

Commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France



M. Philippe Latombe

Président, Député de Vendée
(Dem)

Mme Cyrielle Chatelain

Rapporteure, Députée de l'Isère
(EcoS)



Une commission d'enquête interrogeant la souveraineté numérique de la France dans un contexte géopolitique défavorable, marqué par l'entrée des Gafam dans l'ère Maga

Le groupe Écologiste et social a pris l'initiative de la création de la commission d'enquête, notamment en raison du contexte géopolitique. **Les dépendances numériques deviennent, sous la présidence de Donald Trump, un levier de menaces supplémentaire**, au même titre que les ressources énergétiques importées ou les droits de douane.

Les diagnostics établis par une commission d'enquête sénatoriale en 2019 et par un rapport de M. Philippe Latombe en 2021 convergeaient déjà pour souligner l'acuité du sujet et la **nécessité de reconquérir une souveraineté numérique pour s'extraire des dépendances à des acteurs étatiques ou privés**. En réalité, ces dépendances sont la résultante de **plusieurs décennies durant lesquelles cinq géants ont constitué des empires industriels** et se sont profondément implantés en Europe. **Google, Apple, Amazon, Meta et Microsoft détiennent ou maîtrisent une très grande partie de l'infrastructure et des services numériques** utilisés dans notre quotidien.

Ce constat est devenu d'autant plus critique aujourd'hui que, sous la présidence de Donald Trump, **l'ensemble du cadre international en vigueur depuis la Seconde Guerre mondiale est fortement remis en cause**. La stratégie de sécurité nationale américaine, publiée début décembre sous l'égide du nouveau président, dénigre nos réglementations environnementales, désigne l'Union européenne comme ennemi de la liberté et recherche l'alignement des valeurs européennes sur celles des MAGA.

Cette situation rend nécessaire **l'examen des dépendances systémiques des citoyens, des administrations et des acteurs économiques aux technologies numériques**. La commission d'enquête s'est donc efforcée de mener un **travail cartographique précis des vulnérabilités liées aux logiciels et services cloud extra-européens** (relevant notamment du modèle *des hyperscalers*), de façon à pouvoir ensuite **dégager des propositions d'actions concrètes**.

Où sont nos vulnérabilités?

La commission s'est concentrée sur les dépendances et vulnérabilités au cœur du modèle mis en place par les acteurs états-unis, fondé sur la constitution de monopoles, le contrôle de plateformes structurantes, la mise en place de systèmes massifs de stockage et de traitement des données. Faute de disposer du temps suffisant, elle n'a pas pu traiter des sujets de cybersécurité, d'ingérences informationnelles et d'infrastructures, qui auraient fait ressortir d'autres vulnérabilités à des grandes puissances internationales, en particulier la Russie et la Chine.

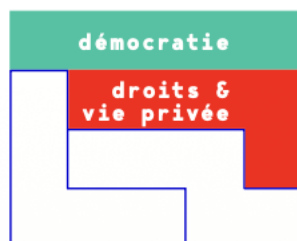
ATTAQUES CYBER



VERROUILLAGE DES UTILISATEURS



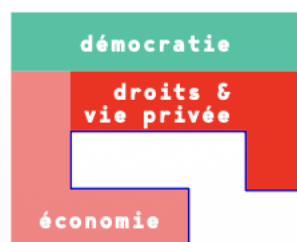
MONÉTISATION DES DONNÉES



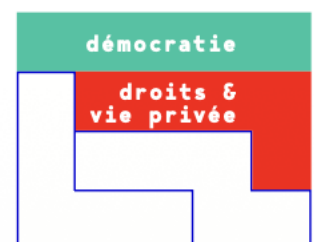
DÉPENDANCE AUX INFRASTRUCTURES



GESTION DES DONNÉES



INGÉRENCES INFORMATIONNELLES



Objectifs et Méthodes de travail

Le premier objectif était de **mesurer ces dépendances et d'examiner dans quelle mesure des solutions françaises ou européennes pouvaient constituer des alternatives**, et à quelles conditions (compétitivité, performance, etc.). Cela exigeait de :

- Disposer d'un panorama le plus complet possible et chiffré des achats logiciels et services cloud des administrations et des services publics clés ;
- Déterminer dans quelle mesure des stratégies techniques et contractuelles sont mises en œuvre pour assurer la résilience des systèmes d'information, des services et la protection des données ;
- Comprendre la place des acteurs et de l'emploi français dans la fourniture des services informatiques à la sphère publique et le rôle de la commande publique et privée dans l'accompagnement de la structuration d'une filière numérique française.

Pour ce faire, la rapporteure a sollicité de nombreux acteurs par le biais de questionnaires.

SOLLICITATIONS DE LA COMMISSION D'ENQUETE PAR TYPE D'ACTEUR PUBLIC

Acteur public	Modalités de sollicitation
Administrations d'État	Questionnaires à destination des administrations (voir liste dans le rapport d'enquête) Auditions des directions des systèmes d'information (DSI) Questionnaire à destination de la direction interministérielle du numérique (Dinum)
Administration hospitalière	Questionnaire à destination de l'AP-HP (Assistance publique-Hôpitaux de Paris)
Collectivités territoriales	Non traité en raison du temps d'enquête limité et de la concomitance avec les élections municipales
Grands instituts de recherche publics	Table ronde réunissant des DSI d'organismes de recherche
Opérateurs d'importance vitale	Questionnaires à destination d'une sélection d'entreprises publiques opérant un service critique d'importance vitale (voir liste dans le rapport d'enquête)
Transverse	Table ronde réunissant les centrales d'achat publiques Questionnaire à destination de l'Ugap

Enfin, le secteur bancaire, et plus particulièrement la question des moyens de paiement, a fait l'objet d'une étude de cas.

Objectifs et Méthodes de travail

Le second objectif consistait à **évaluer les dépendances systémiques engendrées par la concentration de pouvoirs** dans les mains de quelques acteurs de taille mondiale.:

- Expliquer pourquoi les produits développés par les firmes américaines se sont imposés et continuent d'évincer du marché leurs alternatives européennes ;
- Décrire l'usage de la donnée personnelle à des fins de monétisation, en identifiant les risques sur la vie privée ;
- Comprendre les prises de position des acteurs mondiaux sur les infrastructures vitales, en prenant comme cas d'étude les data centers.

Afin de mener cette analyse systémique des dépendances liées aux fournisseurs extra-européens, la commission d'enquête a procédé à des auditions d'experts qualifiés et de représentants du monde économique :

- autorités indépendantes : Commission nationale de l'informatique et des libertés (Cnil) et Autorité de la concurrence
- opérateurs économiques de l'État : Caisse des dépôts, Banque publique d'investissement
- chercheurs, journalistes et experts dans le domaine du numérique et de la protection des données personnelles
- associations de protection du droit à la propriété des données personnelles
- représentants d'entreprises du numérique et du monde économique
- anciens dirigeants politiques

Ces auditions ont été complétées d'un déplacement à Bruxelles, afin de rencontrer des représentants des institutions européennes.

Enfin, le sujet des data centers a fait l'objet d'un traitement particulier, à travers l'envoi de questionnaires à l'administration et au gestionnaire du réseau de transport d'électricité.

Les enseignements : une dépendance dangereuse et aux nombreux effets nocifs

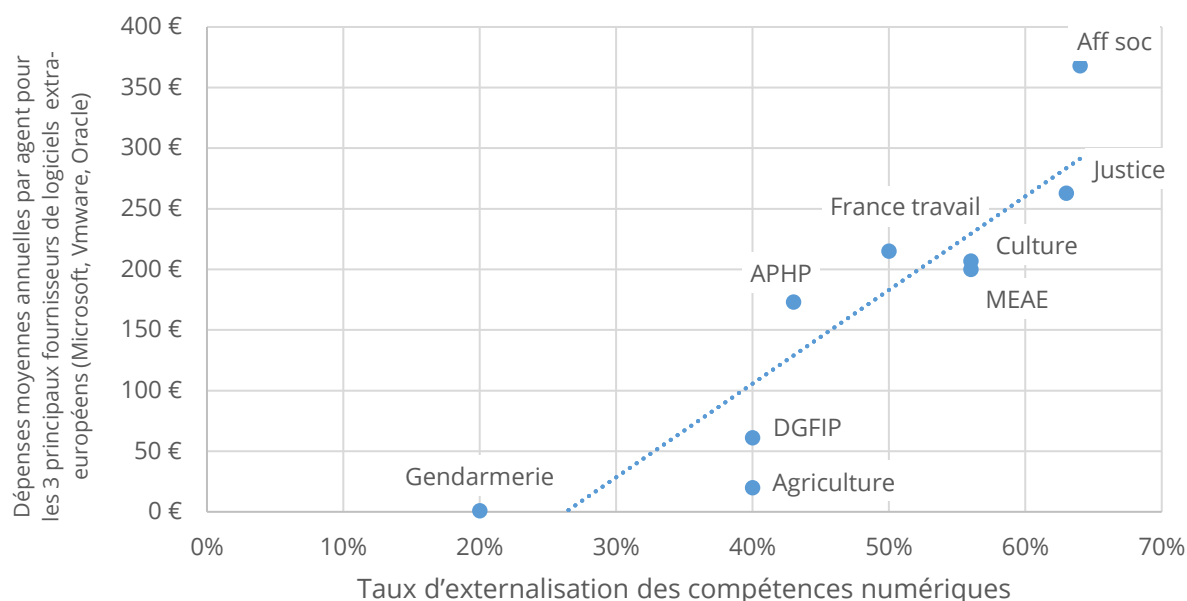
La commission d'enquête a documenté des dépendances profondément ancrées dans les systèmes d'information des administrations et des entreprises. Sur le périmètre des cinquante premiers fournisseurs de logiciels de la première centrale d'achats publics (Ugap), **les acteurs états-uniens représentent près de 80 % des achats** – un constat concordant avec celui établi par le Cigref s'agissant du secteur privé. **La dépendance à trois éditeurs, Microsoft, VMWare et Oracle, est quasi généralisée.**

Selon les estimations de la commission, les achats publics de logiciels extra-européens pour l'ensemble des administrations publiques représenteraient à minima chaque année **1,5 milliard d'euros**. 1 milliard de ces dépenses pourraient dès aujourd'hui être réorientées vers des solutions open source.

Exemple Microsoft

L'utilisation généralisée des produits Microsoft auprès de la **quasi-intégralité des administrations des ministères** est à l'origine des dépenses les plus importantes : **115 millions d'euros en 2025 sur le périmètre de la commission d'enquête** (et en hausse).

DEPENDANCE DES ADMINISTRATIONS A L'EGARD DES FOURNISSEURS DE LOGICIELS EXTRA-EUROPEENS EN FONCTION DE LEUR TAUX D'EXTERNALISATION DES COMPETENCES NUMERIQUES



Source : réponses écrites aux questionnaires de la rapporteure

Aide à la lecture : Le ministère de la justice et les ministères sociaux présentent les niveaux de dépendance les plus élevés, en lien avec un déficit avéré de compétences numériques.

Les enseignements : une dépendance dangereuse et aux nombreux effets nocifs

Vulnérabilité des données et dépendances aux infrastructures de stockage

La **doctrine Cloud au centre** a permis à l'État de contenir les risques liés au stockage de données en exigeant que les données les plus sensibles soient hébergées en interne ou sur un cloud qualifié SecNumCloud. **La commission constate cependant que certains ministères ou administrations stockent sur des clouds états-unis des données à caractère personnel et des données d'une sensibilité particulière.** C'est notamment le cas pour les ministères sociaux, mais aussi la CNAF et France Travail.

Les entreprises continuent, en revanche, de recourir massivement aux services cloud américains, y compris celles qui sont en charge de services publics critiques.

OPÉRATEURS DE CLOUD DES SIX ENTREPRISES PUBLIQUES INTERROGÉES

	AWS	GCP	Microsoft Azure	S3NS	Bleu
EDF	X	X	X	X	X
Enedis	X	X	X		
ADP			X		
Natran	X		X		
RATP	Recours à une société américaine pour la billettique en mobilité et la monétique				
SNCF Réseau	X		X		

Source : réponses écrites aux questionnaires de la rapporteure

Avec le déploiement naissant des outils d'intelligence artificielle pour les agents publics, le risque de développer de nouvelles dépendances est important. Les ministères régaliens semblent privilégier des solutions à façon, développées à partir de modèles d'IA open source ou propriétaires, notamment celles du français Mistral AI, et hébergées par des acteurs français. **Cependant, les travaux de la commission d'enquête ont mis en évidence des cas d'usage du modèle Claude d'Anthropic, de Copilot de Microsoft, de Gemini de Google ou de GPT d'OpenAI au sein de plusieurs ministères, des caisses de sécurité sociale, de l'AP-HP et de France Travail.**



Les enseignements : une dépendance dangereuse et aux nombreux effets nocifs

Une contribution réduite des Gafam à l'activité économique nationale et *in fine* aux rentrées fiscales

Quelques géants états-uniens captent l'essentiel de la richesse liée au numérique. La rapporteure a mesuré que **seule une faible fraction du chiffre d'affaires réalisé par les Gafam en France correspondait à une création de valeur ajoutée sur le territoire** – entre 9 et 28 %, contre 42 % en moyenne dans le secteur des plateformes et du cloud, et 49 % dans les logiciels.

VALEUR AJOUTÉE DE L'ACTIVITÉ FRANÇAISE – COMPARAISON DES ACTEURS ÉTATSUNIENS À LA MOYENNE DU SECTEUR

	Valeur ajoutée sur chiffre d'affaires (%)
Secteur du logiciel – France (*)	49 %
Microsoft France	18 %
Oracle France	28 %
Secteur des plateformes et du cloud – France	42 %
Google France	26 %
Facebook France	19 %
Amazon online France	9 %
AWS EMEA	19 %
Google cloud France	28 %

L'impôt sur les sociétés acquitté par les Gafam demeure très faible au regard de leur activité. La **taxe sur les services numériques**, qui a généré **542 millions en 2025** sur le périmètre des grandes plateformes extra-européennes, s'avère donc absolument essentielle pour assurer des retombées pour la collectivité.

Les enseignements : une dépendance dangereuse et aux nombreux effets nocifs

Une utilisation inconsidérée des données personnelles

Le modèle économique des grandes plateformes, fondé sur la collecte et la **monétisation des données personnelles** à des fins publicitaires, prospère au prix de la violation de la vie privée des citoyens européens. Elles se servent désormais des volumes considérables de données amassées pour **alimenter leurs modèles d'IA, sans consentement préalable des utilisateurs**. S'y est greffé un écosystème opaque de courtiers en données, les **data brokers**, qui font circuler les informations de façon incontrôlée et sont en mesure de les agréger pour établir des profils précis des individus, avec un **risque de fichage systémique de la population** en cas d'instrumentalisation par un gouvernement.

Un danger géopolitique majeur

Les données stockées auprès des *hyperscalers* sont accessibles aux autorités américaines, en vertu des lois extraterritoriales. **Microsoft a reçu des Etats-Unis, au second semestre 2025, 5 587 demandes de divulgation de données, pour l'ensemble de ses clients dans le monde, et a donné suite à 75 % d'entre elles. Ses dirigeants ont notamment reconnu avoir transmis les données de contenu (content data) de deux entreprises européennes au titre du Cloud Act durant l'année 2025.**

Mais **les cas de divulgation de données européennes pourraient être bien plus nombreux**, puisque l'entreprise maintient une opacité totale sur la transmission des métadonnées, des données des particuliers européens et des requêtes des autorités américaines à des fins de sécurité nationale (*Fisa* et *National security letters*).

La situation n'est pas propre à Microsoft : Google a reçu 60 000 demandes des autorités américaines, satisfaites à 89 %.

Ces dépendances constituent, enfin, **un levier de pression géopolitique majeur** à la main des Etats-Unis. Les autorités américaines sont en mesure de couper les services numériques américains à l'Union européenne (**kill switch**) par l'application de mesures de contrôle d'exportation. L'activation de cette arme pourrait en effet entraîner en quelques mois une **paralysie complète des systèmes d'information**, avec des vulnérabilités dès les premiers jours.

La coupure d'accès pourrait également être **utilisée de façon ciblée afin de faire pression sur des personnalités politiques**. L'isolement numérique du juge de la Cour pénale internationale **Nicolas Guillou** pourrait se reproduire de façon systémique à l'encontre de parlementaires, de défenseurs des droits, ou de responsables de la Commission européenne en charge d'appliquer le DMA ou le DSA.



Quelles sont les racines profondes de cette situation ?

Une régulation qui doit être appliquée de manière plus rigoureuse

La puissance financière des Gafam, et la complaisance des juridictions irlandaises et luxembourgeoise, leur permet d'enfreindre la régulation européenne.

Le RGPD, texte pilier de la régulation des données à l'échelle européenne, **est régulièrement contourné**, avec la complicité de l'Irlande. Sur les 3,5 milliards d'euros d'amendes prononcés entre 2020 et 2024, par la Data Protection Commission irlandaise, seuls 0,6% ont été effectivement recouvrés.

Les **sanctions envers les Gafam au titre du droit de la concurrence s'élèvent à 17 milliards d'euros**, dont 12 milliards pour le seul Google. Ces amendes demeurent faibles au regard de leur chiffre d'affaires, et trop tardives pour contrecarrer leur expansion. La question de savoir si le Digital Markets Act (DMA) et le Digital Services Act (DSA), avec leur logique d'intervention *ex ante*, parviendront à redonner de l'effectivité à cette régulation, demeure entière.

Plusieurs enquêtes de la Cnil ont montré que les géants du numérique avaient adopté des pratiques contraires à la législation sur les cookies. De fait, sur les 953 millions d'euros d'amendes prononcées par l'autorité sur le fondement de la directive e-privacy depuis 2019, 903 millions l'ont été à l'encontre des grandes plateformes extra-européennes.

SANCTIONS PRONONCÉES PAR LA CNIL À L'ENCONTRE DES GRANDES ENTREPRISES EXTRA-EUROPÉENNES ENTRE 2019 ET 2025)

Date	Société	Amende administrative (en millions d'euros)
07/12/2020	Google	100
07/12/2020	Amazon	35
31/12/2021	Google	150
31/12/2021	Facebook	60
19/12/2022	Microsoft	60
29/12/2022	Apple	8
27/12/2023	Amazon	15
01/09/2025	Google	325
01/09/2025	Shein	150

Quelles sont les racines profondes de cette situation ?

Un lobbying féroce et massif

Les Big Tech déploient des moyens massifs pour infléchir la réglementation européenne en leur faveur. Les dépenses de lobbying atteignaient **35 millions d'euros en 2025** pour les Gafam, avec **210 lobbyistes déclarés**, dont 85 disposant d'un badge officiel pour accéder au Parlement européen.

Au total, ces entreprises ont obtenu **265 rendez-vous avec la Commission** européenne, soit plus d'un par jour ouvré. Le dernier exemple en date de l'efficacité de ce lobbying est celui de **l'omnibus numérique**, qui crée des failles béantes dans le RGPD au seul bénéfice des grands acteurs extra-européens. Le rapport met ainsi en évidence les modifications proposées par l'omnibus numérique, directement inspirées des contributions des Gafam.

Un verrouillage systématique

Grâce à leur **domination de l'ensemble de la stack numérique**, les géants états-uniens sont en mesure d'enfermer les utilisateurs dans leur écosystème propriétaire. Par des offres attractives, telles que les crédits cloud, et **une stratégie de pénétration dans les établissements scolaires**, ils favorisent une acculturation précoce à leurs outils, dont il est ensuite complexe de sortir en raison de pratiques commerciales abusives, de verrous technologiques, et du poids des habitudes.

Cette stratégie mobilise un réseau de **passeurs de technologie**, des entreprises de services du numérique liées aux Gafam par des partenariats technologiques, qui diffusent le narratif d'une absence d'alternative européenne auprès de leurs clients. Il convient également de souligner le rôle indirect des centrales d'achat, qui entretiennent le **sovereignty washing** faute d'identifier clairement les offres souveraines.

Avec l'intelligence artificielle, la domination américaine risque d'atteindre un nouveau palier

Les entreprises américaines occupent d'ores et déjà le terrain : Chat GPT est utilisé par 79% des Français utilisant l'IA, soit 22 millions de personnes, contre seulement 14 % pour le Chat de Mistral (4 millions de personnes). Une grande majorité d'entreprises déploient des solutions américaines sur des plateformes sans s'occuper de la propriété de leurs données. Cette domination se déploie dans un contexte qu'on pourrait qualifier de **nouveau Far West**.

La soutenabilité de l'IA sur le long terme est soumise à de fortes interrogations

Le FMI lui-même évoque un **risque de bulle du secteur de l'IA**. **Les montants d'investissement des Gafam et des nouveaux géants de l'IA ne sont pas en rapport avec les revenus générés, ni même les revenus potentiels**. Pour être en mesure de rentabiliser leurs investissements dans les data centers IA, les entreprises de la tech devraient générer 2 000 milliards de revenus par an. Même en suivant une approche maximaliste, il en manque 800 millions. Le cœur du problème est le coût de l'utilisation de l'IA : **95 % des entreprises n'arrivent pas à rentabiliser leur investissement aujourd'hui**. Cette approche financière doit se doubler d'une prise en compte de **l'impact environnemental massif de la consommation d'électricité et de la construction des data centers**.

Face aux conséquences de l'IA, la régulation publique est d'ores et déjà nécessaire

Les implications sociales peuvent être importantes, en particulier pour les jeunes travailleurs. Dans les domaines du logiciel et de la communication, l'Insee a publié des premiers chiffres alarmants : l'emploi des jeunes de 15 – 29 ans (hors alternants) est en baisse de 7,4% sur un an dans le domaine de l'informatique, de 5,8% dans l'édition et de 3,7% dans les activités de conseil en gestion.

Un déploiement chaotique des Data centers au détriment de notre souveraineté

Dans le **domaine énergétique**, les *hyperscalers* sont en train de **capter les capacités électriques à leur profit**. La **localisation des data centers en France** ne garantit ni la **protection des données**, ni l'**utilisation des capacités au profit de l'économie européenne**.

15 GW de capacités énergétique sont déjà réservés sur le réseau pour les data centers, soit 24 % de la puissance du parc nucléaire français.

- Parmi les 15 GW d'ores et déjà réservé, environ :
- 2 GW réservés directement par les hyperscalers
 - 2,5 GW développés par des acteurs de data centers extra-européens
 - 9 GW portés par des acteurs non spécialisés dans une logique d'investissement : iront prioritairement aux hyperscalers
 - **Reste seulement 1,4 GW développé par des acteurs des data centers européens**

Les territoires où les capacités réservées sont les plus importantes : Seine et Marne (1 845 MW), Essonne (1 475 MW), Nord (1 340 MW), Indre (1 310 MW), Seine-Saint-Denis (1 170 MW) et Moselle (1 049 MW).

Dans le cadre de la **task force** qui a été mise en place par le gouvernement suite au sommet de l'IA, 57 entreprises sont accompagnées (seules ou dans le cadre de partenariat) :

ENTREPRISES ACCOMPAGNÉES PAR LA TASK FORCE DATA CENTERS

Nationalité de l'entreprise	Nombre d'entreprises	Pourcentage des entreprises accompagnées
Union européenne	25	44 %
<i>Dont Française</i>	21	35 %
Hors Union Européenne	29	51 %
<i>Dont étatsuniennes</i>	14	25 %
Indéterminée	3	5 %

Les propositions de la commission d'enquête pour un nouveau modèle français et européen du numérique

L'Europe n'est condamnée ni à la vassalisation, ni au reniement de ses principes. Nous devons redéfinir une politique du numérique qui nous permette de reconquérir la maîtrise de nos outils, faire respecter le droit et soutenir le développement d'un écosystème pérenne et diversifié.

Il convient de **ne pas reproduire un modèle fondé sur la violation des droits des personnes et l'illégalité permanente**, mais au contraire de **bâtir un nouveau modèle** construit autour de l'**open source** et de l'**interopérabilité**.

Henri Verdier : « Remplacer un monopole américain, adversaire assumé de la démocratie, par son équivalent français, n'améliorerait ni la situation démocratique ni la liberté du marché. (...) ***Il ne suffit pas de changer la nationalité du tyran.*** »

Nos propositions

Faire du Libre et de l'open source le pilier d'une politique numérique française ambitieuse

Pourquoi le Libre et l'open source ?

- Les solutions open source, libres et interopérables **suppriment les risques de dépendance à des solutions propriétaires** et favorisent l'innovation. A rebours de la logique d'émergence de champions, elles reposent sur la construction de communautés actives autour de solutions partagées.
- La France est le **1^{er} marché de l'open source en Europe** (5,9 milliards d'euros de chiffre d'affaires).
- **Le marché de l'open source en France** – rassemblant à la fois la vente de logiciels et de services – représentait **5,9 milliards d'euros en 2022, soit 11 % du marché** total des logiciels et services numériques. Le marché est **en croissance de 7,8 % par an**, une tendance supérieure à celle du secteur (+ 6,3% par an). **L'open source représentait 63 800 équivalents temps plein en 2022.**

Comment le promouvoir ?

Les propositions de la rapporteure visent à construire une **véritable politique industrielle** reposant à la fois sur la commande publique et les entreprises.

- Les **marchés publics d'État 100 % open source à partir de 2030**
- 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.
- **Crédit d'impôt « open source » pour les PME**

Quels instruments et quels moyens pour assurer sa pérennité ?

- Une **fondation « France libre open source »** pour assurer la pérennité des briques open source essentielles, notamment celles sur des outils numériques développés par l'État et les collectivités. La gouvernance sera représentative de la diversité des contributeurs aux briques hébergées, associant la sphère publique et la sphère privée.
- Un **fonds pour le libre, l'open source et la garantie de l'indépendance des communs**. Il soutiendra financièrement la maintenance et le développement des briques open source de bas niveau indispensables, en contractualisant des projets relevant des communs ou en salariant des contributeurs.
- **Un renforcement des effectifs numériques de l'Etat**, et notamment au sein du ministère de la justice. Le manque de compétences fragilise la capacité à maîtriser les systèmes informatiques et pousse les administrations concernées à acheter des solutions propriétaires clés en main.

Quels effets attendus ?

- Des **économies budgétaires**. La gendarmerie nationale a réalisé 534 millions d'économies depuis 2004 grâce au choix de l'open source. Pour la DGFiP, les coûts évités grâce au logiciel libre représentent environ 10 millions d'euros par an.
- **Renforcer les compétences au sein des ministères** afin de garantir une meilleure maîtrise globale du SI des ministères dans un contexte d'évolution extrêmement rapide des technologies et dans une logique de contribution des ministères aux briques logicielles open source.
- Soutenir la filière numérique française et contribuer à la création d'un écosystème diversifié et innovant, grâce à une **réorientation de la commande publique et privée**.

Marc Boget : « *La gendarmerie nationale a été précurseur en opérant, dès le début des années 2000, un virage stratégique vers Linux pour ses serveurs et ses postes de travail. Ce choix du logiciel libre visait à rompre avec les dépendances aux éditeurs étrangers pour garantir l'intégrité de nos systèmes et redevenir maîtres de notre destin numérique et financier. Aujourd'hui, nous ne possédons plus aucun serveur Windows et seuls 1 054 postes sur 80 000 conservent ce système pour des besoins de niche très spécifique* »

Se doter d'un arsenal de souveraineté

Pourquoi un arsenal de souveraineté ?

- La politique française de soutien au numérique a été « financière ». L'unique objectif était de créer les nouvelles « licornes ».
- Aujourd'hui, de nombreuses entreprises soutenues par l'État ont été rachetées par des investisseurs extra-européens.
- Comme le montre l'exemple du blocage par l'administration américaine des modèles Mythos et Fable 5 d'Anthropic, nous pouvons être privés d'un outil détenu par des acteurs extra-européens.

Quels instruments ?

- Prévoir le **remboursement des aides** à l'amorçage et du crédit d'impôt recherche **en cas de vente d'une entreprise à un acteur extra-européen**.
- L'État doit détenir des « **golden shares** » dans **Mistral AI et ChapsVision**. A l'heure où les administrations font des choix qui les engagent pour de nombreuses années, il convient de maîtriser le devenir des entreprises technologiques stratégiques.
- Intégrer une **clause de souveraineté finale** dans les marchés publics ou les contrats de financement pour garantir la continuité de l'État.

Les data centers : stopper la captation de nos ressources par les hyperscalers

Pourquoi la politique de soutien tous azimuts est un « but contre le camp » de la souveraineté ?

- Avec le Sommet de l'IA et Choose France, **le gouvernement a déroulé le tapis rouge aux investisseurs internationaux pour qu'ils investissent dans des data centers sur notre sol**.
- Les demandes de raccordement ont explosé : les capacités de connexion réservées auprès de RTE, le gestionnaire du réseau de transport d'électricité français, s'élèvent à **15 gigawatts, soit près d'un quart de la capacité du parc nucléaire français**.
- Sur les 15 GW, **moins de 10% (1,3 GW) sont aujourd'hui développés par des acteurs français**. Sans action immédiate, la quasi-intégralité des capacités seront captées par les *hyperscalers*. Une fois construits, les data centers créent très peu d'emplois. L'essentiel de la valeur ajoutée, qui réside dans la maîtrise de la capacité de calcul, partira ainsi à l'étranger.

Quels instruments ?

- Un **moratoire immédiat sur les projets de data centers qui profitent aux acteurs extra-européens**.
- La définition d'un **nouveau cadre de régulation pour orienter les projets au profit de l'intérêt public national**. Plusieurs outils peuvent être mobilisés, dont une structure publique d'investissement qui pourrait ainsi être envisagée.

Lutter contre les effets systémiques des plateformes numériques

Les vulnérabilités aux solutions américaines et aux effets des plateformes se font sentir chaque jour et se renforcent. L'Europe a mis en place le DMA et le DSA pour réguler les géants américains, mais les effets d'une telle régulation sont encore incertains. Des mesures immédiates doivent être engagées pour lutter contre les effets systémiques des grandes plateformes et leur ancrage au plus profond de notre économie :

- **Zéro Microsoft dans les écoles** : apprentissage du numérique obligatoirement sur des logiciels open source.
- **Fin de la communication de institutions publiques sur des réseaux sociaux non interopérables**, à commencer par X.
- Au niveau européen : renforcer la crédibilité dissuasive du **règlement de blocage** et de **l'instrument anticoercition**, et mettre en place une **entité bancaire immune à l'extra-territorialité du dollar**.
- Au niveau national : **création d'un syndicat des données, mise en place d'une procédure de recours collectif au titre du RGPD**, mobilisation du droit pénal en cas d'atteinte aux droits des personnes, **suspension des plateformes dangereuses**.

Placer le numérique au premier rang des priorités politiques

Le numérique a été le grand absent des politiques publiques, alors qu'il s'agit désormais d'un enjeu de survie pour nos démocraties et notre économie.

- **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**.
- Créer un **ministère du numérique de plein exercice**, capable de piloter le déploiement d'outils au sein de l'ensemble des administrations, d'imposer une vision industrielle du numérique en France, et de porter une voix forte au niveau européen.
- Créer une **délégation au numérique à l'Assemblée nationale**. Le numérique est transverse : il touche à la fois à l'économie, au droit, au social, aux affaires étrangères et à la défense. Nous, parlementaires, devons nous saisir de ce sujet, et de façon transpartisane.

[illegible]

