SYNTHÈSE

du rapport de la commission d'enquête parlementaire sur les vulnérabilités et dépendances numériques de la France

Président : Philippe Latombe (député MoDem)
Rapporteure : Cyrielle Chatelain (députée Écologiste)

Édité le 15 juillet 2026

Table des matières

La commission d'enquête de l'Assemblée nationale sur les dépendances et les vulnérabilités dans le secteur du numérique s'est déroulé du 3 février au 15 juillet 2026. Cette commission d'enquête a été créée à la demande du groupe Écologiste et Social. Elle était présidée par Philippe Latombe et Cyrielle Chatelain en était la rapporteure. La commission a entendu 112 personnes au cours de 45 auditions. Elle a également étudié 61 contributions écrites.

Pourquoi cette commission d'enquête ? Les GAFAM à l'ère MAGA

Les diagnostics antérieurs sur la souveraineté numérique convergeaient d'ores et déjà pour souligner la criticité du sujet et la nécessité de reconquérir une souveraineté numérique pour s'extraire des dépendances à des acteurs extra-eurpopéens. Commission d'enquête au Sénat en 2019, rapport Latombe à l'Assemblée nationale en 2021, rapport de la Cour des Comptes en 2025, les alertes existaient. Mais le second mandat de Donald Trump à la présidence des États-Unis, démarré en janvier 2025, ainsi que le déploiement à grande échelle de l'intelligence artificielle générative, ont donné à ces dépendances une acuité nouvelle.

Un choix marqué par le contexte géopolitique internationale

2025 a marqué une rupture dans les relations entre les États-Unis et les pays de l'Union européenne. L'ensemble du cadre en vigueur depuis la seconde guerre mondiale - le respect du droit international, des règles de l'organisation mondiale du commerce et plus récemment l'engagement commun dans les Conférence internationales de lutte contre le dérèglement climatique – est fortement remis en cause. La stratégie de sécurité nationale américaine, publiée début décembre, dénigre nos règlementations environnementales, désigne l'Union Européenne comme ennemi de la liberté et recherche l'alignement des valeurs Européennes sur celles des *MAGA*.

C'est pourquoi le groupe Écologiste et social a pris l'initiative de la création de cette commission d'enquête, pour examiner les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France. Ne pouvant plus nous satisfaire de constats généraux, l'objectif est de mener un travail cartographique précis, dans un impératif de lucidité, de façon à pouvoir ensuite dégager des actions concrètes.

Une typologie des vulnérabilités dans le secteur du numérique

TYPOLOGIE DES RISQUES ET VULNÉRABILITÉS SYSTÉMIQUES DANS LE DOMAINE DU NUMÉRIQUE : SYNTHÈSE

	Atteinte au fonctionnement politique ou démocratique	Risque économique pour les entreprises	Continuité de fonctionnement des services essentiels	Atteinte aux droits et à la vie privée des personnes
Attaques cyber	X	X	X	X
Ingérences informationnelles	X			X
Gestion des données	X	X		X
Monétisation des données	X			X
Stratégies de verrouillage des utilisateurs	X	X	X	
Dépendances aux infrastructures et composants clés		X	X	

Première partie - LE DIAGNOSTIC

Chapitre 1 – Microsoft, VMWare, Oracle, ces trois logiciels qui nous gouvernent : les dépendances des administrations aux solutions américaines

Des questionnaires ont été envoyés aux administrations, les interrogeant sur les fonctions support (bureautique, systèmes d'exploitation, gestion de bases de données), sur les logiciels métiers (développé spécifiquement pour les besoins du ministère), les solutions cloud, les outils IA, avec des précisions sur les développements internes et externes, la répartition des achats de progiciels « sur étagère » et évidemment les fournisseurs et les contrats

A. Les applications métiers : le recours principalement à des fournisseurs français, mais des vulnérabilités dans certains ministères

Les chiffres recueillis auprès des administrations montrent que **les logiciels spécifiques (développés pour les besoins propres des ministères) représentent deux tiers du total, contre seulement 30 % pour les logiciels sur étagère** ; les développements réalisés par des sociétés externes représentent 57 % du total, les équipes projets interne mais avec un appui prestataire externe concernent 25 % des cas, une minorité conçue en interne totalement (11 %).

La détection des vulnérabilités a été faite selon plusieurs critères :

- Pays d'origine du fournisseur ;
- Capacité à substituer une solution par une autre, immédiatement ou selon un horizon de temps défini
- Criticité de l'application : catégorie 1 « applications dont le défaut est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique ou à la vie des personnes » et catégorie 2 « applications dont le défaut est susceptible d'engendrer l'interruption de l'exercice d'une mission de service public essentielle ».
- Coûts de développement engagé pour la réalisation de l'application ou les coûts de licence payée annuellement
- Maîtrise des codes sources ou le recours à des solutions open source

Le calcul fait à partir des réponses aux questionnaires montrent que, pour les applications critiques, **les fournisseurs français sont très majoritaires, avec respectivement 69 % du total pour les applications de catégorie 1 et 83 % pour celles de catégorie 2.**

Sur les 417 applications pour lesquelles la rapporteure dispose des informations, 64 % sont la propriété des administrations utilisatrices (224) et 16 % sont développées en open source (67).

La commission note cependant une dépendance à des fournisseurs extra-européens pour certaines applications critiques. Les États-Unis constituent le deuxième pays fournisseur, et parmi ces applications, certaines ne sont pas substituables et d'autres ne peuvent l'être qu'à un

horizon compris entre un et trois ans, ce qui justifie une vigilance particulière malgré le faible nombre relatif des solutions concernées.

Les dépendances ne se situent donc pas prioritairement dans la masse des applications métiers critiques, mais dans certains points de fragilité très ciblés, d'autant plus sensibles lorsqu'ils concernent des solutions coûteuses, difficiles à substituer et porteuses de données ou de fonctions essentielles (gestion des hôpitaux, utilisation dans la justice ou par la police, comptabilité administrative).

B- Logiciels supports : la dépendance à trois acteurs américains, Microsoft, Oracle et VMware

En réalité, **les dépendances les plus structurantes résident dans les logiciels supports,** et concernent plus particulièrement à **trois acteurs américains, Microsoft, Oracle et VMware**. À l'exception de la Gendarmerie nationale, qui a généralisé le recours à des solutions *open source,* les administrations d'État apparaissent dans une dépendance généralisée et ancrée à Microsoft pour les systèmes d'exploitation et la suite bureautique Office 365. Elles dépendent également d'Oracle pour la gestion des bases de données, et de VMware pour la virtualisation, dans une moindre mesure d'IBM et de Red Hat.

La dépendance à ces briques de base est jugée particulièrement forte, car elles soutiennent le fonctionnement transversal de l'ensemble des systèmes d'information. Mais un état des lieux sérieux a déjà souvent été fait, et beaucoup administrations lancent des actions de réductions des dépendances, se désengagent progressivement de certains outils américains et font évoluer leurs architectures techniques (APHP, CNAM et CNAV, ministères de l'éducation nationale, économiques et financiers).

Il faut souligner l'importance de poursuivre dans le déploiement des solutions open source, en mettant en avant l'exemple à suivre de la gendarmerie nationale et des transitions progressives engagées par d'autres ministères.

La gendarmerie nationale est un modèle : elle a mené un programme de bascule de l'intégralité de ses systèmes d'information vers des solutions en open source, couvrant les outils bureautiques, mais aussi les systèmes d'exploitation et les solutions permettant de faire fonctionner les applications métiers. Ainsi *« Le recours à Microsoft Office, contraint pour des raisons de compatibilité avec des outils tiers notamment judiciaires, ou le format de fichiers échangés avec des entités partenaires, reste marginal : moins de 2 % du parc des postes de travail en sont équipé »*

Si dès le début des années 2000, la gendarmerie nationale a opéré un virage numérique stratégique, d'autres administrations ont adopté ces solutions de façon partielle, principalement pour la partie bureautique. Les Ministères économiques et financiers ont amorcé une transition partielle vers les solutions open source, qui touche d'abord les outils bureautiques. Le Ministère de l'intérieur poursuit la même démarche d'intégration progressive de solutions open source pour les briques essentielles de son système d'information, et le Ministère de la transition écologique a développé une alternative open source dans le panel des applications proposées à ses agents, sans toutefois que le déploiement en soit systématique.

UTILISATION PAR ADMINISTRATION DES LOGICIELS FOURNIS PAR LES CINQ PRINCIPAUX FOURNISSEURS EXTRA-EUROPEENS

	Microsoft	Oracle	VM Ware	IBM	Red Hat
Ministères sociaux	X		X		
MAASA	X		X		X
AP-HP	X	X	X		
MEF	X	X	X	X	X
CNAF	X	X	X	X	X
CNAV	X		X	X	X
CNAM	X	X	X	X	
CULTURE	X				
DEFENSE	X				X
MTE	X				
Edu Nat	X	X	X	X	X
Gend nat	X				
Justice	X	X	X		X
MEAE	X		X		
Intérieur - DGPN	X		X		
France Travail	X		X		

Source : réponses aux questionnaires de la rapporteure.

C- Une vulnérabilité dans le domaine des données dû aux choix des infrastructures de stockage

Un hébergement en interne largement privilégié

Pour rappel, les enjeux de souveraineté et un impératif de protection des données sensibles sont désormais formalisés par la doctrine **« Cloud au centre »** de l'État. Cette circulaire de juillet 2021, demande de recourir au cloud et impose de **s'orienter vers des solutions disposant de la qualification SecNumCloud** de l'Anssi quand les données sont d'une sensibilité particulière.

Les administrations stockaient historiquement leurs applications et leurs données en interne, en s'appuyant sur le parc de datacenters de l'État, qui comptait 166 sites en 2012, réduit à 58 après la mise en œuvre d'efforts de rationalisation. Dans les faits, **l'hébergement en interne demeure largement privilégié, en particulier sur le périmètre régalien et dans les grands ministères disposant d'infrastructures historiques (transition écologique, éducation nationale, agriculture et souveraineté alimentaire),** tandis que le recours au cloud commercial est plus fréquent parmi les administrations les plus faiblement dotées (ministères sociaux et culture sauf les Archives nationales).

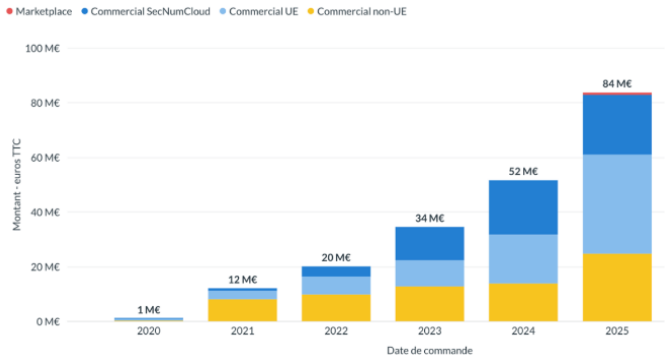
Le ministère de l'intérieur et la direction générale des finances publiques se distinguent par une vigilance particulière quant à la maîtrise de leurs systèmes d'information. La volonté de bénéficier des fonctionnalités de l'informatique en nuage tout en maintenant un niveau élevé de protection des données les a conduits à développer leur propre cloud interne à vocation interministérielle : **le cloud Nubo pour la DGFIP, et le cloud Pi pour le ministère de l'intérieur, devenus opérationnels respectivement en 2018 et 2017**. S'ils disposent de

moyens plus limités, le ministère de la justice et le ministère de l'Europe et des affaires étrangères (MEAE) veillent également à garantir l'intégrité de leurs données en les hébergeant sur leurs propres infrastructures tout en étudiant l'opportunité d'une migration vers l'un des clouds interministériels.

Un niveau de maîtrise variable en cas de recours à des offres commerciales

Le déploiement du cloud est en forte progression parmi les administrations, avec l'État comme principal moteur. Les derniers bilans de la doctrine « Cloud au centre » de la Dinum font état d'une **multiplication par quatre des commandes sur le marché « Nuage public » de l'Ugap entre 2022 et 2025,** de 20 millions d'euros à 84 millions d'euros.

L'hébergement des données est majoritairement assuré par des **prestataires européens**, et un recours croissant aux offres certifiées SecNumCloud s'observe également : en 2025, les offreurs qualifiés SecNumCloud ont représenté 49,7 % des commandes passées par les administrations centrales sur ce marché « Nuage public ».



Source : Dinum, février 2026

En parallèle, **les hyperscalers perdent des parts de marché de l'UGAP, mais les dépenses adressées aux hyperscalers continuent de croître en valeur.**

Certaines administrations se tournent exclusivement vers des solutions SecNumCloud, même lorsqu'elles n'en ont pas l'obligation juridique car les données ne sont pas d'une sensibilité particulière au sens de la loi Sren (Justice, Agriculture ou DGCCRF), données personnelles mais non sensibles. D'autres ministères, au contraire, tirent parti du caractère officiel « non sensibles » pour recourir à des offres moins sécurisées.

Plusieurs situations de fortes vulnérabilités identifiées

Parfois des données sensibles sont hébergées en non-conformité avec l'article 31 de la loi Sren. **France Travail concentrait en 2025, 83 % de ses dépenses de services cloud sur trois fournisseurs américains, essentiellement ServiceNow, AWS et Microsoft Azure** ; les **hébergeurs américains** représentaient également près de **98 % des dépenses de cloud de la CNAF.**

Les **ministères sociaux**, le ministère de la **justice** et le **ministère de la culture** ont porté à la connaissance de la commission d'enquête leur utilisation des services de **cloud Microsoft Azure** qui accompagnent la suite Office 365, dans le cadre d'une dérogation à la doctrine Cloud au centre. La direction du numérique des ministères sociaux a étudié à l'été 2025 deux alternatives, la solution Bleu et LaSuite.

Les travaux de la commission d'enquête ont également mis en évidence des applications métiers critiques hébergées par des prestataires américains, là encore pour des raisons de coût. Par exemple, le **projet Virtuo du ministère de l'Éducation nationale,** destiné à la gestion RH qualitative et couvrant notamment le recrutement, la formation, l'évaluation des agents et la

gestion des compétences, repose sur la **solution SaaS de Salesforce**. La CNIL et l'ANSSI avaient rendu un avis négatif sur le niveau de protection offert contre les lois extraterritoriales. Salesforce a notamment reconnu, dans une réponse à une demande de précision du ministère, qu'il pouvait faire l'objet de demande d'accès aux données des clients de la part d'autorités étrangères. Mais le ministère a considéré que, bien que les données soient d'une sensibilité particulière, leur violation n'est pas 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.

La police nationale et la gendarmerie hébergent leurs **plateformes d'aide aux victimes** sur les plateformes non SecNumCloud, portées respectivement par **Easiware et l'éditeur américain Salesforce**. L'Anfsi travaille à évoluer vers une plateforme commune hébergeable en SecNumCloud.

D- Intelligence artificielle : le début de nouvelles dépendances

Le déploiement naissant des outils d'intelligence artificielle pour les agents publics se fait sans réflexion sur les usages pertinents et sans alerte sur les dangers. **Les travaux de la commission d'enquête ont mis en évidence que les modèles Claude d'Anthropic, de Copilot de Microsoft, de Gemini de Google ou de GPT d'OpenAI étaient répandus au sein de plusieurs ministères**, des caisses de sécurité sociale, de l'AP-HP et de France Travail, portés par les *hyperscalers* Microsoft, AWS ou Google. Le ministère de la transition écologique de privilégier Mistral, opéré en SecNumCloud, lorsqu'ils ont à traiter de données sensibles.

Le risque sous-jacent est celui d'une captation des données sensibles de l'État par des acteurs extra-européens, et de leur réutilisation pour l'entraînement de leurs modèles ce qui devrait conduire certaines administrations ou organismes à privilégier des solutions plus maîtrisées.

L'Inserm a ainsi décidé de développer des outils de type LLM (Large language model) sur son infrastructure cloud interne ; idem pour la DGFIP qui choisit l'open source, et la Dinum a structuré un socle interministériel de l'IA générative reposant sur l'API (Application Programming Interface) Albert, une plateforme spécifique de données et un Assistant IA construit sur des modèles Mistral AI en environnement SecNumCloud, avec un objectif de déploiement auprès de 10 000 agents publics à l'horizon de juin 2026.

Mais il faut souligner la persistance d'un risque important de « shadow IA ». Une enquête interne réalisée entre janvier et avril 2026 auprès de 1 867 agents montre que 89 % des personnes interrogées utilisent déjà l'IA dans leur travail, 85 % recourent aux outils fournis par leur employeur, mais 55 % reconnaissent également utiliser des agents conversationnels de manière informelle, ce qui implique un grand risque de divulgations de données sensibles non maîtrisées.

Chapitre 2 – Le risque numérique : élargissement de l'analyse aux entreprises publiques et privées

A- Les entreprises publiques : des systèmes d'information industriels sécurisés, l'utilisation croissante du cloud public

Par nature, et du fait des dispositions applicables aux opérateurs d'importance vitale (OIV), les entreprises publiques consultées se doivent de mettre en œuvre des processus d'évaluation de leurs fonctions critiques pour identifier les risques structurels et pouvoir assurer la continuité d'activité. Les réponses aux questionnaires font apparaître la prise en compte récente du risque numérique dans sa nouvelle dimension géopolitique ou de vulnérabilité des fournisseurs extra-européens.

Dans les systèmes industriels, les constats sont relativement rassurants. Les systèmes SCADA (dispositifs de conduite des outils industriels) sont généralement fournis par des sociétés européennes et opérés sur des infrastructures dédiées, cloisonnées et largement maîtrisées ; chez Enedis, par exemple, une partie du pilotage du réseau électrique repose sur un SCADA développé par les équipes internes, appuyé sur Red Hat et sur une migration en cours vers OpenStack ou Kubernetes. Pour SNCF Réseau, le logiciel de tracé des sillons est fourni par une société allemande et utilisé par plusieurs autres gestionnaires d'infrastructure européens, ce qui facilite l'interopérabilité transfrontalière

En revanche, les mêmes dépendances que dans l'administration sont relevées pour les applications tertiaires. Microsoft Office 365 est déployé très largement chez l'ensemble des opérateurs, sans perspective concrète de basculement rapide ; les dépendances à VMware et Oracle font cependant l'objet de transitions plus concrètes. Mais surtout, les données concernant les opérateurs de cloud fait apparaître une utilisation préoccupante et systématique de cloud extra-européen. D'une manière générale, les architectures mises en œuvre sont hybrides, avec maintien en interne des applications ou données les plus sensibles et recours au cloud public pour une partie importante des usages moins critiques.

OPERATEURS DE CLOUD DES SIX ENTREPRISES PUBLIQUES INTERROGEES

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

B- Les Entreprises privées : une prise en compte balbutiante, pas d'actions concrètes

S'agissant des entreprises privées, la commission conclut à une prise en compte encore balbutiante des dépendances numériques. La création de l'indice de résilience numérique, en janvier 2026, vise à fournir un outil de mesure du degré de dépendance pour certaines

organisations partenaires : RTE, Docaposte, Caisse des dépôts, CMA-CGM, MAIF, SNCF Aéroports de Paris, Orange et Ouest-France.

Phénomène nouveau, la dépendance à des outils propriétaires clés est désormais identifiée comme un risque majeur compte tenu du contexte géopolitique. On peut considérer que les observations faites dans les administrations sont largement généralisables à l'ensemble des acteurs économiques, en particulier du point de vue du *vendor lock-in*, des hausses tarifaires imposées par les grands éditeurs et de la difficulté à organiser des migrations hors des solutions propriétaires.

Le poids économique de la commande privée, bien supérieur à celui de la commande publique, pourrait leur conférer un rôle important dans la réduction des dépendances systémiques de notre économie. Mais la mise en place d'actions concrètes n'est aujourd'hui pas une priorité pour les entreprises, y compris les plus grandes.

Dans le prolongement des travaux sur l'IRN, la rapporteure propose de compléter cet outil par **l'édiction de grilles d'achat, de cahiers des charges et de clauses types** pour orienter la commande privée vers des solutions dont la souveraineté repose sur des éléments tangibles et renforcer les exigences de réversibilité et d'interopérabilité.

C- Le cas particulier du secteur bancaire et des outils de paiement

Avec le règlement européen Dora (Digital Operational Resilience Act), pour encadrer la résilience opérationnelle numérique du secteur financier, les établissements financiers doivent cartographier l'ensemble de leurs sous-traitants numériques et analyser les risques liés à leur localisation géographique : risque de verrouillage technologique, substituabilité, capacité à maintenir les fonctions critiques en cas de défaillance d'un sous-traitant, concentration des acteurs, possibilités de migrations, interopérabilité, risques liés à l'extraterritorialité du droit.

Dora met en place un cadre européen de surveillance des prestataires dont les services et solutions sont les plus largement répandus parmi les établissements bancaires et financiers. **Dix-neuf prestataires critiques européens** – fournisseurs de services tiers essentiels (CTTP) – ont ainsi été désignés pour la première fois par les autorités européennes de surveillance le 18 novembre 2025. **Parmi eux, onze ont leur siège aux États-Unis, et seulement quatre dans l'Union européenne.** Dans cette même liste se trouvent les trois grands fournisseurs de services cloud – Google Cloud Services, Microsoft et Amazon Web Services –, mais également les fournisseurs de technologie déjà identifiés dans l'analyse des dépendances des administrations – Oracle, IBM, SAP.

L'application du règlement Dora oblige donc les établissements financiers à acquérir une meilleure connaissance de leurs vulnérabilités aux fournisseurs stratégiques du secteur. Elle fournit également des instruments d'analyse prudentielle aux autorités de régulation, qui peuvent s'appuyer sur un recensement sérieux. Mais cela ne constitue que la première étape d'une réduction des dépendances, dont toute la difficulté réside dans la mise en œuvre.

La souveraineté des moyens de paiement : de la protection de la souveraineté des paiements par carte bancaire au développement de nouveaux moyens de paiement

Visa et Mastercard sont en situation d'oligopole, ce qui signifie que 60% des paiements européens ne sont plus souverains. La dépendance à ces réseaux se retrouve aussi dans les paiements transfrontières, faute d'interconnexion entre réseaux nationaux.

La France bénéficie d'une situation singulière grâce au groupement d'intérêt économique (GIE) Cartes Bancaires (CB), système depuis 1984 supervisé par la Banque de France et appuyé sur une filière française complète, de la puce aux terminaux et aux infrastructures de traitement, ce qui garantit une forte souveraineté technique et des données. 95 % des paiements de détail français – carte, cash, mobile – sont domestiques et gérés par CB.

La préservation de la souveraineté sur les moyens de paiement passe également par le développement d'autres technologies souveraines. Dans cinq pays européens, dont la France, la société European payments initiative (EPI) construit une solution de paiement électronique instantané, **Wero**, conçue dès le départ à l'échelle européenne.

Enfin, se prépare également le lancement de **l'euro numérique**. Ce projet, qui est porté par l'Eurosystème (1) et auquel participe activement la Banque de France, consiste à mettre en place un moyen de paiement public utilisable partout dans la zone euro grâce au cours légal et s'appuyant sur une infrastructure de paiement souveraine développée et opérée entièrement par des acteurs européens.

Deuxième partie- La profondeur des vulnérabilités : pertes économiques et risques systémiques pour les personnes et les services publics

Chapitre 3 – Fuites de valeur et gaspillage d'argent public, la contribution des GAFAM à l'économie française

En France, la contribution réelle des grands acteurs américains du numérique (GAFAM et assimilés) a longtemps été peu documentée. Or, **l'essentiel de la valeur ajoutée est créé hors de France, et l'omniprésence de solutions étrangères sur certains segments du marché conduit à restreindre l'espace économique des acteurs nationaux**. La commission d'enquête analyse cette situation à partir de données fiscales (DGFIP), d'études sectorielles (Insee, Banque de France, OMC, Asterès/Cigref) et d'un recensement détaillé des dépenses numériques publiques.

A- Acteurs français et américains du numérique : un déséquilibre flagrant

Secteurs des logiciels : les filiales françaises de Microsoft et Oracle dans le top 5

L'étude Numeum sur les 250 plus grands éditeurs de logiciels français chiffre à 23,1 milliards d'euros le chiffre d'affaires réalisés par les développeurs de logiciels *pure players* en 2024. Le

(1) L'Eurosystème, qui regroupe la Banque centrale européenne et les banques centrales nationales des États membres de l'Union européenne qui ont adopté l'euro, est l'autorité monétaire de la zone euro.

secteur compte 35 sociétés réalisant un chiffre d'affaires supérieur à 100 millions d'euros. Trois d'entre elles ont un chiffre d'affaires supérieur à 1 milliard : Dassault Systèmes (5,6 milliards sur le développement de logiciels et 6,2 milliards au total), Ubisoft (1,9 milliard) et Criteo (1,8 milliard).

Les chiffres d'affaires mondiaux des principaux éditeurs français doivent être comparés aux chiffres réalisés en France par les leaders mondiaux. Microsoft France atteint 4,744 milliards d'euros (2e rang du classement Numeum sur le seul périmètre français), SAP France 1,376 milliard (4e), Oracle France 972 millions (5e), VMWare France 159 millions (25e) et Red Hat 115 millions (33e).

Plateformes en ligne : une domination écrasante de Google, Facebook et Amazon

Le chiffre d'affaires combiné de Google, Facebook et Amazon dans la publicité en ligne en France est de 3,752 milliards d'euros, soit 72 % du chiffre d'affaires total du secteur. Ces éléments illustrent **le poids économique de ces trois acteurs sur le segment des plateformes en ligne, sans aucun acteur français comparable.** Le nombre de salariés associé à l'activité générée en France est faible. Ainsi, **Dailymotion compte 239 salariés pour un chiffre d'affaires réalisé de 54 millions d'euros, soit un ratio de 0,2 million de chiffre d'affaires par salarié. Ce ratio est de 1,8 pour Google France, 2,6 pour Facebook et 4,8 pour Amazon.**

Cloud : OVH, un chiffre d'affaires comparable aux hyperscalers avec un modèle d'affaires opposé

Le marché du cloud (hors SaaS) est très concentré. OVH se distingue par un modèle intégré, avec la conception, production, maintenance et recyclage, en plus de la gestion opérationnelle des data centers, ce qui explique un niveau d'emplois plus de deux fois supérieur à celui de ses concurrents américains pour un chiffre d'affaires comparable.

COMPARAISON DE L'ACTIVITE DES ACTEURS FRANÇAIS ET AMERICAINS DU CLOUD SUR LE PERIMETRE FRANCE

Opérateur de cloud	Chiffre d'affaires (M€)	Nombre de salariés	Résultat du dernier exercice (M€)
Amazon web services EMEA	1 205	817	34
Google Cloud France	803	464	21
OVH	880	2 033	– 23
Scaleway	160	Non disponible	– 36
Outscale	142	Non disponible	28

Source : pour Scaleway, communication financière du groupe Iliad [(2)] ; pour Outscale, comptes sociaux [(3)] ; pour AWS, GCD et OVH, DGFiP (réponse aux questionnaires de la rapporteure).

B- Faible valeur ajoutée, recettes fiscales minimes : les conséquences d'une activité offshore

(2) Iliad URD 2025

(3) Outscale - Comptes sociaux 2025 29-05-2026.pdf

Un taux de valeur ajouté très bas du fait d'une contribution réduite des GAFAM à l'économie

Pour l'ensemble des sociétés américaines identifiées, le taux de valeur ajoutée est toujours bien plus faible que la moyenne du secteur. Pour les plateformes et le cloud (15,3 milliards de chiffre d'affaires, 6,4 milliards de valeur ajoutée, soit 42 % en moyenne) : Google France atteint 26 %, Facebook France 19 %, Amazon Online France 9 %, AWS EMEA 19 % et Google Cloud France 28 %. En comparaison, des acteurs français comme Outscale et OVH atteignent respectivement 65 % et 42 %.

Ces chiffres témoignent d'un modèle économique basé sur l'importation de produits réalisés à l'étranger, avec une faible base d'activité sur le territoire.

Des recettes d'impôts sur les sociétés très faibles compensées par la taxe sur les services numériques

Les informations transmises par la DGFIP révèlent les éléments suivants :

– **les hyperscalers acquittent des montants d'impôts sur les sociétés très faibles** au regard de leur activité

– s'agissant des plateformes en ligne, **le dispositif de taxe sur les services numériques, générant 542 millions d'euros de recettes sur le périmètre des sociétés étudiées, est absolument essentiel** pour assurer des retours pour la puissance publique. Sans cette fiscalité spécifique, le montant d'impôt sur les sociétés acquitté serait également très faible

– le taux de contribution des entreprises de logiciels est plus élevé que celui des acteurs des deux premières catégories.

Le rôle joué par l'Irlande et le Luxembourg

Une étude de la Banque de France révèle que quelques États membres de l'UE concentrent l'essentiel des exportations de services numériques vers la France, et cela dû à l'implantation des sièges européens des grandes plateformes : Airbnb et Amazon au Luxembourg, Meta et Google en Irlande.

L'étude Asterès montre qu'en 2022, sur 25,7 milliards d'euros d'importations françaises de services numériques, 7,4 milliards proviennent d'Irlande et 2,4 milliards des États-Unis. Les documents financiers des filiales françaises de Microsoft, Facebook et Google montrent qu'elles agissent principalement comme agents commerciaux et non comme une société de développement logiciel à proprement parler.

Ces chiffres témoignent d'un modèle dans lequel l'essentiel de la valeur ajoutée est localisée offshore.

C- Dépenses de logiciel : 1,5 milliard d'euros par an au profit des acteurs extra-européens, 1 milliard de dépenses substituables dès aujourd'hui

Le recensement opéré par le gouvernement couvre 2,3 milliards d'euros de dépenses numériques, contre 4,2 milliards évoqués lors des auditions, ce qui confirme son caractère incomplet mais indicatif.

Les fournisseurs extra-européens représentent 19 % des études et conseil et 23 % du développement/maintenance (qui sont les plus gros postes avec 981 millions et 750 millions) ; mais ils **représentent 64 % des logiciels DSI, 90 % des logiciels d'environnement de travail et 59 % des logiciels et services d'IA.**

Au total, les fournisseurs extra-européens captent 29 % des 2,3 milliards recensés (soit 658 millions d'euros), avec une position ultra dominante sur les logiciels support (bureautique, OS, socle) mais une présence plus limitée sur les prestations de services.

Dépenses de logiciel : le très fort positionnement des acteurs extra-européens

Avec les données des administrations d'État, la commission d'enquête a pu constater que les dépenses de logiciels reflètent les dépendances techniques constatées, et sont critiques.

Les produits Microsoft, généralisés auprès de l'ensemble des administrations à l'exception de celles ayant opté pour le logiciel libre, sont à l'origine des dépenses les plus importantes : 115 millions d'euros en 2025.

Moins généralisées, mais néanmoins des dépenses importantes sont les solutions VMWare (34,1), Oracle (23,1), Red Hat (17,1) et IBM (12,6 millions), en achats en 2025.

Par son positionnement auprès de l'ensemble des administrations, l'Ugap dispose d'une vision panoramique des achats numériques. **Parmi les dix principaux fournisseurs de logiciels les plus importants en termes de chiffre d'affaires réalisé auprès de l'UGAP en 2025, 8 sont américains et 2 sont français** : Docaposte et Cegid (actionnaire français, mais avec une localisation de tête de groupe au Luxembourg). **Microsoft se situe en 1ère position avec 293 millions d'euros de chiffre d'affaires en 2025, soit 22 % du total**. Oracle et VMWare représentent 5 % du total, avec respectivement 69 et 61 millions d'euros de chiffre d'affaires.

Au périmètre des **50 principaux fournisseurs**, (au-delà, nous ne disposons pas d'informations fiables sur la nationalité), **la part des logiciels américains était de 81% en 2024 et 79% en 2025,** très proche des 80% auxquels parvenait le cabinet Astérès. Mais il est vrai que les chiffre d'affaires des fournisseurs français auprès de l'Ugap est en forte augmentation.

Des choix contestables au regard des conséquences fortes pour l'administration

La généralisation de solutions propriétaires entraîne le paiement de frais de licences aux sociétés qui les proposent. **Les dépenses logicielles du périmètre État strict sont évaluées à 361 millions d'euros, dont 268 millions d'euros** auprès de fournisseurs extra-européens (74 %).

Pour l'ensemble des administrations (incluant les collectivités territoriales, les établissements publics et les établissements de santé), les chiffres de l'Ugap ne sont pas exhaustifs mais ils permettent cependant de donner une tendance. En 2024, l'UGAP a enregistré 1, 174 milliards d'euros de commandes dans les logiciels, soit une part de marché estimée à 40%. Le montant des achats via l'UGAP auprès des entreprises américaines en 2025 était d'au minimum 609 millions d'euros. Cela aboutit donc à **une estimation globale d'achats minimale de tout ce qui est lié à l'administration auprès des entreprises américaines d'environ 1,5 milliard d'euros**.

Parmi les dépenses réalisées, **les principales solutions concernées disposent d'alternatives en open source** (pour la bureautique, LibreOffice ou les produits de la Dinum ; pour les systèmes d'exploitation, Linux ; pour la virtualisation, Openstack, Proxmox ou Kubernetes ; pour la gestion de bases de données PostgreSQL, Tomca.

Modèle singulier parmi les administrations, **la gendarmerie nationale a procédé à un basculement complet vers des solutions open source**. Elle a ainsi limité son budget annuel de licences pour des solutions propriétaires à un million d'euros, **les économies réalisées au total sont estimées à 534 millions d'euros par an cumulés depuis 2004**.

Les dépenses réalisées auprès du fournisseur Microsoft étant les plus importantes, le choix de produits open source pour la bureautique est le plus à même de dégager des économies importantes. Par exemple, **pour la DGFIP, l'économie générée est de l'ordre de 10 millions d'euros par an.**

Les montants estimés de **dépenses publiques substituables par des solutions open source** étaient sur le périmètre de l'État **a minima de 185 millions** et sur le périmètre de l'ensemble des administrations de **1 milliard d'euros**. Ces recensements n'étant pas exhaustifs, les dépenses publiques évitables sont probablement beaucoup plus importantes.

Impact des choix de solutions logicielles sur la hausse des dépenses numériques

L'analyse des achats de logiciels auprès de l'UGAP entre 2024 et 2025 montre **une hausse des dépenses de licences significative**, bien au-dessus de l'inflation constatée dans les services. Sur les 10 fournisseurs les plus importants (tous à plus de 10 millions d'euros de chiffre d'affaires via l'UGAP), le taux de croissance moyen est de 74 % : +26 % pour Microsoft (de 233 à 293 millions), +113 % pour VMWare (de 29 à 62 millions), +90 % pour Red Hat (de 13 à 25 millions), +138 % pour Salesforce (de 9 à 22 millions), +201 % pour Bureau Van Dijk et +150 % pour Pegasystems. Seul les dépenses pour Oracle baisse de - 29 % (de 97 à 69 millions).

Il y a les pratiques tarifaires qui consistent à augmenter fortement les tarifs à chaque nouvelle version, nouveau contrat, renégociation pluriannuels imposées, mais aussi le sujet de la vente liée (bundling) en incluant sans discussion des produits qui ne sont pas utilisés et demandés, ou des fonctionnalités supplémentaires non nécessaires mais comptabilisés dans le prix.

Du côté des administrations d'État, la comparaison entre 2025 et la moyenne 2023–2025 montre des augmentations de 27 % pour Microsoft, 7 % pour Oracle, 37 % pour VMWare, 46 % pour Red Hat, 24 % pour Sopra HR et 13 % pour SAP. Les témoignages d'organismes comme le CEA, le CNRS ou UniHA confirment des hausses unilatérales de prix, parfois très élevées (+20% à chaque renouvellement avec Microsoft, de 60% jusqu'à +800 % dans le cas de VMWare après le rachat par Broadcom). **Plus un produit propriétaire est intégré au fonctionnement d'une institution ou d'une entreprise, plus la vulnérabilité est grande**.

D- Hausse des prix : une menace croissante pour l'ensemble des entreprises françaises

Les phénomènes observés dans les administrations (inflation des licences, dépendance aux fournisseurs dominants) se retrouvent dans l'ensemble de l'économie française. Une autre étude Asterès/Vanson Bourne de 2022 indique que près de **90 % des entreprises françaises ont subi des hausses de tarifs de 3 à 6 % par an sur les licences,** et que la progression moyenne du coût des **services de cloud-logiciel est de 8,7 % par an** sur les trois dernières années, avec des pics pouvant dépasser 50 % lors de renouvellements.

Les pratiques de *vendor lock-in* (prix d'entrée attractifs, hausses au renouvellement, bundling de fonctionnalités non désirées) limitent la capacité de négociation des administrations et entreprises, qui doivent absorber ces hausses en réduisant d'autres postes (investissement, R&D, recrutements).

La rapporteure conclut que la domination des entreprises extra-européennes dans les logiciels transverses (présents dans tous les systèmes d'information) et le cloud, combinée à ces pratiques tarifaires, **constitue une source majeure de vulnérabilité économique** pour les administrations comme pour les entreprises françaises. Les dépenses vers ces acteurs ne génèrent que très peu d'activité sur le territoire et doivent être considérées, pour l'essentiel, comme **des pertes nettes pour la collectivité**.

Chapitre 4 – Atteintes aux droits des personnes : un modèle fondé sur la captation de l'attention et la monétisation des données personnelles

La domination de grandes entreprises numériques étrangères affecte également la capacité de l'Union européenne à imposer le respect de son droit et le développement de services conformes à ses valeurs.

A- Un hébergement des données personnelles sur le territoire américain, qui expose les citoyens européens à des violations de leur vie privée

Du fait de leur recours aux services des hyperscalers, un volume considérable de données personnelles de citoyens européens se trouvent hébergées dans des centres de données américains, avec un niveau de protection inférieur à celui de l'Union européenne.

Le data privacy framework : un nouveau cadre toujours fragile

Depuis la directive de 1995, les données personnelles de résidents européens ne peuvent être transférées vers un pays tiers que si celui-ci assure un niveau de protection « adéquat », sanctionné par une décision d'adéquation de la Commission Européenne. Dans le cas des États-Unis, trois cadres successifs ont été mis en place et invalidés ou contestés.

En 2022, Joe Biden a adopté *l'Executive Order* 14086 visant à renforcer les garanties entourant les activités de renseignement et à créer un nouveau mécanisme de recours pour les Européens.

Un Civil Liberties Protection Officer, au Bureau du directeur du renseignement national américain, est chargé de traiter les plaintes transmises par les autorités européennes de protection des données et les contestations se feront devant une *Data Protection Review Court* (DPRC), juridiction spécialisée composée de juges fédéraux indépendants.

Sur cette base, la Commission européenne a adopté le 10 juillet 2023 une nouvelle décision d'adéquation dite Data Privacy Framework, considérant que les États-Unis apportaient désormais un niveau de protection substantiellement équivalent à celui de l'UE pour les données transférées dans ce cadre.

Toutefois, le 29 juin dernier, la Cour suprême américaine a rendu sa décision dans l'affaire qui opposait Donald Trump à Rebecca Slaughter, directrice de la Federal Trade Commission (FTC). En validant le limogeage de Rebecca Slaughter, la Cour valide la stratégie présidentielle de politisation des agences d'État indépendantes. Cette décision remet en cause l'indépendance de la DPRC, elle revient donc à rendre caduques les bases sur lesquelles reposaient le Data Privacy Framework (DPF). M. Philippe Latombe, président de la commission d'enquête, a donc saisi par recommandé la présidente de la Commission européenne, afin que le DPF soit immédiatement annulé.

Le président et la rapporteure invitent de toute urgence les entreprises européennes à ne plus utiliser le DPF dans les clauses contractuelles types lors de transfert de données vers les États-Unis. Ils invitent également 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 étatsuniens.

B - Exploitation massive des données personnelles par les géants du numérique

Les géants du numérique (réseaux sociaux, moteurs de recherche, applications) ont construit leur modèle économique sur la collecte et la monétisation de volumes considérables de données personnelles à des fins de publicité ciblée, souvent en contournant le RGPD et la directive e-privacy. **Cette logique de profilage intrusif permet de personnaliser les contenus, de maximiser le temps passé en ligne et d'alimenter une véritable « guerre de l'attention », au détriment des droits fondamentaux.**

Modèle fondé sur la collecte massive de données

Les grandes plateformes ont construit un modèle économique fondé sur la monétisation des données personnelles. Grâce à leur écosystème de services intégrés (moteur de recherche, navigateur, application de géolocalisation, services de messagerie, réseaux sociaux…), Ce ciblage repose principalement sur le dépôt de traceurs, comme les cookies, sur le terminal des utilisateurs, c'est-à-dire des petits fichiers qui permettent de suivre l'activité des internautes en ligne.

Cette accumulation rend possible la construction de profils extrêmement fins, commercialisés auprès des annonceurs, et renforce leur domination sur la chaîne de valeur de la publicité en ligne. Elle permet également de personnaliser l'édition des contenus, au risque de créer des biais discriminatoires ou d'engendrer des pratiques addictives. Ce profilage peut également être mobilisés par des gouvernements pour des dispositifs de surveillance et de limitation des libertés (exemples de communication de messages privés dans des affaires pénales sensibles).

Violations répétées du cadre européen de protection des données

Le RGPD, adopté en 2016, confère aux citoyens européens un contrôle accru sur leurs données : consentement libre et spécifique, droit à l'oubli, portabilité, protection dès la conception. En parallèle, la directive e-privacy demeure applicable pour les cookies et exige un consentement préalable.

Malgré ce cadre, les autorités de protection des données (CNIL, DPC irlandaise, autorités luxembourgeoise, etc.) ont constaté de nombreuses violations : dépôt de cookies sans consentement, impossibilité de refuser aussi facilement que d'accepter, conditionnement de l'accès au service à l'acceptation de cookies (cookie walls), transfert illicite de données vers les États-Unis, défauts de sécurisation des données, paramétrages publics par défaut pour des mineurs. Les sanctions se chiffrent en centaines de millions, voire milliards d'euros (Google, Amazon, Meta, TikTok, Microsoft, Apple, LinkedIn, Shein), mais ne suffisent pas à faire disparaître les pratiques problématiques.

Rien qu'en France, la Cnil a prononcé 953 millions d'euros d'amende, sur le fondement de la directive e-privacy tant les grandes plateformes étrangères bafouent la législation sur les cookies. Cela les a conduit à se mettre en conformité, désormais il est très souvent possible de refuser dès le premier écran.

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

*L'amende initialement prononcée par la Cnil s'élevait à 32 millions. Par un arrêt du 23 décembre 2025, le Conseil d'État a réduit cette amende à 15 millions d'euros.Source : Cnil. https://www.cnil.fr/fr/les-sanctions-prononcees-par-la-cnil

Les autorités ont aussi pointé l'usage systématique de dark patterns (interfaces trompeuses) qui biaisent le consentement : parcours plus long pour refuser, cases pré-cochées, sollicitations répétées, mise en avant des options les plus intrusives. Le DSA interdit désormais ces pratiques, mais leur présence reste massive dans l'écosystème numérique. **La Cnil a développé des applications de sensibilisation destinées au grand public**, issus des travaux de son laboratoire d'innovation numérique. Il existe notamment un site permettant d'apprendre à repérer les apparences trompeuses, **apparences-trompeuses.beta.cnil.fr** et une application adaptée aux mineurs, **FantomApp**, qui permet de vérifier si son mot de passe est robuste, mais également de découvrir comment déposer plainte ou quel est le rôle de la Cnil.

Exploitation des données pour l'entraînement des modèles d'IA

Les grandes plateformes réutilisent les données accumulées (contenus publics, historiques de navigation, localisation, données issues d'appareils connectés et du web scraping/extraction automatique) pour entraîner des modèles d'intelligence artificielle générative, sans cadre stabilisé sur l'application du RGPD à ces usages. Certaines entreprises comme Meta annoncent explicitement l'utilisation des photos et messages publics d'utilisateurs adultes pour l'entraînement, avec une opposition possible seulement via des paramètres de confidentialité. D'autres vont acheter des données de sites web de discussions en ligne, de moteurs de recherche annexes, de plateformes de références nourries par les internautes.

Des chercheur·ses qualifient cette dynamique de « colonialisme des données », en soulignant la captation de ressources issues de financements publics ou de travail bénévole, sans réciprocité ni contribution aux communs numériques. L'entraînement des modèles s'effectue en agrégeant de vastes volumes de données, souvent traitées par des travailleurs peu rémunérés dans les pays du Sud, sans garde-fous suffisants contre les risques d'empoisonnement ou de régurgitation de données personnelles. Max Schrems parle d'un « *tsunami qui aspire toutes les données et les utilise à des fins que nous ne pouvons pas contrôler, et que les entreprises elles-mêmes ne peuvent pas contrôler* ».

C- Un écosystème de captation et de monétisation des données

Une captation massive et opaque des données personnelles, intermédiée par les data brockers

L'enquête réalisée par le journal Le Monde et huit médias partenaires (4), a mis en lumière le rôle central **des courtiers en données** (data brokers), c'est-à-dire les entreprises spécialisées dans la collecte, l'analyse et la revente des données personnelles. Ces courtiers en données achètent et croisent des informations issues de multiples sources : achats en ligne ou en magasin (via les cartes de fidélité), données issues des applications mobiles (localisation, usages), historique de navigation sur internet ou parfois dans le cadre des enchères en temps réel organisées pour attribuer les encarts publicitaires.

Les données collectées peuvent ensuite être croisées et agrégées pour constituer des profils extrêmement fins. Si les informations sont a priori anonymes, il est possible d'identifier très précisément des personnes en recoupant différentes données de géolocalisation avec l'identifiant publicitaire unique associé à chaque terminal. Une fois établis, ces fichiers de données sont vendus à une grande diversité d'acteurs économiques. M. Martin Untersinger décrit l'« **industrie de la surveillance étatique ».** Au-delà du risque manifeste pour la sécurité intérieure, ces profils comprennent également des informations sensibles quant aux convictions religieuses, à l'orientation sexuelle, aux opinions politiques, à l'appartenance syndicale ou au secret médical, **qui peuvent potentiellement être utilisées à des fins répressives ou discriminatoires.**

---

(4) Adrien Sénécat, Martin Untersinger, Elsa Delmas, Léa Girardot et Anne Morel, « Données personnelles en vente libre : les data brokers, une industrie hors de contrôle », Le Monde*, le 12 février 2025.*

En droit, la réutilisation et la revente de données sont strictement encadrées par le RGPD et la loi « informatique et libertés » (information des personnes, consentement pour la publicité et la revente). **En pratique, ces conditions ne sont pas remplies, faute de transparence et de traçabilité dans des chaînes d'intermédiaires complexes, mouvantes et souvent situées en dehors de l'UE**, ce qui rend difficile l'identification des responsables et la mise en œuvre de sanctions. En bout de chaîne, les grandes plateformes demeurent cependant les principaux bénéficiaires, car elles constituent un point incontournable de la monétisation des contenus publicitaires.

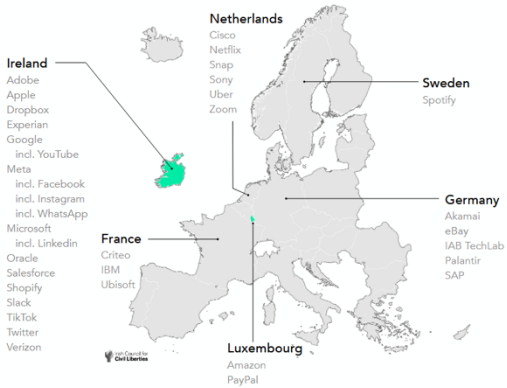
Données de géolocalisation

Les enquêtes sur les « StravaLeaks » (journal Le Monde) et d'autres cas illustrent la sensibilité des données de géolocalisation : des profils publics révèlent les trajectoires quotidiennes d'utilisateurs, permettant d'identifier des bases militaires, des déplacements de porte-avions ou les domiciles de personnels de sécurité. Des applications de rencontres, combinant localisation et informations personnelles, exposent également des militaires en opérations extérieures. Le RGPD impose un consentement spécifique pour la collecte de la géolocalisation lorsqu'elle n'est pas indispensable au fonctionnement de l'application, ainsi qu'un principe de minimisation (géolocalisation approximative lorsque suffisante) et la possibilité de désactiver l'accès aux données dans l'appareil.

Toutefois, l'architecture actuelle repose largement sur une responsabilisation de l'utilisateur, contraint de modifier lui-même des paramètres qui sont par défaut publics (et souvent l'utilisateur l'ignore), ce qui est dénoncé comme une « déresponsabilisation réglementaire ». **Une piste avancée est d'imposer plus systématiquement la désactivation par défaut de l'accès à la géolocalisation et du partage public des informations,** en appliquant concrètement le principe de paramétrage le plus protecteur prévu par l'article 25 du RGPD et détaillé dans les recommandations de la CNIL sur les applications mobiles.

D- Une application inégale du RGPD

Le rôle bloquant de l'Irlande



Le mécanisme de « guichet unique » (article 60 RGPD) prévoit qu'en cas de traitement transfrontalier, l'autorité compétente est celle du pays où se situe l'établissement principal de l'entreprise, ce qui concentre une part importante des plaintes vers l'Irlande, les Pays-Bas et le Luxembourg.

SOURCE : ICCL, 2023. autorites cheffes de file des principales entreprises technologiques.

De nombreuses organisations dénoncent le manque de fermeté de la Data Protection Commission irlandaise, qui recourt largement aux accords amiables, rend peu de décisions, et laisse les dossiers s'accumuler dans le temps. Les ressources de la DPC ont longtemps été insuffisantes au regard de la montée en charge des plaintes, et **les sanctions prononcées sont très peu recouvrées (0,6% des sanctions prononcées de 2020 à 2024 ont été recouvrées)** et du fait de procédures judiciaires longues, coûteuses et suspensives, systématiquement engagées par les grandes plateformes. Des critiques visent aussi le fonctionnement interne de l'autorité (turnover, pantouflage, conflits d'intérêts dans les nominations) dans un contexte où les revenus liés au numérique représentent une part significative du PIB irlandais (35%).

La rapporteure propose de supprimer la règle du guichet unique pour les plus grandes plateformes et de confier au Comité européen de protection des données (CEPD) la compétence de contrôle et de sanction pour les traitements transfrontaliers, afin de surmonter ce « verrou irlandais ».

Des sanctions insuffisamment dissuasives ?

Si le RGPD permet théoriquement des amendes allant jusqu'à 4% du chiffre d'affaires mondial, les sanctions prononcées atteignent rarement ces plafonds, ce qui interroge leur effet dissuasif vis-à-vis de groupes dont les bénéfices se chiffrent en dizaines de milliards. La détermination du montant doit concilier proportionnalité et rôle dissuasif, en tenant compte de la nature et de la gravité de la violation, de sa durée, du caractère délibéré ou non, des catégories de données concernées et des avantages tirés de la violation, comme rappelé par les lignes directrices du CEPD. Dans plusieurs affaires transfrontalières, la procédure de résolution des litiges (article 65 RGPD) a permis au CEPD d'imposer des relèvements substantiels des amendes initialement envisagées par l'autorité irlandaise, notamment dans le cas du transfert de données par Meta vers les États-Unis.

Chapitre 5- Espionnages et pressions sur les personnalités politiques, les menaces stratégiques dans un contexte de montée des tensions géopolitiques

A- Un risque d'espionnage industriel ou politique

Henri Verdier qualifie cet espionnage de « systématique », en soulignant que le cadre juridique des États-Unis permet aux administrations d'accéder aux données relevant de leur juridiction, tandis qu'en Chine, c'est « un sport national ». Cette situation expose l'Europe, en cas de conflit, à des risques majeurs d'accès à ses données sensibles et à des opérations de manipulation de l'information.

Des produits extra-européens soumis aux législations extraterritoriales

Des législations américaines à portée extraterritoriale obligent de fait les fournisseurs de cloud immatriculés aux États-Unis à communiquer aux autorités américaines les données qu'ils hébergent, indépendamment du lieu de stockage : Le Foreign Intelligence Surveillance Act (FISA), le Cloud Act. Des données de citoyens européens peuvent ainsi être transmises sans notification, en dehors du contrôle des administrations et tribunaux européens.

En Chine, la loi sur le renseignement national impose aux organisations et citoyens de « soutenir, assister et coopérer » avec les services de renseignement, ce qui peut conduire les entreprises chinoises à transmettre des données de citoyens européens qu'elles détiennent.

L'application de ces droits extraterritoriaux constitue une menace directe pour la souveraineté et l'intelligence économique européennes. Les services de renseignement de pays tiers peuvent accéder à des données sensibles d'États, à des secrets industriels d'entreprises stratégiques ou à des résultats de recherche de pointe hébergés sur des infrastructures étrangères.

En pratique des garanties juridiques et techniques insuffisantes pour supprimer le risque de divulgation des données.

Lors de leurs auditions, Microsoft, Amazon Web Services et Google ont affirmé vérifier la légalité des demandes d'accès, les contester systématiquement ou les rediriger vers leurs clients. Mais Microsoft a du reconnaitre avoir transmis les informations d'au moins une entreprises européenne.

Les rapports de transparence font état de milliers de demandes gouvernementales. **Le gouvernement américain a ainsi formulé a minima : 444 demande à AWS ; 5 587 à Microsoft dont 75% ont donné lieu à la transmission d'informations (de données stockées ou de métadonnées) ; 60 000 demandes à Google et dans 89% des cas les informations ont été divulguées.**

Dès lors, la seule véritable garantie de protection des données contre les risques de transferts à des États tiers consiste à assurer que le fournisseur de cloud soit uniquement soumis au droit européen.

Le référentiel SecNumCloud vise précisément à garantir l'immunité au droit extraterritorial en fixant des exigences capitalistiques, techniques et organisationnelles : siège dans l'Union européenne, limites de détention du capital par des entités extra-européennes, absence de droits de veto ou de contrôle majoritaire par ces entités, autonomie d'exploitation de la solution et impossibilité d'accès aux données pour des sous-traitants non européens.

B- La menace d'une coupure des services numériques

Le durcissement des relations transatlantiques oblige à envisager l'hypothèse qu'une décision du président américain impose **une coupure, générale ou ciblée, des services numériques** fournis à l'Union européenne.

Le ciblage de personnalité : le cas du juge Guillou, un exemple qui pourrait se systématiser

L'*executive order* 14203, pris à l'encontre de juge de la Cour pénale internationale (CPI) réaction aux enquêtes de la Cour pénale internationale (CPI), prévoit les sanctions suivantes : interdiction de territoire américain, gel des avoirs et interdiction pour toute personne ou entité américaine de leur fournir biens et services, et ce sans recours juridictionnel.

Le juge Nicolas Guillou, l'un des juges ciblés par cette décision, décrit sa vie personnelle comme un « *laboratoire de la perte de souveraineté* ». Il s'est vu privé de nombreuses des fonctions suivantes : blocage ou la résiliation des comptes Apple, iCloud, Amazon et PayPal. Idem pour Google et ses services. Les personnes sanctionnées ne sont pas prévenues et perdent

immédiatement leurs archives sur le cloud. Les positions de Microsoft ont varié entre obligations juridiques et protection du modèle économique.

Pire, il y a également eu retrait des moyens de paiement et des prestations d'assurances, et le juge s'est vu refuser toute nouvelle carte bancaire, les banques craignant d'avoir des clients sous sanctions américaines, en raison des opérations de marché réalisées en dollar.

La situation du juge révèle des comportements de **surconformité (*over-compliance*) d'acteurs européens**, bancaires et assurantiels, qui appliquent par précaution des mesures extraterritoriales même sans lien juridique direct avec les États-Unis, au détriment des droits de leurs propres assurés et clients. S'ajoute à cela une regrettable **inaction de l'Union européenne** qui n'a pas activé le règlement de blocage de 1996 pour neutraliser les effets extraterritoriaux de ces sanctions.

Le juge Guillou met en garde contre la généralisation potentiel de ces sanctions ciblées, qui pourraient peser sur procureurs, juges, avocats, parlementaires ou fonctionnaires européens chargés d'appliquer le DMA et le DSA, les dissuadant de prendre certaines décisions. Cette logique de peur évoque le fonctionnement de la justice dans des régimes autoritaires, où les magistrats anticipent les attentes du pouvoir plutôt que d'appliquer le droit, constituant un risque fondamental pour l'État de droit en Europe.

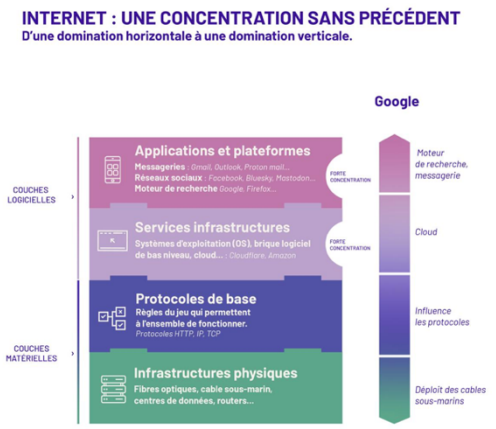
Une coupure générale des services numériques : un scénario critique qui doit être préparé

La politique extérieure actuelle de l'administration américaine rend crédible le scénario de *kill switch* généralisé : une coupure des services numériques fournis par des entreprises américaines à l'Europe au moyen de mesures de contrôle des exportations. Cette coupure pourrait interrompre le support, la maintenance et la vente de ventes de logiciels, l'accès aux applications, aux réseaux sociaux, aux services mails et de messages instantanées, aux données hébergées sur des clouds américains, aux sites hébergés aux USA, aux paiements par Visa ou Master Card…, paralysant une part importante de l'économie européenne. Si les grandes entreprises numériques assurent qu'un *kill switch* serait contraire à leurs intérêts économiques, leur marge de manœuvre face à une injonction de l'administration fédérale sont faibles.
Or, aucune des mesures techniques ou contractuelles proposées par les *hyperscalers* (cloud dit souverain et opéré par du personnel européen, clauses de préavis de douze mois,…) n'élimine totalement le risque. Les infrastructures numériques reposent sur un flux continu de mises à jour de sécurité. Et cela est d'autant plus important dans un moment où le nombre de vulnérabilités détectées progresse fortement et qu'une part importante est exploitée dès leur publication. Cet état de fait qui rend difficilement crédible le maintien d'un niveau de sécurité acceptable sur plusieurs trimestres sans mises à jour. Les solutions hybrides - exploitées par un opérateur européen mais reposant sur une technologie américaine, solutions qui peuvent obtenir une certification SecNumCloud - apparaissent particulièrement exposées, et la rapporteure s'interroge sur leur capacité à garantir une sécurité optimale en cas d'interruption prolongée des mises à jour

Troisième partie – Les causes d'un enracinement profond

Chapitre 6 - Le droit à la concurrence : toujours un temps de de retard

A- Les GAFAM : des positions de domination grâce à la maîtrise de l'ensemble de la stack du numérique et l'effet cumulatif de cette intégration



Francesca Musiani souligne que chacune de ces couches est théoriquement gouvernée par des acteurs différents, mais qu'on observe désormais une concentration de pouvoir avec une montée en puissance de grandes entreprises privées comme Google et Meta, qui investissent massivement dans les infrastructures physiques. Cette concentration est à la fois horizontale (au sein de chaque couche) et verticale (entre les couches), créant des positions ultradominantes pour les GAFAM.

B- Le droit de la concurrence européen et français face aux GAFAM : des sanctions multiples et 17 milliards d'euros d'amendes au total

Les vingt-six sanctions envers les GAFAM au titre du droit de la concurrence depuis 2010.

Pour Google (Alphabet), douze sanctions dont huit avec amendes, pour un total de 12,1 milliards d'euros ; pour Apple, six sanctions dont quatre avec amendes (3,6 milliards d'euros) ; pour Meta, trois sanctions dont deux avec amendes (998 millions d'euros) ; pour Microsoft, trois sanctions dont une avec amende (561 millions d'euros) ; pour Amazon, deux sanctions, principalement sous forme d'engagements obligatoires.

Au total, les amendes atteignent 17,2 milliards d'euros, complétées par des injonctions et engagements sur l'interopérabilité, la transparence, la limitation des offres groupées et l'arrêt de certaines pratiques (par exemple, l'interdiction pour Amazon d'utiliser les données non publiques des vendeurs tiers, ou le découplage de Teams de la suite Office 365). La logique est toujours la même : self-preferencing, blocage ou pénalisation des concurrents, monopole de certains standards et conditions contractuelles inéquitables.

Le cloud : l'intérêt de mesures ciblées pour faire cesser les pratiques problématiques

Une enquête sectorielle de l'Autorité de la concurrence sur le cloud a mis en lumière en 2023 la prédominance de trois acteurs – AWS, Google Cloud et Microsoft Azure – et un verrouillage constant. Certains acteurs appliquent désormais la gratuité de la sortie de données donc l'encadrement réglementaire peut produire des effets correcteurs rapides, mais en revanche le décret issu de la loi Sren, pour plafonner et encadrer à un an la durée des crédit cloud abusifs, n'a jamais été publié.

Mais l'application du droit de la concurrence n'est pas toujours possible : il n'est pas aisé de prouver qu'il y a abus de position, préjudice pour le consommateur, et la Big Tech se partagent à 4 ou 5, 80% du marché dans toutes les couches. Mais surtout il y a un déséquilibre de moyens : les ressources humaines et financières des autorités de concurrence sont très inférieures à celles des grandes entreprises, ce qui rend les procédures longues, coûteuses et fragiles face à des équipes juridiques très puissantes.

C- Le DMA, nouveau règlement européen, l'introduction de mesures de régulation ex acte applicables aux principales plateformes

Le DMA (Digital Market Act) est une réponse pour agir rapidement contre certaines pratiques des grandes plateformes, dans un environnement où la vitesse d'évolution des technologies rend l'action ex post trop lente et partielle. Les obligations du DMA reprennent, sous forme de règles ex ante, des pratiques déjà sanctionnées par les autorités antitrust : exigence d'interopérabilité, interdiction du self-preferencing, limitations aux ventes liées et aux groupages, contrainte sur la combinaison de données personnelles entre services, portabilité renforcée des données. Les premières décisions visent Apple (500 millions d'euros) et Meta (200 millions d'euros). La mise en œuvre du DMA a déjà modifié le comportement des *gatekeepers*, en ouvrant des opportunités pour des acteurs alternatifs (autres navigateurs et moteurs de recherche, boutiques d'applications tierces, services de messagerie interopérables, développeurs PME intégrant les API des plateformes) et pour l'autonomie des utilisateurs finaux (capacité à désinstaller les applications par défaut, choix élargi de services, contrôle accru sur le partage de leurs données entre services, portabilité facilitée des données).

Chapitre 7 - Le narratif de l'absence d'alternative européenne

Le discours largement répandu est qu'il n'existerait pas d'alternative européenne crédible aux grands fournisseurs américains contribue à enfermer les choix publics et privés dans un horizon dominé par les hyperscalers, et à empêcher une évaluation actualisée des offres européennes qui sont de qualité et tout à fait capables de répondre aux besoins.

A- Un discours constant de résignation

Les solutions américaines seraient incontournables pour des raisons de performance, de prix, de richesse fonctionnelle, d'écosystème et de capacité d'innovation. Les témoignages évoquent une quasi-automatisme dans les choix de cloud public, où AWS, Azure et Google Cloud sont considérés comme la norme, tandis que les offres françaises ou européennes, même qualifiées SecNumCloud, sont perçues comme des solutions marginales ou de niche. Pourtant, des acteurs industriels et des responsables d'infrastructures critiques soulignent qu'ils utilisent déjà des solutions qualifiées SecNumCloud ou des clouds européens pour des charges de travail

sensibles, avec des niveaux de sécurité et de performance compatibles avec leurs exigences, et des coûts qui ne sont supérieurs (souvent même inférieurs).

En la matière, la France peut se prévaloir d'acteurs d'envergure nationale tels que OVHcloud, Scaleway, Cloud Temple ou Outscale, qui ont démontré leur capacité à répondre aux besoins des administrations et des entreprises. L'offre de solutions qualifiées SecNumCloud s'est étoffée, avec l'émergence de services d'orchestration de conteneurs managé. Les personnes auditionnées ont également démenti l'idée selon laquelle les offres européennes seraient plus coûteuses que celles des hyperscalers.

B- Des passeurs de technologie : le rôle des cabinets de conseil et des centrales d'achat.

Les grandes entreprises numériques extra-européennes peuvent s'appuyer sur tout un écosystème pour diffuser les usages de leurs technologies, ceux qualifiés par Ophélie Coelho de « passeurs de technologie ». Les entreprises de service numérique (ESN) recommandent en priorité et parfois systématiquement les solutions américaines, et ainsi contribuent grandement à perpétuer ces dominations sur le marché. L'exemple de Capgemini : En 2025, Capgemini a réalisé 588 millions de chiffre d'affaires avec le secteur public. Or, Capgemini a des partenariats stratégiques avec Microsoft, AWS et Google pour accompagner ses clients dans l'adoption de ces technologies, mais contribue très peu au développement de solutions européennes. **La rapporteure relève pourtant que les ESN perçoivent un montant de crédit d'impôt recherche (CIR) très important, bien supérieur à celui que reçoivent de jeunes entreprises technologiques innovantes. À elles deux, les sociétés Capgemini et Sopra Steria ont obtenu cinquante fois plus de CIR que Mistral AI en 2025.**

Les **centrales d'achat publiques** ont un rôle structurant : leur poids dans la commande publique numérique leur confère un rôle déterminant dans l'orientation de la demande. En 2025, ce sont plus de 2,6 milliards d'euros d'achats numériques – matériels, logiciels, services, cloud, télécommunications – qui ont été réalisés par le biais de l'Ugap. L'offre de l'Ugap a longtemps reflété la domination des acteurs étatsuniens sur le marché, mais la centrale a amorcé un changement, et permet maintenant d'identifier les solutions logicielles françaises et européennes, les conditions d'hébergement et de traitement des données, ainsi que les qualifications et référentiels applicables. Cependant, la rapporteure a constaté que l'Ugap avait retenu une méthodologie défaillante, en retenant le seul critère de la localisation de la maison mère mondiale, et a donc classé les logiciels américains VMware ou Zoom comme français sur son marché multi-éditeurs, faisant preuve d'une certaine forme de « sovereignity washing ».

C- Une dépendance culturelle forgée dès l'école

La dépendance aux solutions américaines se construit dès l'école, via les environnements bureautiques et pédagogiques principalement de Microsoft, fournis via l'Éducation ou les collectivités, et qui façonnent les pratiques des élèves et des enseignants, jusqu'au niveau universitaire.

En 2025, le ministère de l'éducation nationale a reconduit pour quatre ans l'accord-cadre qui le lie à Microsoft pour l'utilisation des logiciels et solutions bureautiques installés sur près d'un million de postes de travail et de serveurs au sein du ministère, des organismes de recherche,

des universités et des écoles supérieures, pour un montant maximal de 152 millions d'euros (5), dont 2,4 millions par an pour les services centraux et déconcentrés du ministère. Les établissements scolaires, les enseignants et les élèves sont, pour leur part, équipés par les collectivités locales, sans doctrine claire pour privilégier des logiciels français ou européens.

Cette acculturation précoce crée des habitudes enracinées chez les utilisateurs mais aussi les futurs décideurs. L'adhérence est particulièrement forte parmi les DSI, et elle est entretenue par la mainmise des hyperscalers sur les offres de formation continue.

D- La plateforme des données de santé : une double émancipation de Microsoft et des cabinets de conseil

Voici un cas emblématique d'un écosystème qui favorise l'enfermement dans des solutions américaines. Le Health Data Hub avait vocation à organiser et mettre à disposition les données issues du système national des données de santé (SNDS), à des fins de recherche et d'innovation. Malgré la grande sensibilité des données traitées, le ministère de la santé a fait le choix d'héberger la plateforme sur Microsoft Azure, considérant qu'elle était la seule avec les fonctionnalités et certifications de sécurité requises. Sans appels d'offres, ni mise en concurrence, mais avec un rôle important des cabinets de conseil pour un coût estimé à 10 millions d'euros sur l'ensemble du processus (conception, préparation des réunions, formalisation des spécifications).

Avec la loi Sren, a été acté la migration de la Plateforme des données de santé vers une solution d'hébergement souveraine. Malgré de multiples alertes, c'est seulement en février 2026 qu'a été engagé la migration de la PDS vers une solution souveraine définitive. Cette bascule de la PDS vers un opérateur de cloud français envoie un signal fort quant à l'existence d'offres d'hébergement souveraines solides, capables de répondre pleinement aux demandes de grandes entités publiques ou privées.

Chapitre 8 - La politique du numérique : la grande absente des débats politiques

A- Un État désarmé par l'externalisation des compétences numériques

Les taux d'externalisation des compétences informatiques sont élevés et très variables selon les ministères, avec des niveaux de 10% à 80 % sur certaines fonctions critiques. Au-delà de 60 % d'externalisation, la situation est jugée risquée, et au-delà de 80 %, « non maîtrisable ». Le manque de compétences internes pousse les administrations à privilégier des solutions « packagées » de grandes entreprises numériques, plutôt que des technologies souveraines ou libres nécessitant une exploitation et un développement en interne.

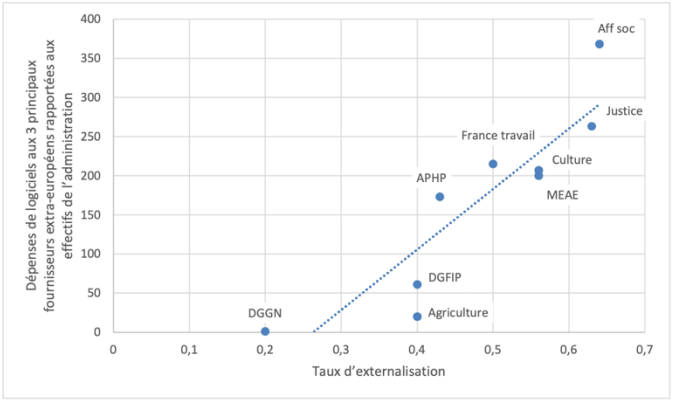
(5) Réponse du ministère de l'éducation nationale, publiée le 28 octobre 2025, à la question écrite n° 5312 de M. Philippe Latombe.

Une répartition très inégale des ressources humaines numériques qui reflète des stratégies ministérielles fragmenté

Les chiffres rassemblés mettent en évidence de fortes disparités avec quelques ministères qui disposent d'une filière numérique dédié. Ainsi, la Direction générale de la gendarmerie nationale (DGGN), la Direction générale de la police nationale (DGPN) et les ministères économiques et financiers se distinguent par leur plus grand recours à des développements internes. Les deux ministères conjuguent des impératifs forts de garantie d'indépendance et de confidentialité et des choix stratégiques réalisés en matière d'internationalisation des ressources de développement.

A l'inverse, certaines administrations sont contraintes d'externaliser toute la gestion de leur SI. Dans les ministères sociaux, les applications développées en interne représentent moins de 3 % du parc applicatif, si bien que 97 % des fonctions de développement sont externalisées ; au ministère de la Justice, la direction du numérique dispose de moins d'une vingtaine de développeurs et dépense 200 millions d'euros par an en prestations intellectuelles informatiques (équivalent à 1500 ETP).

DÉPENDANCE DES ADMINISTRATIONS À L'ÉGARD DE FOURNISSEURS DE LOGICIELS EXTRA-EUROPÉENS EN FONCTION DE LEUR TAUX D'EXTERNALISATION



**Les dépenses moyennes annuelles par agent sont calculées pour chaque administration en se fondant sur le plafond des autorisations d'emploi pour l'État en 2025 (article 144 de la loi de finances pour 2025)*

***Le ministère de l'éducation nationale n'a pas été retenu dans le périmètre car les personnels enseignants sont équipés par les collectivités locales. Les données les ministères économiques et financiers ou les caisses de sécurité sociale, n'ont pas non plus été traitées faute de disposer des données suffisantes.*

Source : commission d'enquête à partir des réponses écrites des administrations.

Souvent, l'État apparaît comme dessaisi des compétences de développement et de conception ; certains DSI ministériels comptent plusieurs centaines de personnes, mais très peu de développeurs, ce qui renforce une culture de l'« achat de solutions » au détriment de la capacité à coder et architecturer les systèmes d'information. L''administration perd la capacité même de concevoir un basculement vers d'autres solutions et de remettre en cause des contrats coûteux et peu sécurisés.

Un effort de réinternalisation des compétences à peine amorcé et déjà suspendu

Un rapport de l'Inspection générale des finances (IGF) et du Conseil général de l'économie (CGE) a recommandé en 2023 un effort de réinternalisation avec la création de 3 500 postes numériques supplémentaires d'ici 2028 dans les ministères civils, notamment en direction de projet, maîtrise d'ouvrage, chefferie de produit et architecture.

En 2024, ont été ouverts 345 ETP supplémentaires, permettant par exemple au ministère de l'éducation de réduire des taux d'externalisation jugés dangereux et au ministère de la justice de retrouver une maîtrise d'ouvrage systématiquement internalisée, et cela aurait généré une économie nette de 18,3 millions d'euros en 2025. Cependant, ces efforts sont restés limités, les ministères sociaux n'ont bénéficié que de renforts marginaux.

B- L'ébauche d'une stratégie de souveraineté numérique, sans véritable pilotage interministériel.

Depuis 2023, la Dinum a pour mission la préservation de la souveraineté numérique comme axe prioritaire, et trois leviers : prescriptions pour orienter les choix technologiques, animation interministérielle et développement de briques technologiques mutualisées (clouds internes, outils bureautiques). Mais elle n'a pas d'autorité hiérarchique sur les directions numériques ministérielles

Des exigences de souveraineté aisément contournées

Le principal outil de contrôle de la Dinum est la procédure d'audit des grands projets numériques de l'État, qui impose un avis conforme pour les projets au-delà d'un certain seuil financier, avec consultation de l'Anssi et de la direction du budget. La Dinum s'est efforcée d'utiliser ce dispositif pour identifier les dépendances technologiques et recommander des architectures alternatives, mais elle ne peut se prononcer sur le choix final des prestataires. De plus, jusqu'à mars 2026, les opérateurs de l'État n'étaient pas soumis à avis conforme. Et l'obligation de saisir la Dinum est fréquemment contournée : refus de soumettre le projet ou avis défavorable non pris en compte, et donc cela n'empêche pas la poursuite de projets fortement externalisés et hébergés sur des clouds commerciaux non conformes.

Une mutualisation inachevée de solutions numérique souveraines

La stratégie numérique de l'État fait du déploiement de produits numériques interministériels le principal levier de reprise en main des systèmes d'information, en misant sur des outils de cloud et de collaboration mutualisés pour réduire la dépendance aux suites propriétaires étrangères. La doctrine « Cloud au centre » a rationalisé les infrastructures d'hébergement autour de deux offres de cloud interministériel : Pi (porté par le ministère de l'intérieur, basé sur OpenShift) et Nubo (porté par la DGFIP, basé sur OpenStack et des briques open source). Ces clouds ont vocation à héberger les systèmes d'information les plus sensibles, avec un niveau de sécurité comparable aux offres commerciales certifiées SecNumCloud. Mais Pi et Nubo restent peu utilisés par l'ensemble des ministères. La Dinum reconnaît la nécessité de réviser les tarifs. Des travaux sont aussi engagés pour enrichir les fonctionnalités et rapprocher les deux clouds afin de renforcer l'interopérabilité et la résilience, ce qui pourrait faciliter des migrations majeures comme l'hébergement des SI du ministère de la justice sur Pi.

Les produits numériques interministériels au défi d'une généralisation à l'ensemble de l'État

La Dinum développe également des produits opérationnels (Réseau interministériel de l'État, FranceConnect, data.gouv.fr) ainsi qu'une suite bureautique souveraine : La Suite numérique, qui rassemble des outils de messagerie instantanée (Tchap), visioconférence (Visio), transfert de fichiers (FranceTransfert), messagerie électronique (Messagerie), stockage et partage de documents (Fichiers), et des briques collaboratives en expérimentation (Docs, Grist). L'adoption s'est nettement accélérée : en 2026, Tchap compte plus de 420 000 utilisateurs actifs mensuels, Visio plus de 200 000 participants mensuels, et FranceConnect 44 millions d'usagers. Les retours des ministères soulignent la qualité, la sécurité et l'adéquation fonctionnelle des outils, qui commencent à se substituer à des solutions américaines comme Zoom, Webex ou Teams. La Suite est ainsi perçue comme un levier crédible de réduction des dépendances à Office 365 et aux suites collaboratives des hyperscalers. Des limites subsistent toutefois : incompatibilités avec certains systèmes informatiques, absence d'outil intégré pour les diapositives, contraintes de passage à l'échelle (par exemple, impossibilité d'organiser des réunions de plus de 1 000 participants). La Dinum adopte une démarche de type « lean

start-up », privilégiant d'abord l'impact utilisateur puis l'industrialisation mais il faut être vigilant pour éviter les changements de stratégie qui déstabilisent les déploiements, comme cela avait déjà été le cas avec des outils précédemment conçus par l'Etat. En avril 2026 a été créé l'Ariane, Autorité du numérique et de l'intelligence artificielle de l'État, chargée de définir des standards communs, piloter les infrastructures stratégiques, et coordonner les partenariats technologiques.

Chapitre 9 - Le lobbying : des moyens massifs, le combat en passe d'être gagné pour l'abolition de la régulation

A- Un lobbying féroce

Les grandes entreprises numériques extra-européennes, en particulier les GAFAM, déploient des moyens humains et financiers considérables pour influencer la régulation européenne et nationale, et les montants vont croissant depuis 2021. En 2025, dix entreprises ont dépensé 49 millions d'euros en lobbying auprès des institutions européennes, dont **35 millions pour les seuls GAFAM**, dépassant les montants investis par les secteurs de la pharmacie, de la finance ou de l'automobile. **Ces entreprises mobilisent un réseau dense de 210 lobbyistes, ce qui se traduit par plus d'une réunion par jour ouvré avec la Commission et de nombreux contacts avec le Parlement.** Ce lobbying vise principalement à contenir ou détricoter les réglementations numériques (DSA, DMA, loi SREN), en pesant sur les autorités de régulation (Arcom, Autorité de la concurrence, Arcep) et en exploitant une nouvelle dynamique de dérégulation à Bruxelles.

Les États-Unis interviennent aussi directement pour défendre les intérêts de leurs entreprises : les pressions de l'administration américaine ont fort probablement contribué à l'abandon des critères d'immunité aux lois extraterritoriales dans le projet européen de certification cloud EUCS.

B- L'omnibus numérique : un recul de la régulation européenne qui donne satisfaction aux big tech

La Commission européenne a présenté, en novembre 2025, un paquet législatif de « simplification » des normes numériques, comprenant une proposition de règlement dit omnibus numérique, qui modifie notamment le RGPD et le droit des données. Si le discours officiel insiste sur des « modifications ciblées » pour simplifier le cadre existant sans réduire la protection, plusieurs dispositions opèrent en réalité des changements pour affaiblir la protection des données personnelles et des droits fondamentaux.

L'introduction de failles béantes dans la protection des données personnelles

L'omnibus propose de redéfinir la notion de données à caractère personnel pour exclure les données pseudonymisées du champ du RGPD. Les experts auditionnés (Max Schrems, Cnil, autorités européennes de protection des données) estiment que le texte proposé va bien au-delà

de la jurisprudence de la Cour de Justice de l'Union Européenne, en introduisant un relativisme dangereux, ouvrant la voie à ce que des jeux de données très révélateurs (par exemple des séries de géolocalisation horodatées permettant de déduire la religion, les habitudes ou la vulnérabilité d'individus) soient traités comme anonymes. Elles échapperaient alors aux garanties du RGPD, malgré des risques physiques ou sociaux sérieux pour les personnes concernées.

Par ailleurs, l'omnibus fragilise plusieurs droits clés : la définition de la « recherche scientifique » est étendue de manière très large, y compris pour des travaux poursuivant un intérêt commercial, ce qui augmenterait les possibilités de déroger aux droits d'accès, d'information, d'opposition et d'effacement des personnes. Les responsables de traitement pourraient refuser ou facturer les demandes jugées « excessives » selon leur bon vouloir. L'omnibus introduit également un nouvel article destiné à faciliter le traitement de données personnelles pour l'entraînement et l'exploitation des systèmes d'IA, en fondant ce traitement sur l'« intérêt légitime » des responsables, très loin de la notion de proportionnalité posé par la jurisprudence. **Le risque est de transformer une base légale exigeante en blanc-seing pour l'exploitation massive de données, sans garanties suffisantes en matière de minimisation, anonymisation et respect effectif des droits d'opposition ou d'effacement.**

L'intégration de la régulation des cookies dans le RGPD: une perte de contrôle pour la CNIL

L'omnibus porte une profonde refonte des règles applicables au dépôt de traceurs dans l'objectif de simplifier leur mise en œuvre et de lutter contre la « fatigue des cookies » des utilisateurs confrontés à la multiplication des bandeaux de consentement. Il est proposé que le traitement des données à caractère personnel stockées sur des équipements terminaux soit uniquement régi par le RGPD, et non plus par la directive e-privacy Cette fusion apparaît éminemment problématique, en ce que le respect en France des règles sur les cookies par les plus grandes plateformes numériques ne relèverait plus de la Cnil, mais des trois autorités de protection des données dont la supervision s'est montrée défaillante s'agissant du RGPD (irlandaise, luxembourgeoise, néerlandaise). Il en résulterait également une perte de recettes significative pour la France. **Sur les 953 millions d'euros d'amendes prononcées par la Cnil depuis 2020, 903 millions l'ont été à l'encontre de grandes entreprises qui n'ont pas leur siège en France**. L'omnibus prévoit, en outre, de larges exceptions à l'obligation de recueil du consentement pour placer des traceurs ou accéder aux informations stockées dans les équipements terminaux.

Une simplification manquée et un énorme cadeau aux Big Tech

Toutes ces modifications risquent vraiment d'accroître la complexité juridique pour les PME, au lieu d'alléger les charges administratives pesant sur les petites entreprises. L'utilisation d'expressions vagues « accroissement des connaissances et du bien-être généraux de la société » ou « motifs raisonnables de croire » renforce l'insécurité juridique au lieu d'apporter de la stabilité. Et le nombre de dérogations, de critères et donc de formulaires à remplir s'est amplifié. Les entreprises qui gagnent à la flexibilité du droit sont celles de la Big Tech car elles ont des armées d'avocats spécialisés. Les grandes plateformes extra-européennes seront aussi mieux placées pour profiter de l'affaiblissement de la protection des données personnelles, en raison du volume de données qu'elles collectent et traitent à travers leurs services de moteur de recherche ou de réseau social, et pourront tirer profit des possibilités offertes par l'omnibus en matière d'IA. L'omnibus numérique va ainsi renforcer la position dominante des grandes plateformes, en accélérant la concentration des données à leur profit.

D'ailleurs la proposition de la Commission européenne porte l'empreinte du lobbying des grandes plateformes extra-européennes. **Une étude conduite par les ONG Corporate Europe Observatory (CEO) et Lobby Control révèle que de nombreux amendements proposés par la Commission répondent directement à des demandes formulées par les Gafam**. Plusieurs experts dénoncent une perte d'expertise au sein des services chargés de rédiger ces textes, et la commission d'enquête appelle le gouvernement français à s'opposer fermement, au Conseil de l'Union européenne, à toute modification du RGPD.

Chapitre 10 – Le financement des entreprises numériques : la chasse à la licorne

Le financement apparaît comme un facteur décisif pour expliquer le retard des entreprises européennes du numérique par rapport à leurs homologues américaines.

A- Les trois moteurs du financement des entreprises numériques étatsuniennes : commande publique, marché unifié, venture capital

Aux États-Unis, la dépense militaire et la reconversion du complexe militaro-industriel vers le numérique ont constitué une source massive de financements pour les technologies, notamment via la commande publique (Darpa, Small Business Act, Buy American Act, Chips and Science Act). Le gouvernement américain est tenu d'acheter au moins 23% de ses volumes à des petites entreprises. Le second moteur est l'accès immédiat à un marché homogène de plus de 300 millions de consommateurs, avec une langue unique et une régulation uniformisée. Ce marché permet d'atteindre rapidement une taille critique, d'amortir les investissements et de financer une croissance rapide, alors qu'en Europe la fragmentation juridique, linguistique et sociale impose aux entreprises de reproduire des démarches complexes pays par pays, ce qui ralentit leur passage à l'échelle. Enfin, l'écosystème américain de capital-risque et de marchés financiers (fonds de pension, fonds spécialisés, IPO) est dimensionné pour financer des entreprises en forte croissance et racheter rapidement des start-up à des valorisations élevées.

B - En Europe, la commande publique : un instrument encore mal mobilisé

La préférence française ou européenne n'est pas compatible avec les règles applicables car la commande publique est encadrée par l'Accord sur les marchés publics de l'OMC (AMP), sauf exceptions (défense, sécurité, certains pays). Cette impossibilité d'utiliser un critère de préférence européenne est un premier handicap. De plus, les start-up et ETI du numérique restent peu présentes dans les achats publics en France, malgré une progression récente (de 1,7 à 2,3 milliards d'euros d'achats publics entre 2022 et 2023, mais cela reste une faible part). Or, le tissu économique du logiciel français est composé de peu de grandes entreprises. 49 % des entreprises numériques ne réalisent pas de chiffre d'affaires avec des administrations, et encore moins avec les ministères, surtout avec les collectivités territoriales. Les entreprises dénoncent la longueur des cycles de vente et de paiement, qui pèse sur leur trésorerie, tandis que les administrations s'inquiètent des capacités industrielles et de la pérennité de structures de petite taille, ce qui limite la possibilité de faire de la commande publique un véritable tremplin.

C- Les prises de participation dans les entreprises du numérique : le risque de la naïveté

L'Europe souffre d'un marché des capitaux fragmenté et insuffisant, ce qui rend difficiles les financements au-delà de 100 millions d'euros. Le financement manque pour la phase dite de scale-up, pour l'industrialisation à grande échelle, ainsi de nombreuses entreprises se cotent en bourse sur des indices américains, déplacent leur siège social à l'étranger, et se vendent à des groupes non-européens (Criteo, Dataïku, Talend). Or, très souvent ces sociétés avaient été aidés par l'argent public français, fait l'objet de contrats avec l'administration, bénéficier de la commande publique.

Depuis plus de quinze ans, la France a construit un continuum de financement (programmes d'investissements d'avenir, French Tech, France 2030, CIR, JEI) pour faire émerger des licornes dans la deeptech, le cloud, l'IA, la cybersécurité ou le quantique. Cependant, les **contreparties associées sont limitées** : l'État actionnaire dispose de peu de leviers pour imposer des choix souverains en matière de cloud ou de localisation de la R&D à ses participations. **Les pactes d'actionnaires ne garantissent pas contre des rachats extra-européens, y compris pour des acteurs stratégiques (Mistral AI).**

D- L'absence de réactions significatives au niveau européen

La Commission a annoncé enfin l'introduction d'un critère « made in Europe », mais rien n'a été fait encore : trop de divergences persistent sur la préférence européenne et l'intensité de la protection du marché. En France, les efforts de soutien à la tech sont réels et significatifs, mais le problème est la tentation de copier la logique de maximisation des valorisations sans en corriger les effets systémiques.

Chapitre 11 – Le déploiement de l'IA : le risque d'une perte de maîtrise

A- Les conséquences économiques

Révolution ou évolution ? Bulle ou pas bulle ?

Tous les chiffres de 2025-2026 montrent une envolée des valorisations et des investissements des hyperscalers (OpenAI, Nvidia, Microsoft, Anthropic), avec des montants obligataires dépassant 100 milliards de dollars et des projets de capacités de calcul de plusieurs gigawatts. Une publication de septembre 2025 (*Technologie report* - Bain) indiquent que les besoins de calcul liés à l'IA augmentent deux fois plus vite que l'efficacité des puces, impliquant des investissements annuels massifs en capacités électriques et data centers, sans que les revenus prévisibles suffisent à les financer intégralement. Plusieurs signaux alertent : Open AI dû arrêter un produit phare Sora trop coûteux, les budgets IA explosent sans bénéfices proportionnels, et 95 majorité des entreprises n'obtiennent pas encore de retour sur investissement de leurs projets

d'IA générative. En fait, on constate une circularité des investissements dans le « cercle de l'intelligence artificielle », composé d'Amazon, AMD, Alphabet (Google), Intel, Microsoft, Nvidia et Oracle, qui jouent simultanément le rôle de clients, d'investisseurs et de bailleurs de fonds, avec un risque de surévaluation de leurs valorisations. Et, à coté de ce gonflement boursier parfois artificiel, se profilent un risque de dépréciations brutales d'actifs liées à l'obsolescence rapide des GPU et infrastructures.

L'impact de IA sur l'emploi : la nécessaire vigilance

Durant les travaux de la commission d'enquête, plusieurs groupes ont annoncé des suppressions de postes en lien avec la généralisation de l'IA. Le secteur bancaire a été particulièrement touché comme celui de la presse. Cependant les études économiques recensées montrent des effets contrastés de l'IA sur l'emploi, selon les secteurs, les types d'outils et les méthodes. Des travaux américains[6] montrent que l'investissement dans l'IA peut augmenter ventes, emploi et valorisation, via une amélioration de l'innovation et une forte hausse de productivité pour les profils novices, sans effet massif de substitution du travail à ce stade. Mais les analyses sur plateformes de freelances mettent en évidence une baisse des missions et des revenus dans les métiers de rédaction, pour les travailleurs qualifiés comme moins expérimentés. Les enquêtes OCDE auprès de travailleurs et employeurs dans 7 pays occidentaux indiquent qu'à ce jour davantage d'entreprises rapportent des baisses d'emploi, avec des suppressions et changements de postes liés à l'IA dans la finance et l'industrie, même si l'ampleur nette des destructions reste difficile à mesurer. En France, l'Insee pointe un phénomène préoccupant : dans les activités informatiques, l'édition et le conseil, l'emploi des 15-29 ans recule nettement, en coïncidence avec la diffusion de l'IA générative.

Les organisations internationales (OIT, FMI, OCDE) développent des indicateurs d'«exposition à l'IA» pour évaluer les tâches substituables. L'OIT conclut que les tâches administratives sont fortement exposées. Plus généralement, il semblerait que certains emplois ont un potentiel d'amélioration avec l'IA et d'autres un potentiel de remplacement, mais la part de l'emploi directement menacé est encore difficile à évaluer. Des travaux sur données françaises (Axelle Arquière - Observatoire des emplois menacés, Antonin Bergeaud - HEC) montrent une rupture par rapport aux vagues précédentes d'automatisation : l'IA se concentre sur les tâches cognitives, complexes et non répétitives, avec de fortes expositions dans les métiers de l'ingénierie, de l'informatique, de la finance, du droit et de certaines activités créatives. Les métiers ancrés dans le monde physique, les soins, la restauration ou le nettoyage restent beaucoup moins automatisables. Des études compilées par la direction générale du Trésor concluent que, agrégés, les effets sur l'emploi peuvent être proches de zéro, mais de nombreux économistes restent très inquiets. Bref, les hypothèses d'évolutions sont complexes, difficilement prédictibles, avec des résultats parfois contradictoires. Les problèmes méthodologiques sont nombreux : incapacité à anticiper les nouveaux métiers de l'IA, manque de prise en compte des contextes organisationnels, juridiques et éthiques, et non-intégration des coûts réels de l'IA (électricité, puces, data centers) dans les modélisations macroéconomiques.

Déploiements de l'IA : impacts pour l'économie française dans la compétition mondiale

Il semblerait admis que l'essor actuel de l'IA tire l'investissement et la croissance américaine, via un effet de richesse lié aux valorisations et aux montants colossaux dans la construction de

6 (Tania Babina, Anastassia Fedyk, Alex He et James Hodson, *Journal of Financial Economics,* janvier 2024 ; Erik Brynjolfsson, Danielle Li et Lindsey R. Raymond, *Quarterly Journal of Economics, mai 2025 ;*Xiang Hui, Oren Reshef et Luofeng Zhou, CESinfo working paper, août 2023)

data center. Mais ce phénomène pourrait être conjoncturel et la *hype* de l'IA pourrait produire un ressenti de productivités supérieur aux gains réels. Pour l'Europe, la question n'est pas le niveau de valeur créée par l'IA, mais la localisation de cette valeur : qui capte les revenus, et où sont réinjectés les gains dans l'économie ? **Le baromètre du numérique (ARCEP, Conseil général de l'écoonomie, Arcom et ANCT) montrent une domination nette des outils d'IA grand public américains (79% ChatGPT) dans les usages des ménages français**, et une forte **dépendance aux hyperscalers pour les solutions professionnelles**. Si les entreprises étrangères captent l'essentiel des gains, les prix intérieurs ne baissent pas, les salariés remplacés peinent à se reclasser et les effets positifs sur le revenu national restent limités. D'où la nécessité d'une régulation de l'accès aux outils d'IA, et de promouvoir des modèles ouverts, afin de limiter les prix et favoriser la concurrence.

B - Les risques techniques : cybersécurité et IA agentique

La diffusion généralisée de l'IA pose la question du contrôle humain, en particulier dans le cas de l'IA agentique, qui vise explicitement à remplacer des personnes dans des actions à effets concrets. Des expertes comme Meredith Whittaker s'inquiètent du paradigme agentique, qui suppose un accès très large aux données des utilisateurs et des capacités d'action autonome, en tension directe avec les exigences de cybersécurité et de protection de la vie privée. L'opacité des décisions algorithmiques est très inquiétante car le salarié, le client, le consommateur ne pourra pas comprendre la décision automatisée prise à son égard, et donc peur être victime d'erreur ou de discrimination.

L'épisode de la suspension par le gouvernement américain de l'accès des non-Étatsuniens aux modèles Fable 5 et Mythos 5 d'Anthropic est un révélateur de la dépendance européenne en cybersécurité. Il est d'abord particulièrement alarmant de constater que la sécurité de l'ensemble de nos systèmes d'information dépend en partie de la décision unilatérale d'une société de fermer ses accès. Mais, plus grave, des tests montrent que Mythos est déjà capable de conduire, de manière autonome, des attaques sur des systèmes faiblement protégés (évaluation du modèle par l'AI Security Institute, agence de recherche britannique). Les experts anticipent une « vague » de découverte massives de vulnérabilités exploitables par des pirates informatiques (« zero days ») dans des logiciels largement répandus, qui pourrait saturer la chaîne de correction (fournisseurs, intégrateurs, clients) et augmenter structurellement le nombre de cyberattaques réussies, y compris sur des systèmes critiques. La dépendance aux solutions extra-européennes n'a jamais été aussi critique en matière de cybersécurité car les leaders mondiaux d'IA sont américains ou chinois, et la capacité européenne de régulation et de contrôle est quasi nulle.

C - De nouvelles vulnérabilités sociales et culturelles

Sur le plan social, les risques de déshumanisation du travail, de précarisation et d'intensification différenciée des tâches sont alarmants. Le cas des livreurs de plateformes, qui sont contrôlés constamment à travers leurs données, et isolés des autres, doit nous alerter sur les dangers du management algorithmique. L'IA pourrait fortement renforcer les inégalités (avec un impact plus fort sur les femmes et les jeunes) et la fragmentation du marché du travail si elle n'est pas accompagnée de politiques de formation, de reconversion et de régulation.

Très préoccupant aussi l'enjeu de la souveraineté informationnelle, avec la généralisation de modèles non européens : les systèmes de recommandation et de génération de contenus peuvent déformer la perception du réel, imposer des biais culturels ou politiques, et rendre la sphère informationnelle dépendante de choix faits aux États-Unis ou en Chine. L'IA façonne les représentations, les langues et les normes, et c'est un pouvoir immense de médiation de l'information. S'ajoute à cela le problème du respect du droit d'auteur : les modèles sont entraînés sur des données littéraires, journalistiques ou scientifiques sans considération pour les droits des auteurs, et les tentatives de légiférer sur ce point se heurtent à un lobbying intense des acteurs de l'IA générative. Une souveraineté numérique européenne ne peut être uniquement économique, elle doit s'articuler à la défense de règles et de valeurs européennes, incluant la protection des données, des droits culturels et du pluralisme informationnel.

Chapitre 12 – Les data centers : instruments clés de la domination des GAFAM?

La démultiplication de projets de très grands data centers en France est directement liée à la perspective d'un développement de l'intelligence artificielle, dont ces infrastructures constituent une condition matérielle indispensable. Le Sommet de l'IA à Paris en février 2025 a servi de déclencheur à une politique offensive de déploiement de data centers, qui soulève des questions de soutenabilité électrique et de souveraineté numérique.

A- Pourquoi implanter des data centers en France ?

Il y a des raisons techniques. L'architecture distribuée de l'internet permet théoriquement de déployer l'IA à partir de capacités de calcul situées partout dans le monde. Cependant, pour certaines applications sensibles à la latence (assistants vocaux, usages industriels avec capteurs et commandes), la proximité géographique entre lieux de requête et capacités de calcul devient déterminante.

Sur le plan économique, la localisation amène au territoire une activité mesurée : construction et exploitation des infrastructures, fourniture des équipements, achat-revente d'électricité, financement des projets et vente de la capacité de calcul des sites. Si les emplois directs liés à la construction sont nombreux, la phase d'exploitation reste peu intensive en main-d'œuvre, avec quelques dizaines d'emplois pour un data center de 100 MW. Enfin ; la localisation du data center ne garantit pas que la valeur créée soit captée par des acteurs français ou européens. Si le data center est utilisé par un *hyperscaler,* la valeur part hors de l'Union européenne.

Du point de vue juridique et politique, la territorialisation des capacités de calcul est pensée comme un outil de souveraineté sur les données. Néanmoins, comme rappelé dans le chapitre 4, la localisation sur le territoire ne suffit pas à assurer la maîtrise des données en raison de l'extraterritorialité de certains droits (notamment états-uniens).

B- État du déploiement : des projets qui bénéficieront en grande majorité aux hyperscalers

La commission d'enquête a eu accès aux données sur les demandes de raccordement au réseau public de transport d'électricité effectuées par les développeurs de projet. Les puissances de raccordement sont présentées de façon agrégée, afin de ne pas divulguer d'informations commercialement sensibles.

Une capacité électrique réservée représentant 24% de la puissance installée du parc nucléaire français et qui pourrait encore augmenter

Les nouvelles demandes de raccordement connaissent une croissance extrêmement rapide et sont d'une ampleur sans commune mesure avec les usages actuels : près de 15 GW de capacité ont été réservés, soit 24% de la puissance installée du parc nucléaire français (qui s'élève à 61,4 GW).

Les porteurs de projet se répartissent en cinq catégories : développeurs-exploitants de data centers, énergéticiens, hyperscalers (AWS, Microsoft, Google), promoteurs immobiliers et logistiques, investisseurs internationaux. La nationalité du développeur ne préjuge pas de celle de l'utilisateur final, et les auditions montrent que **les capacités de calcul sont souvent utilisées majoritairement par des clients extra-européens, comme à Marseille où 60 à 70% des clients de Digital Realty sont non européens**. De nombreux projets portés par des acteurs non spécialisés (promoteurs, énergéticiens, fonds internationaux) cherchent avant tout à valoriser un foncier et une capacité électrique, ce qui renforce la probabilité que les hyperscalers captent l'essentiel des capacités grâce à leur puissance financière.

Au final seul 9% de ces capacités énergétiques réservés le sont par des acteurs français ou européens spécialisés dans le domaine.

C- La trajectoire de développement des datas centers est-elle soutenable pour le réseau électrique français

Les scénarios de RTE suggèrent que, à l'horizon 2030, les volumes d'électricité disponibles devraient suffire pour alimenter les data centers tout en poursuivant la décarbonation des autres secteurs (transport, industrie, bâtiment), notamment parce que tous les projets ne se concrétiseront pas. La consommation des centres de données dédiés pourrait néanmoins atteindre entre 21 et 32 TWh en 2035, puis autour de 50 TWh en 2050. À titre de comparaison, l'électricité totale consommée en région Normandie était de 26,5 TWh en 2024. **Le risque principal n'est pas seulement global (même si RTE affirme que la situation est maîtrisée concernant la demande cumulée de puissance), mais aussi et peut être plus, « infra-territorial » : congestion du réseau dans certaines zones et conflits d'usage avec l'industrie.**

Le mix « bas carbone » : un mauvais argument pour justifier l'accueil des datas centers

La faible intensité carbone du mix électrique français (22 g de CO_2/kWh contre 179 en moyenne dans l'UE) est souvent mise en avant pour attirer des data centers. En effet, les data centers

états-uniens et chinois sont alimentés par un mix énergétique fortement dépendant d'énergies fossiles. Cependant d'une part, dans le cycle de vie, la fabrication, la distribution et la fin de vie continuent de représenter la part la plus émettrice de CO_2. Et d'autre part, l'Ademe indique qu'une expansion tendancielle très forte des consommations pourrait conduire à des émissions incompatibles avec les objectifs de l'Accord de Paris.

Autres enjeux environnementaux majeurs

Les inquiétudes sont connues en termes de consommation d'eau, et une vigilance accrue existe dans ce domaine (avec l'obligation de publication de la consommation de ces centres de données). Mais outre l'empreinte carbone, les projets de très grands data centers, comme Campus IA en Seine-et-Marne, soulèvent des problématiques de consommation de foncier agricole, de pollution atmosphérique liée aux groupes électrogènes de secours, de risques sanitaires liés aux fluides frigorigènes (PFAS) et de création d'îlots de chaleur urbains.

D. Les data centers au cœur des actions du gouvernement : IA summit, fast track et task force

2025, 109 milliards d'euros d'investissements privés ont été annoncés, dont 95 milliards spécifiquement fléchés vers les data centers, avec une très forte présence de capitaux émiratis, canadiens, étatsuniens, britanniques et japonais. Ces annonces sont renforcées en 2026 par de nouveaux projets (quasiment tous à capitaux non français et peu européens) partout en France. Une procédure « fast track» a été créée pour accélérer le raccordement des projets de très grande taille, dépassant 400 MW de puissance électrique. En parallèle, une « task force data centers » pilotée par la DGE, Business France et RTE accompagne 57 entreprises (dont la moitié sont non-européennes et 14 américaines) dans la recherche de foncier, la simplification des procédures et la coordination avec les administrations.

65 sites potentiels ont été identifiés et les atouts français (qualité du réseau électrique, foncier connecté) sont mis en avant dans une vaste opération de marketing territorial destiné aux investisseurs étrangers. Suite à une campagne importante du lobby des Big Tech, le statut de projet national d'intérêt majeur ne sera pas réservé aux acteurs européens, comme l'avait défendu Philippe Latombe. Or si la France dispose effectivement d'une capacité de production électrique importante qui pourrait être utilisée pour fournir des services d'intelligence artificielle, **il y a un risque important d'accaparement de la production électrique par des opérateurs extra-européens et principalement par les *hyperscalers*.**

Aucune hiérarchie n'a été faite entre les différents projets par type d'acteur. La politique de soutien au déploiement des data centers s'effectue tous azimuts, sans aucune prise en compte du profil des futurs exploitants.

Quatrième partie : Pour un nouveau modèle numérique en France et en Europe

La domination des GAFAM sur le numérique européen résulte d'un laisser-faire prolongé qui a créé des dépendances et des vulnérabilités majeures. Leur force tient autant à leurs technologies qu'à l'idée qu'aucune alternative sérieuse n'existerait, les effets de réseau rendant prétendument inéluctables les giga-plateformes.

Chapitre 13 – Des alternatives robustes existent

A- Libre et open source : alternatives à la domination des GAFAM

Le concept de logiciel libre repose sur quatre libertés : d'utiliser le programme pour tous usages, d'étudier le code et l'adapter, de copier le logiciel et de l'améliorer en publiant ces améliorations. La notion de logiciel libre renvoie à une approche communautaire et sociétale, l'open source désigne plutôt la méthode de développement technique. Le logiciel libre a des atouts décisifs dans la lutte contre les vulnérabilités et les dépendances : absence du risque de vendor lock-in, absence de redevances de licence, il s'oppose au principe de captation avec des construction de communautés et d'écosystèmes, la résilience car les utilisateurs gardent la maîtrise du code, la qualité technique, l'auditabilité du code donc la possibilité pour tous d'examiner le code.

Un important potentiel économique

Le modèle économique de l'open source repose sur la vente de services associés : fonctionnalités supplémentaires, contrats de support, hébergement, exploitation. Les clients achètent surtout la capacité à adapter, maintenir et opérer les solutions dans leurs systèmes d'information, ce qui crée un tissu d'entreprises spécialisées. Et la filière française est particulièrement dynamique : une étude Markess de 2022 évalue le marché français open source (logiciels et services) à 5,9 milliards d'euros, soit 11% du marché numérique total, avec une croissance annuelle de 7,8%, et représentait alors 63 800 ETP.

Contribuer aux communs : le défi du financement

Il y a donc nécessité de renforcer cet écosystème pour permettre un véritable passage à l'échelle. Mais les qualités du logiciel libre s'accompagnent de fragilités structurelles. Beaucoup de briques critiques reposent sur des mainteneurs bénévoles ou sous-financés, ce qui expose l'écosystème à des risques de discontinuité, de failles non corrigées et de vulnérabilités globales. Rendre les logiciels libres ergonomiques, robustes et simples d'usage demande des équipes dédiées à temps plein. D'où l'enjeu d'un équilibre entre contributions individuelles et investissements des entreprises ou administrations pour maintenir le code dans la durée.

Soutiens publics aux communs numériques

Plusieurs initiatives publiques visent à stabiliser cet écosystème. En Allemagne, le Sovereign Tech Fund (25 millions d'euros) finance des briques de bas niveau essentielles mais difficiles

à monétiser, en passant par la contractualisation plutôt que la subvention pour préserver l'indépendance des acteurs. La Sovereign Tech Agency salarie, forme et accompagne des développeurs, et peut commander des fonctionnalités jugées d'intérêt général, tout en facilitant l'accès des projets libres aux institutions publique. Au niveau européen, l'Edic Digital Commons réunit plusieurs États (France, Allemagne, Pays-Bas, Italie, Luxembourg) pour investir conjointement dans des briques ouvertes, interopérables et réutilisables.

La commande publique est identifiée comme un levier majeur pour consolider l'écosystème du libre. La loi pour une République numérique (2016) exige que les administrations préservent maîtrise, pérennité et indépendance de leurs SI et encouragent les logiciels libres et formats ouverts, mais ces derniers restent minoritaires en pratique. Plusieurs obstacles limitent l'orientation des achats vers le libre : difficulté à mutualiser les investissements entre communes, contraintes budgétaires qui empêchent d'inscrire certains coûts en investissement amortissable, lourdeur des marchés publics qui favorise les grands groupes au détriment des petits acteurs. Des instruments comme le partenariat d'innovation (directive 2014/24/UE) visent à soutenir des produits innovants développés par de petites entreprises. La CAIH s'est emparée de ce dispositif pour produire une suite hospitalière souveraine open source.

Diffuser la culture des communs numériques dans la sphère professionnelle de l'administration

Le déploiement de logiciels libres se heurte souvent à un manque de compétences internes dans les administrations pour administrer et adapter ces solutions. Les résistances viennent fréquemment des services informatiques dont les compétences sont liées à des technologies propriétaires. Le cas d'Échirolles montre qu'une stratégie de recrutement progressive, profitant du renouvellement des équipes pour intégrer des profils familiers du libre, permet de contourner une conversion brutale d'un service entier. Certains ministères, comme celui de l'Éducation nationale, disposent d'un corps de fonctionnaires spécialisés dans le numérique (ITRF), souvent formés tôt aux technologies libres, ce qui facilite l'appropriation de cette culture. Par ailleurs, des administrations contribuent activement aux communs numériques : la gendarmerie nationale, ou le ministère de l'Éducation nationale via la Forge des communs numériques éducatifs.

B- La nécessaire généralisation des standards ouverts

Les logiciels open source se fondent sur des standards ouverts, mais ceux-ci restent trop peu interopérables avec les solutions dominantes. L'interopérabilité est la capacité de deux systèmes à échanger des données via des formats communs, des protocoles partagés et des interfaces de programmations d'application API. Renforcer les obligations d'interopérabilité est un levier essentiel pour déjouer les monopoles et sortir des dépendances aux acteurs dominants. En brisant les effets de réseau, elle rééquilibre le jeu en faveur des petites entreprises innovantes, qui représentent 99% du tissu productif européen. Les solutions européennes pourraient s'intégrer. Un utilisateur pourrait quitter une grande plateforme tout en continuant à interagir avec des comptes restés sur celle-ci via des réseaux fédérés. Les architectures fédérées et décentralisées (Mastodon, Tchap) illustrent la possibilité d'un écosystème composé de milliers de serveurs détenus par des acteurs différents mais utilisant des protocoles communs.

L'obligation d'interopérabilité s'inscrit progressivement dans le droit européen. Le Data Act (2023) impose la portabilité, l'interopérabilité et l'ouverture des API pour les services cloud,

depuis septembre 2025, et habilite la Commission à adopter des normes harmonisées. En France, la loi SREN (2024) anticipe ces exigences en imposant aux fournisseurs cloud des obligations de portabilité et d'interopérabilité, sous contrôle de l'Arcep. Le DMA impose aux *gate keepers,* plateformes contrôleurs d'accès, une interopérabilité verticale (accès aux fonctionnalités des systèmes d'exploitation) et horizontale (services de messagerie). En pratique, les Big Tech résistent à ces obligations ; ainsi X a délibérément choisi d'empêcher techniquement la portabilité de données.

Or, l'exemple indien d'UPI montre qu'une plateforme publique interopérable peut transformer le système de paiements, en imposant des API gratuites à toutes les banques et en laissant la concurrence se jouer sur les services, sans que les grandes entreprises ne contrôlent l'infrastructure ni les données. En 2024, UPI comptait plus de 500 millions d'utilisateurs et avait fait transiter l'équivalent de 82% du PIB indien. La puissance publique a donc un rôle clé à jouer pour protéger et favoriser ses systèmes, mais aussi pour reprendre le contrôle la définition des standards et protocoles d'internet.

C- Réduire les impacts négatifs de l'IA

Une promotion de l'IA qui ne pense pas les réponses à deux problèmes structurelles - la consommation d'énergie et l'opacité des données d'entraînement - serait une faute politique, aggravant le changement climatique et le pillage de la connaissance.

L'IA frugale

L'Association française de normalisation (Afnor) a publié la Spec 2314, qui définit l'IA frugale comme une réduction des besoins en ressources matérielles et énergétiques via une redéfinition des usages et des exigences de performance, et ce, de la part du producteur, du fournisseur et du client. La frugalité suppose de démontrer que l'IA est nécessaire par rapport à des solutions moins consommatrices, de mesurer et diminuer l'impact environnemental et de questionner les usages à l'aune des limites planétaires.

L'IA open source

L'adaptation de la définition de l'open source aux modèles d'IA a conduit l'Open Source Initiative à publier OSAID 1.0, qui applique les quatre libertés (utiliser, étudier, modifier, partager) aux systèmes d'IA. OSAID 1.0 demande une description complète de toutes les données utilisées, leur provenance, leurs caractéristiques et leurs méthodologies de traitement, ainsi que des listes des ensembles accessibles au public ou via des tiers. Les conséquences de ces choix peu contraignants sont déjà problématiques : de nombreux modèles auto-labellisés « open source » sans respecter OSAID 1.0, créant une situation d'« open-washing » comparable au green-washing. Des recommandations qui ne sont pas pleinement remplies par l'AI Act.

De plus, la définition retenue par OSAID n'exige pas leur publication intégrale des données d'entraînement, privilégiant l'objectif de « reconstruction reproductible » (capacité à pouvoir parvenir au même résultat) plutôt que la transparence complète. Des organisations comme la Free Software Foundation critiquent cette approche et considère ce compromis comme opposé aux valeurs communautaires de l'open source.

Chapitre 14 - Propositions

A - Pour un modèle numérique ouvert et libérateur

L'alternative ne reposera pas sur la reproduction du modèle américain. Les difficultés européennes ne résultent pas d'un excès de régulation ou d'un déficit d'innovation, mais de la position ultra dominante des grandes firmes américaines. Or, « il ne suffit pas de changer la nationalité du tyran » souligne Henri Verdier. Il faut cibler la structure monopolistique elle-même plutôt que la nationalité des acteurs.

L'alternative **réside dans la construction d'un « monde numérique ouvert »,** un écosystème technique à et réglementaire, dans lequel une pluralité d'acteurs peut développer ses solutions sans qu'aucun ne soit en mesure de contrôler les conditions de développement des autres ni d'imposer ses produits**. Et il a deux défis : réussir à concilier la diversité des solutions et le bénéfice des effets de réseau, créer les conditions économiques mécanismes de la pérennité des logiciels libres.**

Il faut aussi revenir à l'ambition fondatrice d'internet : l'accès illimité et non biaisé à la connaissance, sans captation massive de données à des fins lucratives. Nous avons besoin d'une ré-appropriation critique des outils numériques par les administrations, les entreprises et les citoyens et d'une prise de conscience de la nécessité de hiérarchiser les usages numériques ne pas aggraver la situation climatique.

Les dix dernières années ont été celles d'un soutien sans conditions à certains acteurs du numérique, avec l'espoir que la création de licornes résoudrait tous les problèmes. Les prochaines doivent être celles de la redéfinition d'une véritable politique du numérique, axée sur trois objectifs : reconquérir la maîtrise de nos outils, faire respecter le droit et soutenir le développement d'un écosystème économique pérenne et diversifié.

B. Les leviers

La rapporteure formule **29 propositions pour construire un nouveau modèle du numérique plus ouvert et plus indépendant** et **18 recommandations** permettant de réduire les dépendances. *Vous pouvez retrouver toutes ces mesures à partir de la page 381 du rapport.*

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

- 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.

- 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.

- **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.

- **Crédit d'impôt « open source » pour les PME**

Se doter d'un arsenal de souveraineté

- 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.

- 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.

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

- 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

- **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

- 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.
- **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.**

NUMÉRIQUE/S/

UNE ENQUÊTE SUR NOS VULNÉRABILITÉS

Ce document est une synthèse du rapport de la commission d'enquête parlementaire "sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France" créée le 03 février 2026 à l'initiative du groupe Écologiste et Social. **Il a été édité par Madame la Rapporteure Cyrielle Chatelain, le 15 juillet 2026.** Il permet de revenir sur la genèse de cette commission d'enquête, d'établir un diagnostic sur notre dépendance numérique, de comprendre la profondeur de nos vulnérabilités, et les causes de cet enracinement. Et il trace les contours d'un nouveau modèle numérique nécessaire pour la France et l'Europe avec des propositions concrètes et des leviers d'actions.

contact : cyrielle.chatelain@assemblee-nationale.fr