats d'innovation et les achats de groupe entre collectivités.

Recommandation n° 17 : Soutenir et valoriser la forge numérique développée par le ministère de l'éducation nationale.

Recommandation n° 18 : Faire respecter la définition de l'open source dans son acception de l'OSAID 1.0, y compris par des moyens judiciaires.

Annexe 3 : liste des propositions du rapport

La rapporteure formule 29 propositions qui visent à engager un changement de modèle afin de sortir des dépendances et vulnérabilités structurelles liées à l'utilisation des outils numériques extra-européens.

Proposition n° 1 : Soutenir politiquement et financièrement l'Edic Digital Commons, qui vise à coordonner l'action des pays européens dans le développement des communs numériques.

Proposition n° 2 : Créer une fondation France Libre Open Source (Flos) qui assurera la pérennité des briques open source indispensables aux outils numériques développés par l'État et les collectivités pour renforcer la maîtrise de leurs systèmes d'information.

Proposition n° 3 : Instaurer un fonds pour le libre, l'open source et la garantie de l'indépendance des communs (Logic), qui apportera des financements complémentaires au Sovereign Tech Fund européen en faveur des communs numériques.

Proposition n° 4 : Créer un statut de syndicat de données.

Proposition n° 5 : Objectif zéro Microsoft dans les écoles.

Proposition n° 6 : Modifier l'article L. 312-9 du code de l'éducation, pour que la formation à l'utilisation responsable des outils et des ressources numériques comprenne l'enseignement des logiciels libres.

Proposition n° 7 : Prévoir que le code source des logiciels développés par une entreprise entrera dans le domaine public en cas de cessation définitive d'activité.

Proposition n° 8 : Créer un musée du numérique.

Proposition n° 9 : Réinternaliser les compétences, en faisant du ministère de la justice une priorité.

Proposition n° 10 : Rendre obligatoire l'open source dans les marchés publics des administrations et des opérateurs de l'État, des entreprises publiques et des sociétés concessionnaires d'un service public d'ici le 1er janvier 2030.

Proposition n° 11 : Intégrer une clause d'entiercement (escrow) lors de la contractualisation d'une structure publique avec un fournisseur afin de garantir la continuité de service.

Proposition n° 12 : Rendre obligatoire dans les marchés publics l'application de la fiche pratique pour l'achat responsable de solutions d'intelligence artificielle et du référentiel général d'interopérabilité.

Proposition n° 13 : Comptabiliser toutes les dépenses d'open source des collectivités territoriales en dépenses d'investissement.

Proposition n° 14 : Exiger des institutions publiques qu'elles communiquent sur des réseaux sociaux interopérables et décentralisés.

Proposition n° 15 : Instaurer une préférence européenne (Buy European Act).

Proposition n° 16 : Créer un dispositif Open source pour les PME.

Proposition n° 17 : Intégrer une composante de souveraineté dans la certification Hébergeur de données de santé.

Proposition n° 18 : Prévoir le remboursement des aides à l'amorçage et du crédit impôt recherche en cas de vente d'une entreprise à un acteur extra-européen.

Proposition n° 19 : Détenir des actions spécifiques, ou golden shares, dans Mistral AI et ChapsVision.

Proposition n° 20 : Intégrer une clause de souveraineté finale pour garantir la continuité de l'État.

Proposition n° 21 : Prononcer un moratoire sur les projets de data centers ne répondant pas à l'impératif de souveraineté.

Proposition n° 22 : Instaurer un contrôle public du déploiement des data centers répondant à l'impératif de souveraineté.

Proposition n° 23 : Lutter contre l'application extraterritoriale de législations étrangères et les attaques visant le droit européen en activant le règlement de blocage et, si nécessaire, l'instrument anticoercition.

Proposition n° 24 : Mettre en place une entité bancaire immune publique, totalement indépendante du marché américain, qui offre des services de base en matière de banque et d'assurance en zone euro.

Proposition n° 25 : Créer une procédure de recours collectif au titre du RGPD.

Proposition n° 26 : Mobiliser le droit pénal contre les plateformes en cas d'atteinte aux droits des personnes.

Proposition n° 27 : Suspendre les plateformes dangereuses.

Proposition n° 28 : Créer un ministère du numérique de plein exercice, auquel serait rattachée une autorité interministérielle du numérique dotée de prérogatives renforcées.

Proposition n° 29 : Créer une délégation parlementaire au numérique au sein de l'Assemblée nationale.

VI- Bibliographie

« Tome 1 - Rapport ». s. d. Consulté le 27 août 2026. https://www.assemblee-nationale.fr/dyn/17/rapports/cenum/l17b3054-t1_rapport-enquete.

videos.assemblee-nationale.fr. s. d.-a. « Vulnérabilités systémiques dans le secteur du numérique : Audition du collectif Eurostack - Jeudi 26 mars 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18498860_69c53a0a4d17a.vulnerabilites-systemiques-dans-le-secteur-du-numerique--audition-du-collectif-eurostack-26-mars-2026.

videos.assemblee-nationale.fr. s. d.-b. « Vulnérabilités systémiques dans le secteur du numérique : Auditions diverses - Jeudi 7 mai 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18856181_69fc36ed23f6b.vulnerabilites-systemiques-dans-le-secteur-du-numerique--auditions-diverses-7-mai-2026.

videos.assemblee-nationale.fr. s. d.-c. « Vulnérabilités systémiques dans le secteur du numérique : M. David Amiel, ministre de l'action et des comptes publics ; Mme Anne Le Hénanff, ministre déléguée auprès du ministre de l'économie - Mercredi 20 mai 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18960105_6a0dc7442e4ff.vulnerabilites-systemiques-dans-le-secteur-du-numerique--m-david-amiel-ministre-de-l-action-et-de-20-mai-2026.

videos.assemblee-nationale.fr. s. d.-d. « Vulnérabilités systémiques dans le secteur du numérique : M. Henri Verdier, directeur général de la fondation Inria ; M. David Chavalarias, directeur de recherche au CNRS et M. Robin Berjon, directeur de l'agence Supramundane - Mardi 10 mars 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18435565_69b00684b06ed.vulnerabilites-systemiques-dans-le-secteur-du-numerique--m-henri-verdier-directeur-general-de-la--10-mars-2026.

videos.assemblee-nationale.fr. s. d.-e. « Vulnérabilités systémiques dans le secteur du numérique : Mme Christel Heydemann, directrice générale du groupe Orange - Jeudi 16 avril 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18695953_69e09c20f2cf9.vulnerabilites-systemiques-dans-le-secteur-du-numerique---mme-christel-heydemann-directrice-genera-16-avril-2026.

videos.assemblee-nationale.fr. s. d.-f. « Vulnérabilités systémiques dans le secteur du numérique : Mme Maya Noël, directrice générale de France Digitale - Jeudi 16 avril 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18700603_69e0cdbfb436a.vulnerabilites-systemiques-dans-le-secteur-du-numerique--mme-maya-noel-directrice-generale-de-fran-16-avril-2026.

videos.assemblee-nationale.fr. s. d.-g. « Vulnérabilités systémiques dans le secteur du numérique : Mme Stéphanie Schaer, directrice interministérielle du

numérique - Mardi 14 avril 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18661157_69de4db03f9fa.vulnerabilites-systemiques-dans-le-secteur-du-numerique--mme-stephanie-schaer-directrice-intermini-14-avril-2026.

videos.assemblee-nationale.fr. s. d.-h. « Vulnérabilités systémiques dans le secteur du numérique : Représentants de l'Anssi et du Cigref - Jeudi 30 avril 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18789257_69f2fbf68cae3.vulnerabilites-systemiques-dans-le-secteur-du-numerique--representants-de-l-anssi-et-du-cigref-30-avril-2026.

videos.assemblee-nationale.fr. s. d.-i. « Vulnérabilités systémiques dans le secteur du numérique : Représentants de Mistral AI ; M. Fabrice Coquio, pdg de Digital Realty - Mardi 12 mai 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18888392_6a0330a9d4404.vulnerabilites-systemiques-dans-le-secteur-du-numerique--representants-de-mistral-ai--m-fabrice-c-12-mai-2026.

videos.assemblee-nationale.fr. s. d.-j. « Vulnérabilités systémiques dans le secteur du numérique : Table ronde réunissant des fournisseurs de cloud - Mardi 21 avril 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18716690_69e7657677c30.vulnerabilites-systemiques-dans-le-secteur-du-numerique--table-ronde-reunissant-des-fournisseurs-de-21-avril-2026.

videos.assemblee-nationale.fr. s. d.-k. « Vulnérabilités systémiques dans le secteur du numérique : Table ronde sur le logiciel libre - Mercredi 6 mai 2026 ». Consulté le 27 août 2026. http://videos.assemblee-nationale.fr/video.18843051_69fb3ac192f70.vulnerabilites-systemiques-dans-le-secteur-du-numerique--table-ronde-sur-le-logiciel-libre-6-mai-2026.